INSTITUTE FOR DEFENSE ANALYSES

Military and Civilian Collaborations in Deploying Next-Generation 9-1-1

Serena Chan, *Project Leader*
Michael T. Hernon

July 2019

Approved for public release; distribution is unlimited.

IDA Document
D-10771
Copy

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

Ronald A. Enlow

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

Copyright Notice

© 2019 Institute for Defense Analyses
4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (a)(16) [Jun 2013].

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-10771

Military and Civilian Collaborations in Deploying Next-Generation 9-1-1

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).

The objective of this work was to examine the challenges DoD 9-1-1 emergency call centers, also known as *public safety answering points* (PSAPs), face in making the necessary migration from the legacy, analog-based, 9-1-1 environment to the next-generation 9-1-1 (NG911) based on digital technologies; to determine the risks in not making the migration; and to ensure that today's capability gap between DoD and civilian first responder agencies does not endure in the NG911 environment.

Shortcomings in DoD policy and funding are seen as the primary reasons for the current capability gap. Should these issues not be addressed, the capability gap will grow, as civilian agencies are increasingly deploying NG911 solutions at the state and regional levels. Maintaining parity with the surrounding civilian agencies is more critical in the NG911 environment than in the legacy, analog-based 9-1-1 environment, as the telecommunications providers will be retiring their entire legacy 9-1-1 infrastructure. In states with a significant DoD presence, such as California and Virginia, the retirement will be as early as 2022 and 2023 (respectively). Hence, installations that do not migrate will become, at best, islands unable to share information with critical mission partners; at worst, they will be unable to process any emergency requests for service. This could result in higher risk to life and property, an inability to meet relevant DoD and Service policies, and degraded capabilities to fulfill obligations under the numerous mutual aid agreements in place today.

In the absence of additional funding to support an NG911 migration for DoD that significantly reduces the capability gap, collaborative approaches between military installations and the abutting civilian jurisdictions can be adopted to minimize or avoid an NG911 capability gap. Collaboration provides substantial benefits to each partner and reflects the strong economic, human capital, and operational bonds between the DoD installations and the communities in which they reside.

DoD–civilian collaborations exist today on a spectrum ranging from a loosely integrated relationship providing minimal support for NG911 to a tightly integrated partnership that eliminates the capability gap entirely (see Figure 1).

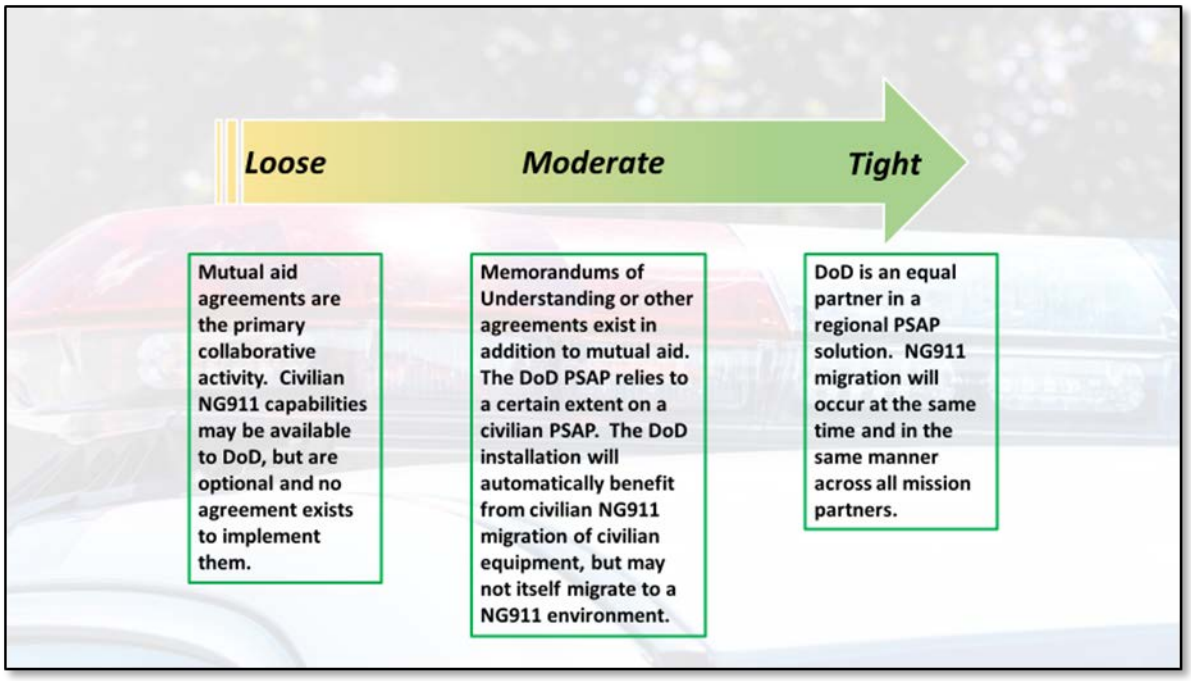


Figure 1. NG911 Collaboration Spectrum

Collaborative approaches deliver a number of enhancements to the mission partner environment, including operational effectiveness, information sharing, interoperability, isolation from .mil networks, improved training, and compliance with DoD and Component policies. Collaboration enhances the ability of all first responders — civilian and DoD — to jointly perform their missions and better serve the entire community in the region.

Examples of the different collaboration models currently in use are discussed as possible models for other DoD installations and their surrounding communities to consider in their NG911 deployments. These case studies highlight a number of issues and lessons learned. Table 1 provides a summary of our findings and recommendations.

Table 1. Findings and Recommendations

Name	Description	Impact	Recommendation
DoD Policy	DoD Components rely on policy to identify requirements and justify budget requests.	Lack of a DoD policy on NG911 could result in a future capability gap.	DoD should release formal guidance on adopting NG911.
Funding	Significant investments in networking, 9-1-1 call handling, and dispatching systems are required to achieve NG911. Much of this funding is being provided by state-administered 9-1-1 user fees and federal grants.	DoD does not, as a rule, benefit from these funding sources.	• The FCC and administrators of 9-1-1 user fees should examine ways of supporting DoD NG911 deployments from the 9-1-1 user fees. • Congress should examine the potential of making federal first responder organizations eligible for federal grants. • DoD Components should identify funding for NG911 migration.
Regionalization	The NG911 architecture facilitates regional approaches which are being adopted by most civilian jurisdictions.	Regional approaches save money while providing better support to every PSAP on the network and in mutual aid operations.	DoD installations should integrate with civilian mission partners' NG911 regional migration plans and governance bodies.
Geographic Information Systems (GIS)	NG911 systems rely on more exact location geocoding than legacy 9-1-1.	Better location information results in faster response times and situational awareness.	DoD installations should develop installation-level GIS data sets following the National Emergency Number Association (NENA) "i3" standards to support NG911.

Contents

1. Introduction....1-1
   A. Background....1-1
2. Problem Statement....2-1
3. The Solution: Collaboration....3-1
   A. NG911 Collaborative Models....3-1
4. Case Studies....4-1
   A. Virginia Beach, VA, Region....4-1
   B. Charleston, SC, Region and Joint Base Charleston....4-3
   C. El Paso and Teller Counties and Fort Carson....4-7
5. Mission Partner Environment Benefits....5-1
   A. Operational Effectiveness....5-1
   B. Information Sharing and Interoperability....5-1
   C. Isolation from .Mil Networks....5-1
   D. Training....5-2
   E. Policy Compliance....5-3
6. Summary and Recommendations....6-1

Appendix A. Secretary of Defense Memorandum: Final Recommendations of the Ft. Hood Follow-on Review....A-1

Appendix B. City of Virginia Beach Request for Proposals....B-1

Appendix C. Memorandum of Agreement Between Charleston County and Joint Base Charleston....C-1

Appendix D. El Paso-Teller County Authority Intergovernmental Agreement....D-1

Appendix E. 2019 Fort Carson PSAP Funding Agreement....E-1

References....R-1

Acronyms and Abbreviations....AA-1

Figures and Tables

Figure 1. NG911 Collaboration Spectrum....ii
Figure 1-1. Legacy (L) vs. NG911 (R) Cellular Call Routing....1-3
Figure 1-2. NG911 Functional Overview....1-4
Figure 2-1. State Deployments of NG911 2012–2017....2-3
Figure 2-2. States' NG911 Progress 2014 (L) and 2017 (R)....2-4
Figure 3-1. NG911 Collaboration Spectrum....3-2
Figure 4-1. Military Facilities in the Virginia Beach Region....4-2
Figure 4-2. Military Facilities in the Charleston, SC Region....4-5
Figure 4-3. Military Presence in Colorado Springs Region....4-8
Figure 4-4. Fort Carson Main Installation....4-9
Figure 4-5. A Wildfire on Fort Carson Threatens State Highway 115....4-11
Figure 4-6. EPTC Regional Call Volume 2009–2018....4-12
Figure 4-7. EPTC Call Volume by Type....4-12
Figure 5-1. High-Level DoD-Civilian ESInet Architecture....5-2

Table 1. Findings and Recommendations....iii
Table 4-1. FY17 DoD Spending in Southeast Virginia....4-2
Table 4-2. FY17 DoD Spending in Charleston, SC Region....4-4
Table 4-3. FY17 DoD Spending in the Colorado Springs Region....4-9
Table 6-1. Findings and Recommendations....6-2

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).

The objective of this work was to examine the difficulties DoD 9-1-1 emergency call centers, also known as *public safety answering points* (PSAPs), face in making the necessary migration from the legacy 9-1-1 environment to next-generation 9-1-1 (NG911); to determine the risks in not making the migration; and to ensure that today's capability gap does not endure in the NG911 environment.

Collaborative approaches between military installations and the abutting civilian jurisdictions is seen as one way to avoid an NG911 capability gap. Collaboration provides substantial benefits to each partner and reflects the strong bonds between DoD installations and the communities where they reside. This document provides current examples of different collaboration models to potentially serve as models for other DoD installations and their surrounding communities to consider in their NG911 deployments.

A. Background

DoD installations do not exist in isolation from the communities that surround them. Rather, the installations and the communities are involved in symbiotic economic, human capital, and operational relationships.

Economically, DoD installations deliver substantial financial benefits to the communities generated by an influx of goods and services provided to the base. Additional benefits come from taxes generated by this DoD-related economic activity and payments to retirees. In fiscal year (FY) 2017, this financial impact was responsible for, on average, 2.3% of a state's gross domestic product (GDP), with a maximum measure of 8.9% of GDP (Virginia).[1] The total spent across the U.S. was $407B, or $1,466 per resident, of which 67% went to procure goods and services. The importance of this impact is clearly recognized by state and local government leadership as evidenced by efforts to avoid base closures and, in many cases, actively promote the expansion of activities on an installation.

[1] All economic data is from the DoD Office of Economic Adjustment, *Defense Spending by State, Revised Version*, March 2019.

From a human capital perspective, most DoD personnel assigned to a base and their family members reside in the community and not on an installation. The population of most installations grows dramatically during the day as civilian employees, contractors, vendors, and military personnel living off-base arrive on the installation to perform their duties. Children of DoD personnel often attend schools in the community regardless of whether they live on- or off-base, and many spouses of DoD personnel work in the private sector off-base.

Lastly, DoD installations and the community-at-large often share operational responsibilities delivering a variety of services. Perhaps the most salient of these operational connections is in public safety, where the ability to effectively answer, process, and respond to a 9-1-1 emergency call directly impacts the health and safety of the entire community, both on- and off-base. There are numerous mutual aid agreements executed between DoD installations and their surrounding jurisdiction(s) that define how these operational responsibilities are shared in any given area.

Protection of the community-at-large, then, can be viewed as neither a DoD nor civilian agency responsibility, but shared by both, given the high level of symbiosis between an installation and the community. However, technological changes threaten to negatively impact how those operations will be conducted in the future.

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. As a result, the networks and systems underlying the way that public safety entities accomplish their missions requires updating or replacement to operate in the NG911 environment.

The benefits of NG911 go far beyond a mere migration from an analog to a digital architecture. NG911 delivers a much broader set of enhanced, as well as new, capabilities throughout the entire life-cycle of an emergency incident, from processing the initial 9-1-1 call, to formulating a response and dispatching first responders, to providing ongoing operational support. These enhancements include the ability to receive text, video, and imagery as a 9-1-1 "call" in addition to voice; increased system resiliency and security; inherent interoperability and information sharing; enhanced support to mutual aid operations; and significantly more accurate caller location information.

Providing more accurate location information is particularly important for DoD installations.[2] As shown in Figure 1-1, a wireless 9-1-1 call made today from within an installation's boundaries will often be delivered to the civilian jurisdiction's PSAP where the cell tower that receives the call is located, not to the installation's PSAP. The call must then be transferred to the installation from the civilian PSAP. Under NG911, that call

[2] For the remainder of this paper, the term *installation* refers to any DoD-owned or -operated base, post, camp, station, or other facility that operates a PSAP or dispatches first responders.

would be delivered directly to the installation's PSAP, saving valuable time in responding to the emergency — time that could save lives.[3]

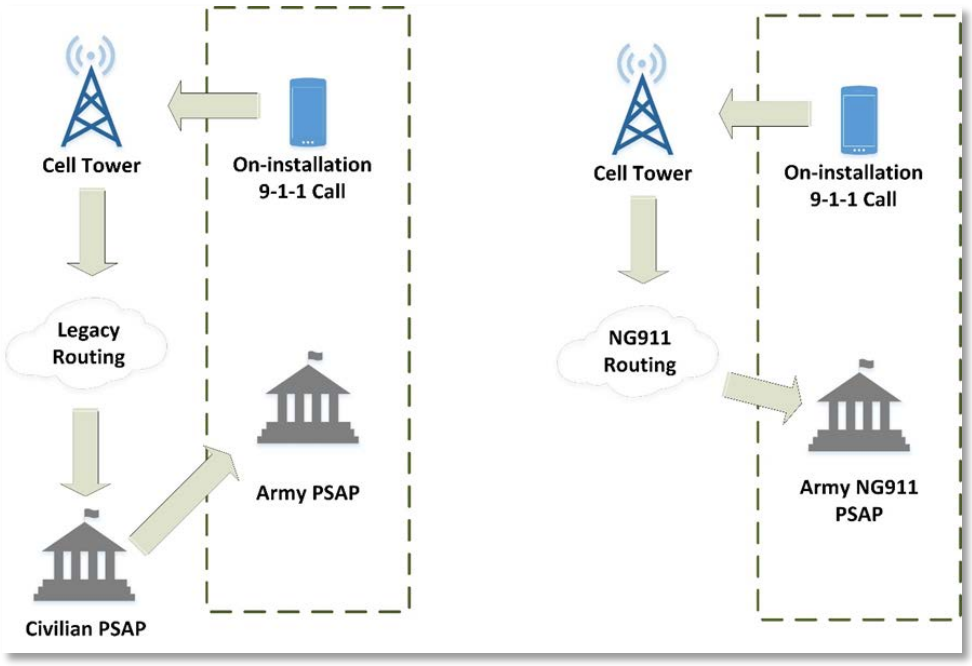


Figure 1-1. Legacy (L) vs. NG911 (R) Cellular Call Routing

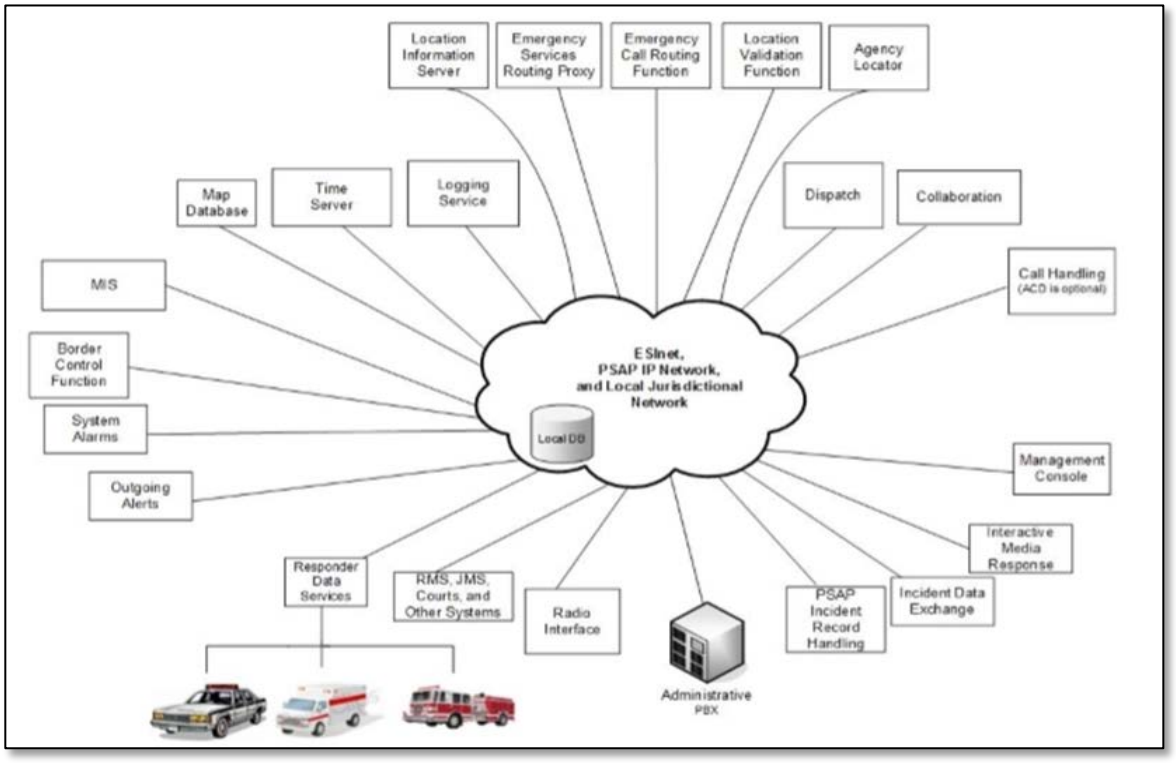
Access to the richer and broader information provided in the NG911 environment results in first responders who are better informed, better prepared, and maximally supported in their missions to save lives and property.

Unlike the legacy 9-1-1 system, NG911 capabilities are based on a common set of technical standards ("i3" standards) developed by the National Emergency Number Association (NENA). These standards include the Emergency Services Internet Protocol Network (ESInet), the digital 9-1-1 network that is replacing the legacy, analog-based 9-1-1 voice network, and Next-Generation Core Services (NGCS), which provide these new capabilities over the ESInet.

Functional requirements, highlighted in Figure 1-2, have been defined by the National 911 Program at the U.S. Department of Transportation (DOT) as well as by the Task Force on Optimal PSAP Architecture convened by the Federal Communication Commission

[3] The Federal Communications Commission (FCC) estimated that providing better location information on 9-1-1 callers would result in reduced response times and save over 10,000 lives a year in the U.S. (FCC14-13)

(FCC).[4] 9-1-1 user fees and various grant programs are supporting much of the state and local government NG911 migrations.



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

Figure 1-2. NG911 Functional Overview

The NG911 technical architecture and the i3 standards render multi-jurisdictional deployments much more feasible than the legacy environment allowed. Regional deployments provide significant economies and operational efficiencies, resulting in a more robust solution. As a result, many jurisdictions are supplementing their 1:1 mutual aid agreements with one-to-many regional NG911 agreements.

From a DoD perspective, NG911 facilitates compliance with DoD Instructions (DoDIs) on emergency management and fire and emergency services (DoDI 6055.17 and 6055.06, respectively), as well as additional policies on information sharing and interoperability with mission partners (DoDI 8320.07 and 8330.01, respectively). NG911 also has a direct, positive impact on many other DoD mission areas, including force protection, anti-terrorism, mission assurance, and critical infrastructure protection.

[4] Similar initiatives are underway in host nations with a DoD presence, such as the NG112 program under the European Emergency Number Association.

2. Problem Statement

Historically, DoD first responder organizations have not, as a rule, maintained parity with their civilian mission partners in 9-1-1 call processing, computer-aided dispatch (CAD) systems, and the various other supporting systems that comprise the 9-1-1 ecosystem. This disparity has led to a 9-1-1 capability gap[5] that often leaves DoD first responders (including call takers and dispatchers, as well as uniformed responders) less optimally equipped to perform their mission than their civilian mission partners abutting the installation.

This gap can be attributed to several factors. Governance is one factor. As a federal agency, DoD is not subject to the FCC regulations governing 9-1-1. Without that mandate, most DoD installations did not build out their 9-1-1 capabilities in a manner that was on a par with civilian standards. After the November 2009 Fort Hood shootings that claimed 13 lives, a Secretary of Defense memorandum endorsed the finding of the follow-on review that "military personnel should receive the same emergency response services as their civilian counterparts."[6] The Secretary's memo also mandated improvements in the DoD emergency management program to deliver capabilities that are common in state and local agencies. These included better information sharing, adopting the National Incident Management System framework, deploying mass warning and notification systems, providing a common operating picture, and adopting Enhanced 9-1-1 (E911), which provides more accurate caller location information, on all installations.

At the time of this writing, there is no DoD policy providing requirements on the suite of information technology networks, systems, and communications supporting DoD first responders or a requirement for NG911. However, the DoD CIO is currently circulating draft policy guidance for senior-level review and adoption.

Funding is another factor that contributes to the capability gap. DoD lacks access to the dedicated, outside funding stream managed by the states and some localities that typically supports civilian PSAPs. This funding stream, provided from the 9-1-1 fees added to monthly phone bills, is covering much of the cost for building civilian ESInets, providing

[5] See Chan, S. and M. Hernon, *Department of the Army: Closing the Next Generation 9-1-1 Capability Gap*, Institute for Defense Analyses, May 2019, for a discussion of the capability gap.

[6] See Appendix A, Secretary of Defense memorandum, *Final Recommendations of the Ft. Hood Follow-on Review*, August 18, 2010, page 15.

access to NGCS, and acquiring other NG911 components. For the year 2017, those fees amounted to nearly $3B, of which almost $200M went to building the NG911 foundation.[7]

An additional source of money supporting NG911 deployments comes from the federal government, including the Federal Emergency Management Agency (FEMA) preparedness grants and the 911 Grant Program in DOT — however, only state-wide or local entities may apply.[8] These grant programs and their eligibility guidelines are established in congressional legislation and enacted into public law. As such, only congressional action could render DoD installations eligible for these NG911 funds.

Without access to a dedicated funding stream, emergency managers on DoD installations are placed in a competition for dollars against the numerous other funding priorities that all installation commanders and headquarters decision makers face each budget cycle.

Although DoD has been slow to implement 9-1-1, E911, CAD, and the myriad other components that make up the 9-1-1 ecosystem as an enterprise, progress has been made over time, and the gap in many installations has been lessened or entirely eliminated. However, all that progress has been accomplished in the legacy, analog environment, which will soon be retired by the telecommunications industry. Hence, the migration to NG911 is as necessary for DoD as it is for their civilian mission partners.

In fact, civilian jurisdictions across the U.S. are well underway in their migrations. As reported in the *2017 National 911 Progress Report* of November 2017, two thirds of states housing major DoD installations had statewide NG911 programs in place. Of those states, almost half had deployed some of their PSAPs onto an ESInet, which is the first step in a migration. ESInets are also being deployed at the sub-state, regional, and even the inter-state level.

The pace of NG911 adoption by the states has rapidly increased since the DOT program began collecting data, as shown in Figure 2-1. Moreover, when one compares the 2014 and 2017 state adoption maps (see Figure 2-2), the gap with DoD mission partners becomes even more evident — many states with a significant DoD presence are utilizing NG911 today by virtue of both being on an ESInet and accessing NGCS over the network.

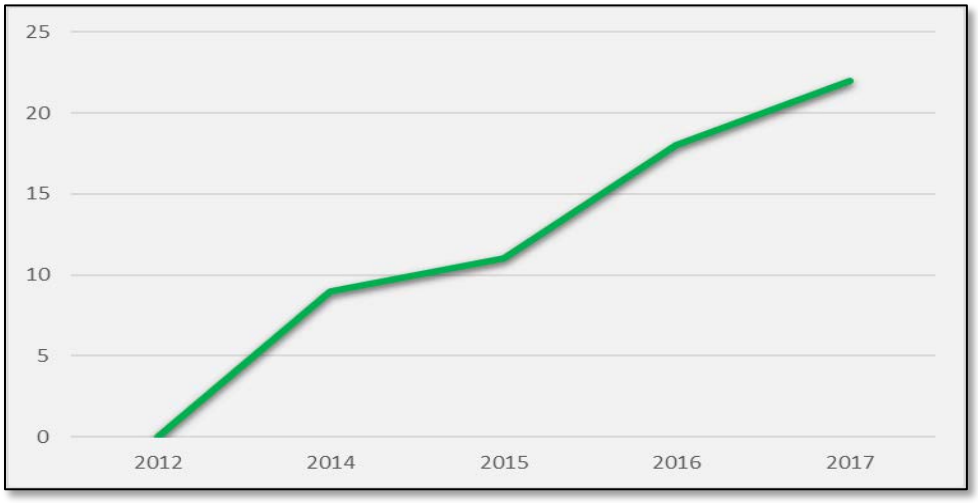
What civilian first responder organizations do in their NG911 migrations is critical to DoD PSAP operations and first responders. Numerous mutual aid agreements exist between DoD installations and civilian police, fire, and emergency services organizations. These outside organizations are key mission partners, and these agreements define how

---

[7] FCC, *Tenth Annual Report to Congress*, December 17, 2018.

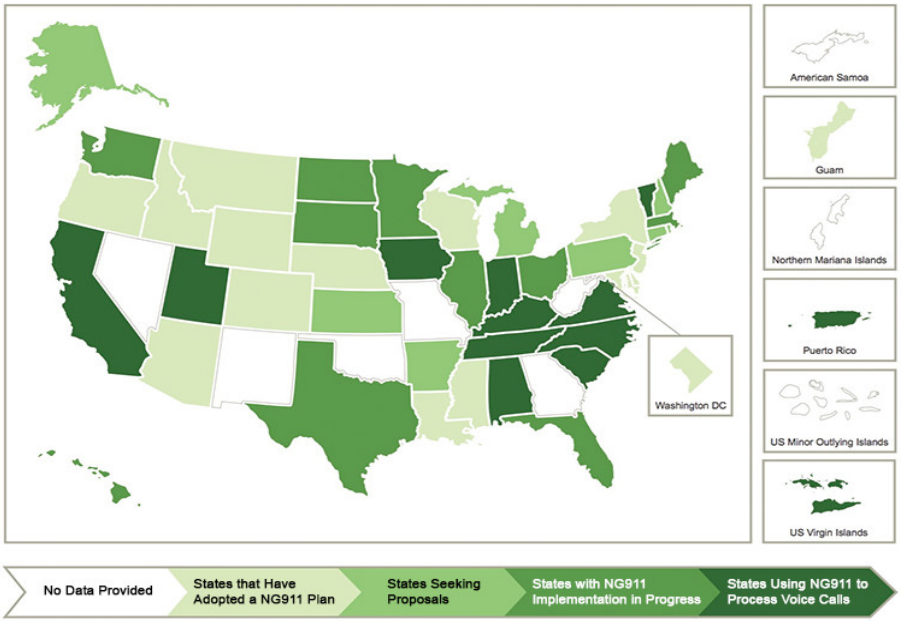
[8] FEMA preparedness grants are available to "state, local, tribal and territorial governments." See https://www.fema.gov/grants. DOT 2019 applications are limited to the District of Columbia and any state, U.S. Territory, or Tribal Organization. See https://www.911.gov/project_911grantprogram.html

non-DoD first responders support emergency operations on DoD installations and vice versa. This support occurs daily for "routine" emergencies, such as an Arlington County ambulance responding to the Pentagon, as well for major incidents, such as the western wildfires, where Fort Carson's firefighters assisted those from civilian and other federal agencies as they, in turn, supported Fort Carson in fighting the wildfires occurring on the installation.



Note: Based on data contained in the *2017 National 911 Progress Report.*

Figure 2-1. State Deployments of NG911 2012–2017



Note: Reprinted from 911.gov, *2014* (top) and *2017* (bottom) *National 911 Progress Report*.

Figure 2-2. States' NG911 Progress 2014 (L) and 2017 (R)

As various regions in the country migrate to an ESInet, the incumbent telephony providers will retire the legacy selective routers that deliver the analog 9-1-1 calls. Eventually, and in the not-too-distant future, all the analog telecommunications networks will be retired.

The decommissioning timetable will vary by state, as the state's public utilities commission or similar body oversees the transition under overarching guidance from the FCC. California, for example, is planning for the selective routers to be retired in 2022.[9] In Virginia, the date is June 2023. However, the decommissioning is an ongoing process — northern Virginia PSAPs, which serve many DoD facilities, including the Pentagon, Fort Belvoir, and Joint Base Myer-Henderson Hall, are expected to begin their transition in late 2019, with the legacy routers in the area expected to be retired within six months. At that point, only an IP-based NG911 solution compliant with NENA i3 standards could support the DoD first responders.[10]

To date, there have been very few NG911-compliant solutions deployed on DoD installations.[11] Installations that do not migrate will become, at best, islands unable to share information with critical mission partners; at worst, they will be unable to process emergency requests for service. This will result in higher risk to life and property, an inability to meet relevant DoD and Service policies, and degraded capabilities to fulfill obligations under the numerous mutual aid agreements in place today.

The ongoing migration to NG911 among DoD civilian mission partners, combined with a lack of DoD progress, represents a significant, growing capability gap for DoD's first responder community as we enter the NG911 era. With the looming retirement of the analog 9-1-1 environment, DoD faces the potential for a dramatic, negative impact on first responder capabilities that would be extremely difficult to mitigate.

---

[9] California Office of Emergency Services, *State 9-1-1 Updates*, November, 2017.

[10] DoD could invest in legacy gateways to provide some level of connectivity with NG911-compliant PSAPs. However, they are designed to be interim solutions and would not mitigate the capability gap.

[11] For a more in-depth analysis of the current environment and NG911 migration from an Army standpoint, see Chan, S. and M. Hernon, *Department of the Army: Closing the Next Generation 9-1-1 Capability Gap*, Institute for Defense Analyses, May 2019.

3. The Solution: Collaboration

Given their symbiotic relationship, DoD installations and their civilian mission partners would ideally migrate to NG911 in a way that ensures alignment and avoids or eliminates capability gaps. A collaborative approach can deliver that objective and enhance the protection of the entire community.

A. NG911 Collaborative Models

Clearly, DoD installations need to migrate to the NG911 environment, but it will be difficult to quickly make a significant reduction in the capability gap without additional funding. Collaborative approaches between military installations and civilian jurisdictions offer one strategy to minimize the impact of the funding shortfall. A collaborative approach would entail leveraging the mission partner environment through DoD 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 most installations compared to a civilian PSAP, a civilian network or system would likely be able to scale up to the increased call volume being introduced from a DoD installation.

Collaboration brings significant benefits to DoD, including the ability to leverage federal and state funding for NG911 that DoD would not normally receive; avoiding the cost of building its own, duplicative, ESInet and contracting for NGCS; as well as the ability to migrate to NG911 much more rapidly than the DoD programming and budgeting process would allow.

Civilian partners also benefit from a collaborative relationship as they are better able to serve the entire community in the area and gain increased visibility into the physical layout and special requirements of the installation – common challenges for many civilian agencies responding to emergencies on DoD property.

The most significant benefit accrues to all partners in the relationship: an enhanced and tightly integrated mission partner environment. This facilitates joint operations under mutual aid agreements and enables first responders from all organizations to accomplish their missions more efficiently and effectively.

There are various models of collaboration between military installations and their surrounding civilian community in place today, ranging from a loose integration at the low end to a tightly integrated mission partner environment at the high end, with a variety of moderately integrated solutions in between. Figure 3-1 below describes each model.

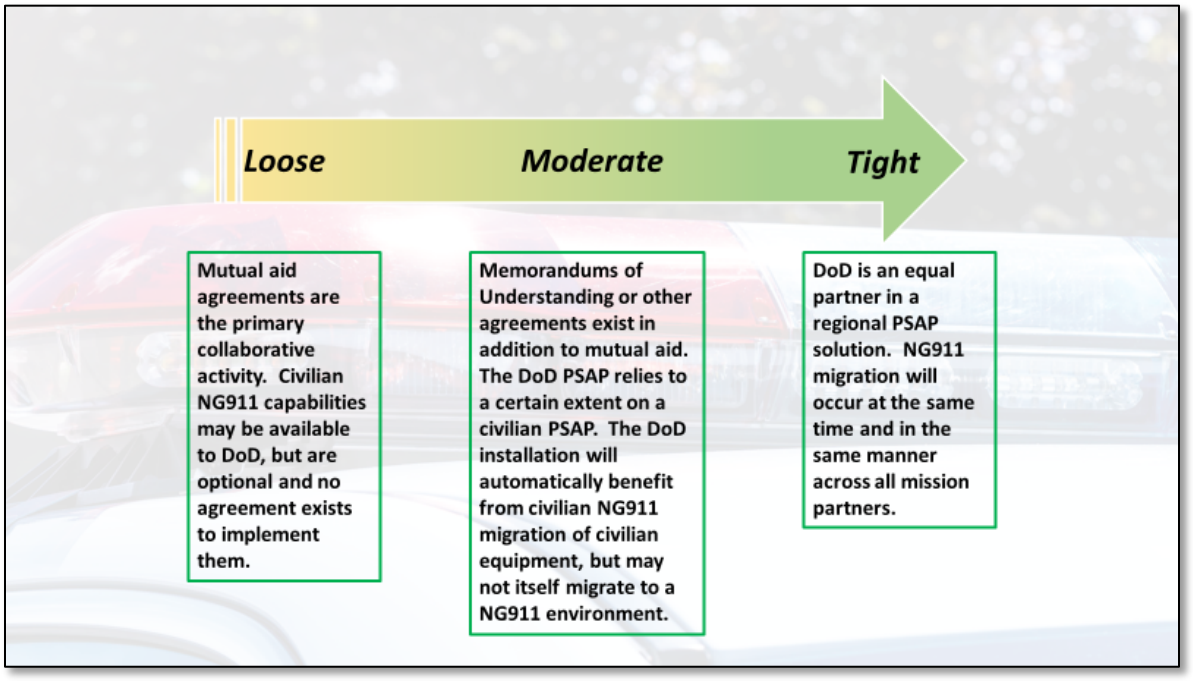


Figure 3-1. NG911 Collaboration Spectrum

The details of how any given collaborative effort is implemented and funded will vary by location depending on the capabilities and resources of the partners. We look at an example exemplifying each model in the next chapter.

4. Case Studies

This section provides examples of current collaborations and the implications for NG911 migration for DoD first responders. For each case, we review the military's impact on the region, current operations, and current or planned NG911 collaborations.

A. Virginia Beach, VA, Region

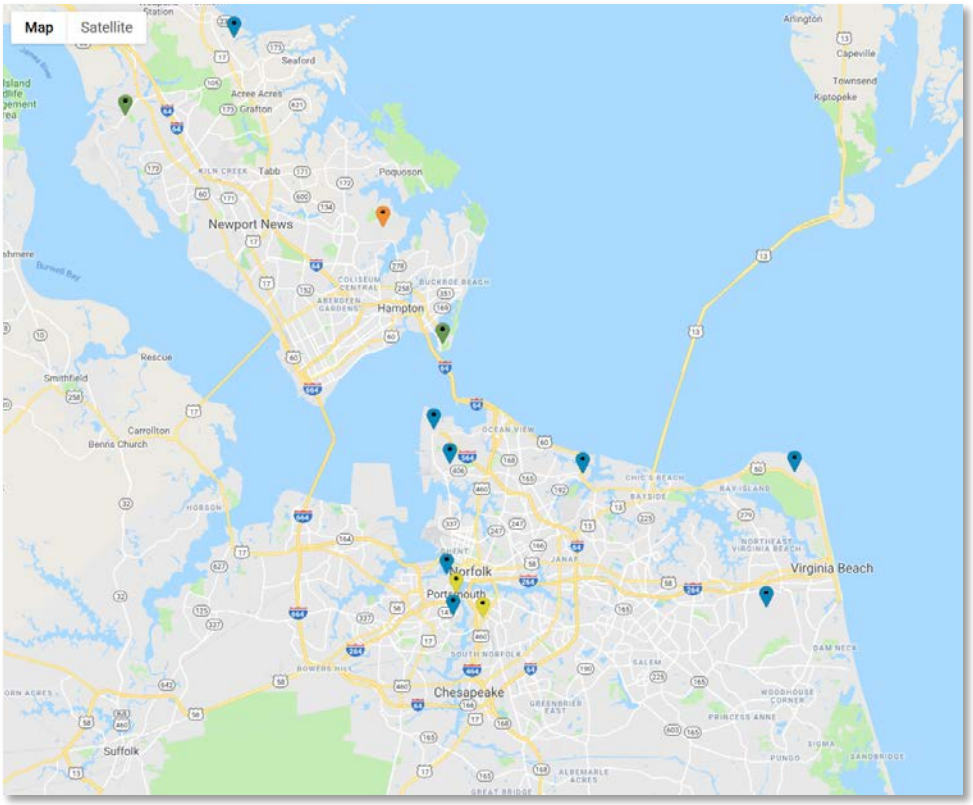
Proactively making civilian NG911 capabilities available to DoD — regardless of whether any agreement is in place to use them — is an example of loose integration. Some civilian jurisdictions have taken this route by including DoD as eligible network nodes in their ESInet and NGCS. The Virginia Beach, VA, region is such a case.

The Virginia Beach region encompasses a number of communities in southeastern Virginia with a 2018 estimated total population of over 1.3M.[12] The City of Virginia Beach is the largest jurisdiction in the region with a 2018 population estimate of 450,189, followed by Norfolk with 244,076, Chesapeake with 242,634, Newport News with 178,626, Hampton with 134,313, Portsmouth with 94,632, and York County, encompassing Tidewater, with 67,846.

The region has a significant military presence (see Figure 4-1) and representation from each Service. These military facilities include Dam Neck Naval Base, Naval Amphibious Base Little Creek, Oceana Master Jet Naval Base, Joint Base Langley-Eustis, Naval Weapons Station Yorktown, and Norfolk Navy Base, the world's largest navy base. In addition, there are other smaller facilities spread throughout the region. According to the latest analysis,[13] there are 97,762 DoD personnel in the region, including active duty and civilian personnel.

[12] All population data are from U.S. Census, July 1, 2018, population estimates. See https://census.gov/quickfacts

[13] DoD Office of Economic Adjustment, *Defense Spending by State, Revised Version,* March 2019.



Source: militarybases.com, retrieved May 25, 2019.

Figure 4-1. Military Facilities in the Virginia Beach Region

As might be expected from the number of DoD installations and personnel, the economic impact to the region is significant. As highlighted in Table 4-1, DoD spending on contracts and personnel in the largest jurisdictions in the region amounted to over $13B in FY2017.

Table 4-1. FY17 DoD Spending in Southeast Virginia

Location	Total
Norfolk	5.0B
Virginia Beach	3.4B
Newport News	2.6B
Portsmouth	1.7B
York County (Tidewater)	0.6B
TOTAL	**13.3B**

Source: DoD Office of Economic Adjustment, *Defense Spending by State, Revised Version*, March 2019.

Current Operations

Each civilian PSAP in the region operates its own 9-1-1 call taking and dispatch facility. Currently, all PSAPs are operating in the legacy, analog environment. Mutual aid agreements exist between each civilian jurisdiction and the military installations their first responders cover.

NG911 Collaboration

The City of Virginia Beach recently released a Request for Proposals (RFP) for a regional ESInet and NGCS to serve the city and surrounding jurisdictions (Appendix B). Included in the RFP is the ability to not only integrate the other civilian regional PSAPs into the solution, but also PSAPs located on the military facilities.

Depending on the results of the RFP, the region may opt to use the existing contract executed by Fairfax County which is available to all Virginia jurisdictions. That RFP (RFP No. 2000002010) and executed contract also requires interoperability with military bases and an option to integrate them into the network.[14]

Impact

In these instances, integrating a military PSAP into the regional ESInet is an option that may or may not be exercised by an installation. However, by including the military locations in the RFP, any subsequent contract awarded to build out the regional ESInet would easily accommodate an installation at a relatively low cost should it choose to exercise the option. This would allow an installation to quickly begin an NG911 migration while ensuring alignment with the regional solution. In this model, the installation would typically be responsible for the cost to connect to the ESInet as well as for its own call-handling equipment (CHE) and CAD solutions.

B. Charleston, SC, Region and Joint Base Charleston

The Charleston, SC, region is an example of a moderate-to-tightly integrated environment.

The City of Charleston is the largest city in South Carolina, with a 2018 estimated population of 136,208.[15] It also serves as the seat of Charleston County, with a total population of 405,905. Berkley and Dorchester Counties abut to the north with populations of 221,091 and 160,647, respectively. Additional counties in the region that will be

[14] The ESInet and NGCS for the Northern Virginia region, which includes a significant military presence, is utilizing this contract and model.

[15] All population data from U.S. Census, July 1, 2018, population estimates. See https://census.gov/quickfacts

participating in NG911 include Horry County, population 344,147; Georgetown County, population 62,249; and Beaufort County with a population of 188,715.

There are a number of military facilities located in Charleston and Berkeley counties that comprise Joint Base Charleston (JB CHS) (see Figure 4-2). The main installations are Charleston Air Force Base and Naval Weapons Station Charleston. JB CHS, which is operated by the Air Force, also contains Marine Corps, Army, and Coast Guard elements, in addition to a number of civilian federal agencies. Nearby, although not part of JB CHS, is Marine Corps Air Station (MCAS) Beaufort in Beaufort County. According to the latest analysis,[16] there are 18,388 DoD personnel in Berkeley and Dorchester counties, including active duty and civilian personnel, with an additional 11,924 in Beaufort County for a regional total of 30,312.

As indicated in Table 4-2, DoD measured the economic impact from contracts and personnel in Charleston, Berkeley, and Beaufort counties to be $3.0B in FY2017. This represents over half of DoD's entire state economic input of $5.1B.[17]

Table 4-2. FY17 DoD Spending in Charleston, SC Region

Location	Total
Charleston County	1.8 B
Berkeley County	0.7 B
Beaufort County	0.5 B
TOTAL	**3.0 B**

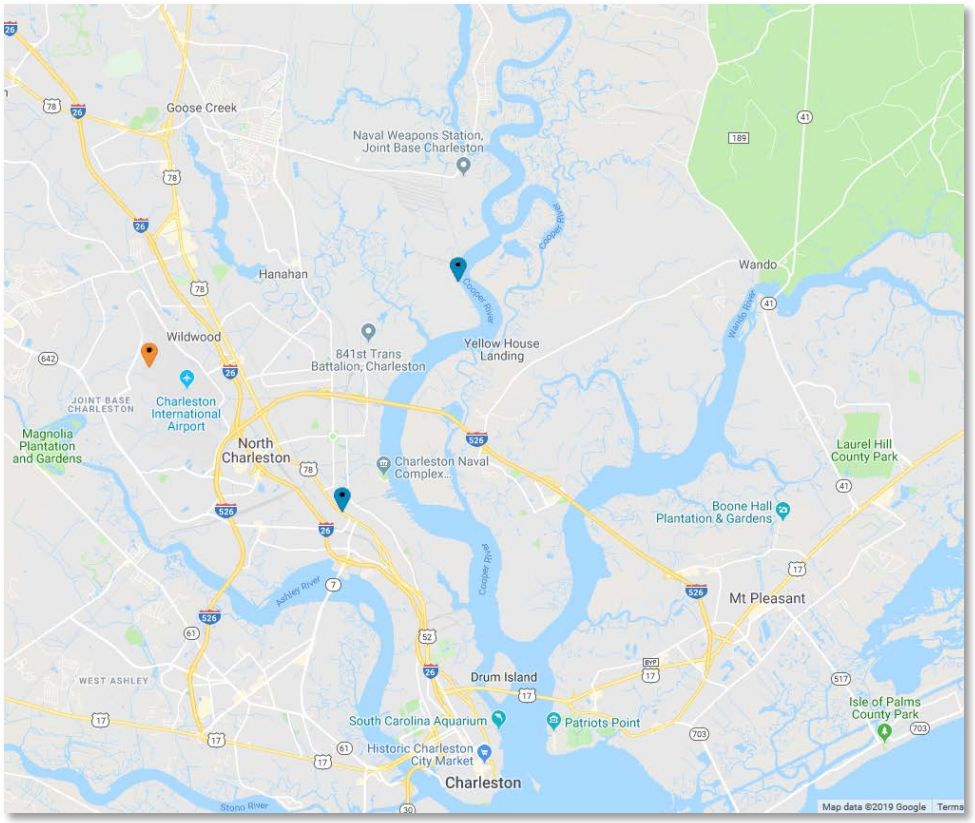
Source: DoD Office of Economic Adjustment, *Defense Spending by State, Revised Version*, March 2019.

A state study[18] looking at the broader economic impact, including contributions from DoD retirees and veterans, estimates that the Charleston region received $10.8B (out of $24.1B statewide) in annual benefits in 2016. The study also estimated that the 18,000 military and DoD civilians in the area were supported by an additional 68,000 jobs — a significant multiplier effect.

[16] DoD Office of Economic Adjustment, *Defense Spending by State, Revised Version,* March 2019.

[17] Ibid.

[18] South Carolina Military Base Task Force, *The Economic Impact of South Carolina's Military Community*, May 2017.



Source: militarybases.com, retrieved May 25, 2019.

Figure 4-2. Military Facilities in the Charleston, SC Region

Current Operations

Charleston County operates the Consolidated Dispatch Center (CDC), which is the primary PSAP in the region. In addition to county first responder agencies, the CDC fields 9-1-1 calls for over 24 other law enforcement, fire, and emergency medical service (EMS) agencies in the area, including the National Park Service. The CDC is staffed by 172 personnel.

The CDC gains significant financial support from 9-1-1 user fees. The state collects $0.62 per month per wireless user, which is then allocated to the counties under a dispersal formula. To collect those monies, the counties must first make an expenditure on eligible items and file for reimbursement. An additional $0.50 fee is collected on wireline bills, which goes directly to the county.

JB CHS maintains an Emergency Communications Center (ECC). The County and JB CHS also each maintain a backup center. All four locations are connected through a private 10MB/s network.

Since 2017, JB CHS has outsourced the answering of all 9-1-1 calls placed from the base's locations in either Charleston or Berkeley County to the CDC.[19] In 2018, the CDC answered an average of 82 calls per month for fire and EMS services and 21 per month for law enforcement from JB CHS. The base maintains the dispatch and response responsibilities through the ECC. This arrangement was formalized under a Memorandum of Agreement (MoA) for 9-1-1 services (Appendix C) executed by both parties.

To further facilitate coordination and interoperability, JB CHS uses remote CAD terminals operating off of the CDC CAD system. The CDC staff also provides training for JB CHS dispatch center personnel. This ensures that JB CHS dispatchers are trained to meet national standards.

Under the MoA, JB CHS paid for CAD licenses and other start-up costs and pays an annual fee to cover a share of the county's PSAP personnel salaries. The MoA builds upon the existing collaborative effort where the county's first responder 800MHz radios are provided to JB CHS first responders to facilitate emergency communications between the parties.

Upgrading the geographic information systems (GIS) data to prepare for NG911 has been an ongoing effort. Currently, almost all structures within the county are geo-coded for NG911. JB CHS has also worked to enhance the available GIS data in the shared system by adding secondary identifying information to structures. This avoids the unique mapping complexities seen on many DoD installations, where a building often has a street address as well as a building number (which is different from the street number).

JB CHS is also adding new capabilities under the MOA, including licenses for mobile data computers for CAD access in emergency vehicles and fire station alerting functionality.

NG911 Collaboration

The county is leading and/or working on several initiatives to facilitate a phased NG911 migration for the region as well as the state as a whole. All expenditures for the following are to be paid for from the 9-1-1 user fee funding stream:

- ***NG911 CHE.*** The county has recently awarded a contract for NG911-compliant CHE, which will be installed over the next several months.
- ***State Legislation.*** Proposed legislation would provide for a state-wide ESInet and NGCS managed by the state 9-1-1 office. The legislation would also permit the

[19] For more information on this model, see Chan, S. et al., *Computer-Aided Dispatch Interoperability Case Studies*, Institute for Defense Analyses, Document D-8778, December 15, 2017.

state office to purchase NG911 equipment on behalf of the counties instead of reimbursing them after they had made expenditures, as is done currently.

- ***Regional ESInet.*** Charleston and five other counties are establishing the Coastal Area ESInet Cooperative. The cooperative collaborated on the requirements for a regional ESInet and NGCS and recently released an RFP (No. 5374-19L). Charleston will serve as the contracting authority, and the partner jurisdictions, including others not in the cooperative, will be able to leverage the contract for their deployments. JB CHS would not be a node on the network, as the base does not handle 9-1-1 calls, but would nonetheless benefit indirectly as CAD users. MCAS Beaufort could potentially benefit from the network as well, directly or indirectly, as Beaufort County is participating in the regional effort.
- ***NG911 CAD.*** The county intends to deploy an NG911-compliant CAD system soon after the ESInet is deployed. One option under consideration is to adopt a cloud-based CAD. Cloud-based CAD systems are relatively new, and the county has been piloting a solution in order to determine the viability of this approach for the region. It is envisioned that JB CHS would operate the same CAD adopted by the county in accordance with the current MoA.

Impact

Outsourcing the call-taker function to the CDC allows JB CHS first responders to focus on their core competencies. It also lets them avoid the difficulties of training, managing, and retaining 9-1-1 call takers, a position that typically has a high turnover rate. Operating on the same CAD platform also avoids the challenges in information sharing and CAD interoperability between the partners.

This partnership will also deliver significant NG911 migration benefits. As JB CHS relies on the CDC systems, the base will automatically benefit from the county's planned NG911 migration. As JB CHS does not answer 9-1-1 calls, they will not be directly connected to the ESInet. Nonetheless, they will benefit from its capabilities through the enhanced information being provided to their dispatchers from the CAD system.

In a June 2019 interview, Jim Lake, Director of the CDC, sees both current and future benefits to the relationship: "Joint Base Charleston and Charleston County have formed a mutually beneficial partnership that allows for information sharing and interoperability. This partnership allows Joint Base Charleston to move forward with Charleston County as we transition to Next Generation 9-1-1."

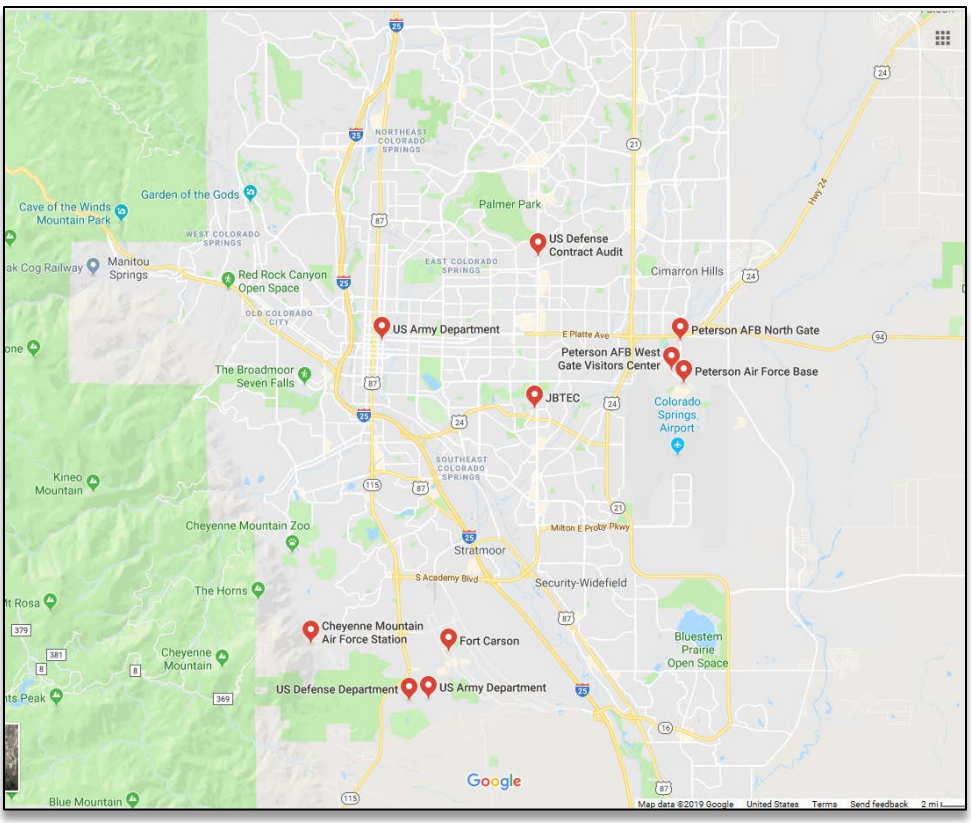
C. El Paso and Teller Counties and Fort Carson

This section focuses on the partnership between Fort Carson and El Paso and Teller Counties (EPTC) in Colorado, which is an example of a tightly integrated environment.

Under this partnership, the Fort Carson PSAP mirrors the capabilities of the civilian PSAPs in addition to being on the regional ESInet.

El Paso County has a population of nearly 700,000 (2017 Census). The City of Colorado Springs is the county seat. Teller County lies adjacent to the west side of El Paso County. Its population is 23,000 (2010 Census).

Military installations in or near EPTC include the United States Air Force Academy, Peterson Air Force Base (AFB), Schriever AFB, and Fort Carson Army Base. These installations, highlighted in Figure 4-3, represent the majority of the DoD presence in Colorado.

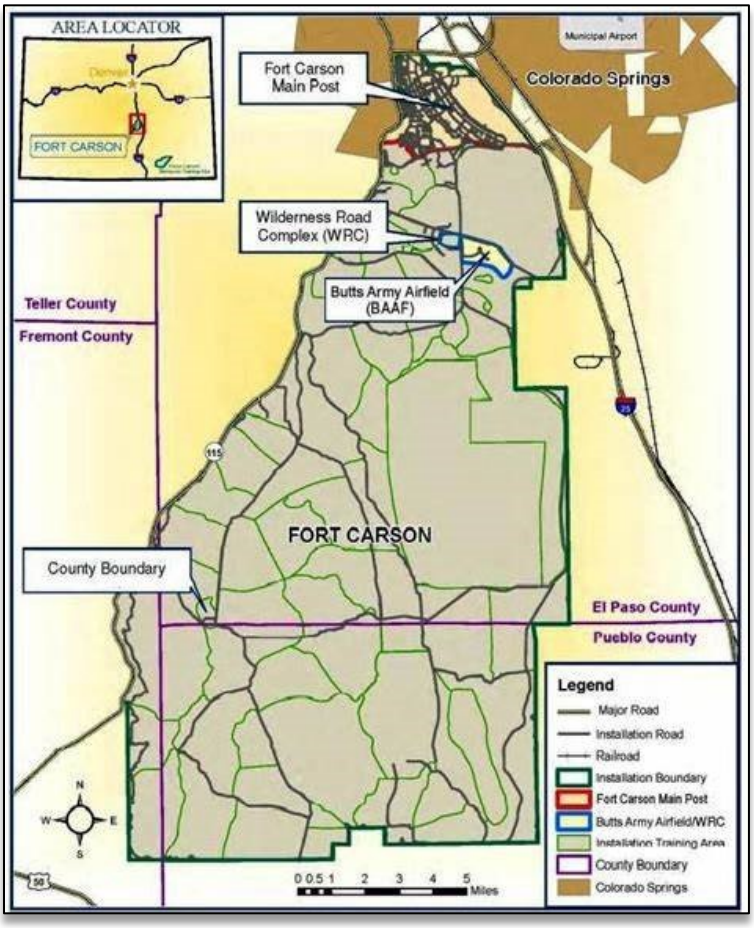


Source: Google Maps.

Figure 4-3. Military Presence in Colorado Springs Region

Fort Carson is a United States Army installation primarily located in unincorporated El Paso County, south of Colorado Springs (see Figure 4-4). The main installation covers 138,523 acres and extends southward into Pueblo and Fremont counties. An additional 235,896 acres is located at the Piñon Canyon Maneuver Site (PCMS) satellite site some 165 miles to the south. The two locations thus combine for a total area of 585 sq. mi. —

nearly as large as the City of Houston, TX (599 sq. mi., 2010 US Census) — making it one of the 10 largest installations in the Army. The installation is the home of the 4th Infantry Division, the 10th Special Forces Group (Airborne), the 440th Civil Affairs Battalion, the 71st Ordnance Group, and a number of smaller commands.



Source: FCF&ES.

Figure 4-4. Fort Carson Main Installation

Table 4-3 summarizes the DoD measurement of the economic impact to the region with nearly $5B spent in El Paso County alone — making it the largest recipient in the state and a majority share of the $8.4B statewide total.

Table 4-3. FY17 DoD Spending in the Colorado Springs Region

Location	Total
El Paso County	4.9B
Pueblo County	0.2B
TOTAL	**5.1B**

Source: DoD Office of Economic Adjustment, *Defense Spending by State, Revised Version*, March 2019.

A 2018 report[20] conducted by the state determined the following additional economic impacts:

- 7.5% of all jobs in Colorado are attributable to the defense sector
- 7.3% of all state taxes and fees were derived from the defense sector
- $25B total Colorado value added from the defense sector
- $36B in products and services from defense sector expenditures
- $11.9M in DoD contracts within Teller County in addition to the above

Current Operations

Both El Paso and Teller Counties have developed a regional approach to 9-1-1 services and created the El Paso–Teller County 911 Authority (the EPTC 911 Authority) as the overarching governance body. The Authority itself is organized under an intergovernmental agreement (IGA) initially executed in 2000 and last updated in 2018 (Appendix D). Fort Carson became a signatory to the agreement in 2019.

The Authority serves as an administrative partner to the seven PSAPs in the two-county service district, including the City of Colorado Springs, Cripple Creek, El Paso County, Fort Carson, Peterson Air Force Base, Teller County, and Woodland Park. The Authority provides systems and services including 9-1-1 call routing, CAD systems, telephones, recorders, training, quality assurance, and public education.

Police services on-base are provided by the Fort Carson Police/Provost Marshal Division with fire and EMS services provided by Fort Carson Fire and Emergency Services (FCF&ES). There are five fire stations located on the installation, including one located in PCMS. Police, fire, and EMS services all fall under the Directorate of Emergency Services.

The Fort Carson ECC is the fort's PSAP and is a consolidated dispatch center serving police and FCF&ES. Sixteen full-time personnel are assigned to the ECC, making it the third-largest PSAP in the region based on staffing.

Automatic aid and mutual aid agreements[21] exist among the FCF&ES agencies in the area, including the Fort. Figure 4-5 shows how a wildfire on Fort Carson threatens its neighboring road – State Highway 115. Although it is not a roadway located on the base,

[20] Colorado Department of Military and Veterans Affairs, *The Economic Impact of Department of Defense, Veterans and Military Retirees, and the Department of Veterans Affairs Activities in Colorado*, May 2018.

[21] Under an automatic aid agreement, one jurisdiction can directly dispatch resources belonging to another jurisdiction without filing a request for assistance, thereby saving time. A mutual aid agreement requires that a request be made whenever assistance is required.

under the automatic aid agreement, FCF&ES are the first to respond to emergencies on the highway, which runs along the western border of the main installation.

Source: Retrieved from https://www.denverpost.com/2008/04/16/three-dead-in-wildfires/ on 5/19/19

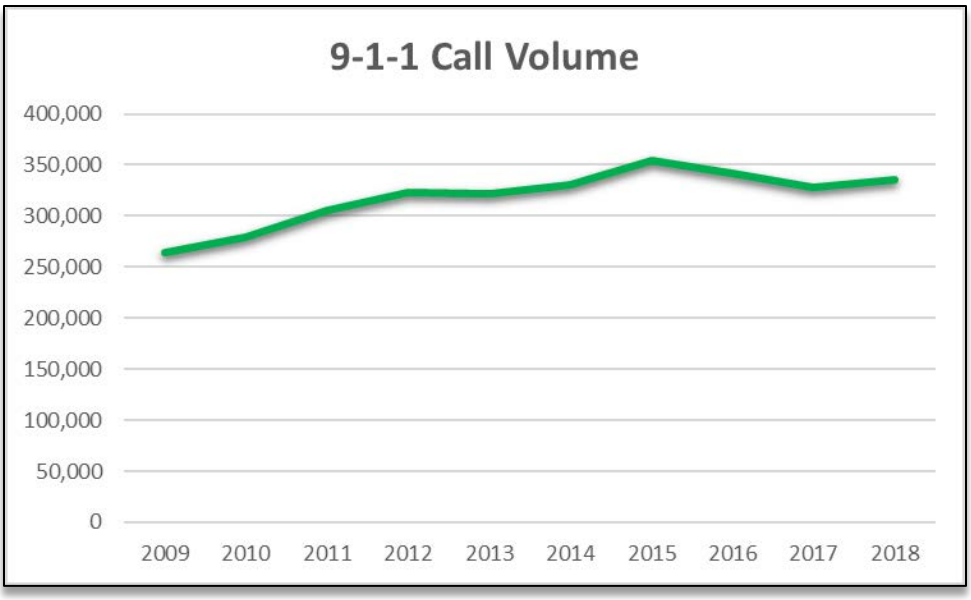
Figure 4-5. A Wildfire on Fort Carson Threatens State Highway 115

The last 10 years have witnessed a rise of more than 25% in the volume of 9-1-1 calls in the Authority's region, with over 335,000 calls for service received in 2018 (see Figure 4-6). As evidenced by a recent analysis of call volumes across all PSAPs, the proportion of calls originating on Ft. Carson is relatively small: a little over 2% of all calls (see Figure 4-7).

The Authority's efforts are funded by a $1.35 9-1-1 fee for users in the region, which is overseen by the state public utilities commission. In calendar year 2016, when the fee was only $.70, those fees amounted to $6.4M.[22]

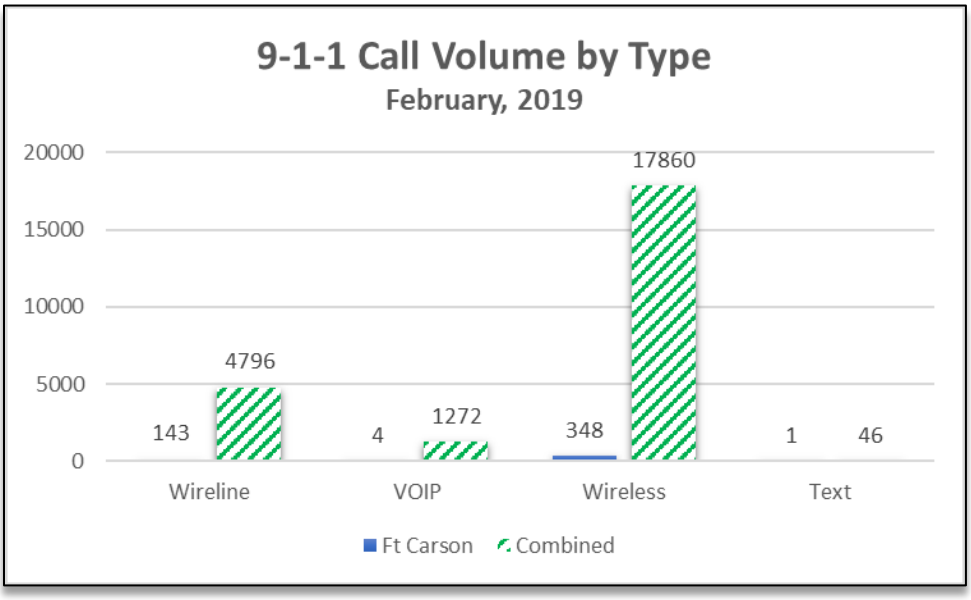
The partnership between Fort Carson and the EPTC 911 Authority has delivered a solution to the installation ensuring that no capability gap exists between civilian first responders in the region and the Army first responders located on the base.

[22] El Paso-Teller County 9-1-1 Authority, *2016 Annual Report*, September 2017.



Based on data from EPCT 911 Authority reports.

Figure 4-6. EPTC Regional Call Volume 2009–2018



Based on data from EPCT 911 Authority reports.

Figure 4-7. EPTC Call Volume by Type

Under the Authority's structure and policies, Fort Carson's PSAP is considered on an equal footing with the civilian facilities the Authority serves and qualifies for financial support under a funding agreement that was recently renewed (Appendix E). This enables Fort Carson to receive benefits and support from the Authority entirely funded by the 9-1-1 fee collection. This represents a rare example of DoD benefitting from the 9-1-1 user fees. Under the policy, the Authority provides the following to each PSAP:

- Console furniture and chairs for 9-1-1 call takers and dispatchers
- IP telephony
- Redundant telephone switches
- 9-1-1 trunks and related telephone lines
- Recording equipment for both telephony and radio systems
- Headsets
- Call-taker software
- Call-taker protocol cardsets (police, fire, and EMS scripts)
- CAD equipment and maintenance
- Mobile data services for emergency vehicles and responders, including automatic vehicle location and automatic person location services
- Servers and workstations
- Training
- Generators and uninterruptable power supplies
- One printer
- Maintenance costs for the above

The Authority also offers additional commercial services that PSAPs may opt into. These include Smart911, which allows the community to populate the PSAP's database with medical and other information prior to an emergency, and RapidSOS, which provides enhanced location information.

Due to this relationship, the Authority recently assumed the expense for upgrading the Fort Carson PSAP as part of the overall PSAP modernization effort in the region. The initial expenditure spent in this effort amounted to over $900,000, which delivered the following:

- The same NG911-capable CAD system used by 6 of the 7 PSAPs served by the Authority
- New 9-1-1 call taking software
- Uninterruptible power supply
- New servers and workstations
- Radio upgrades
- Consoles for call takers and dispatchers

In addition to the acquisition costs, the Authority has assumed the maintenance costs for the above, amounting to nearly $200,000 per year.

Fort Carson's PSAP is also connected to the regional ESInet, making it one of the first DoD installations to reach that NG911 milestone.

The Fort does have commercial cell towers located within its boundaries, and it does receive some wireless 9-1-1 calls directly. While not an NG911 solution at this point, it does deliver emergency calls to the installation PSAP faster than is the case in many DoD installations.

NG911 Collaboration

The Authority is executing an NG911 migration as laid out in their strategic plan. As part of this effort, a regional ESInet has been deployed — the first in the state. Collaboration for the partners regarding NG911 is an ongoing process — the heads of the region's PSAPs meet on a bi-monthly basis to review performance and plan for future enhancements to their environment.

Like most jurisdictions, the Authority is planning to phase in the NG911 deployment across the region, including Fort Carson. This assists in mitigating risks and allows system components to "burn in" before adding new components. Upcoming enhancements planned for the near-future include the following:

- ***NG911 CHE***. New CHE with an integrated mapping capability will be deployed to every PSAP in the region. NG911-compliant CHE is required to reap the benefits of the NGCS being delivered over the ESInet.
- ***CAD Centralization***. A centralized environment is planned to replace the separate CAD systems currently located at each PSAP. This will result in an even more tightly integrated environment and make dedicated testing and training CAD environments available to each PSAP.
- ***Fort Carson GIS***. The Authority's GIS team is working with the Fort Carson GIS team to make the base GIS data compatible with NENA NG911 requirements. This will allow the fort's map to be integrated with the regional map in the NG911 solution.
- ***Location-based Dispatching***. Today's block-based mapping will be updated to support *x, y* coordinates to deliver NG911 enhanced location information.
- ***Next-Generation Text-to-9-1-1***. The Authority will deploy an NG911-compliant, integrated text-to-9-1-1 capability to every PSAP in the region, replacing the current solution.
- ***Expansion to Other DoD Installations***. The Authority is planning to deliver the same benefits to Peterson Air Force Base and the Cheyenne Mountain Complex.

When the NG911 migration is completed, Fort Carson, along with every other PSAP in the region, will reap the full complement of benefits the next generation environment brings.

Impact

The collaboration has led to a number of operational benefits, including seamless, one-button transfers of 9-1-1 calls between PSAPs when necessary, the ability to easily handle overflow 9-1-1 calls from another PSAP, the ability for a civilian PSAP to directly dispatch FCF&ES vehicles to incidents outside the base's fence line, and CAD to CAD data transfers.

The relationship also helps the installation comply with the requirements of Army Regulation 525-27, the Army Emergency Management Program, and Army Installation Management Command's common levels of service requirements. Modernizing the PSAP's network by joining the ESInet is also consistent with the goals of the Army Network Campaign Plan.

The value of this partnership is recognized by the civilian and Army leadership alike. In a May 2019 interview, Dawn Lucero, Fort Carson's ECC Chief, said "Our close working relationship with the El Paso-Teller County 911 Authority and the other local PSAPs has evened the playing field for us. We are equipped to provide the exact same level of care to every 9-1-1 caller who reaches our center as compared to the other much larger 9-1-1 centers in the area. Callers to our PSAP are in great hands thanks to the collaboration and support that we have received from the 911 Authority." In an April 2019 interview, Carl Simpson, the CEO of the EPTC 911 Authority, stated "The bang for the buck is that the PSAPs will gain better interoperability, situational awareness, and will be capable of enhancing information sharing between agencies."

5. Mission Partner Environment Benefits

Collaboration between civilian and DoD PSAPs delivers a suite of benefits to the partners that enhance the ability of all first responders to jointly perform their missions across the entire region and better serve the entire population.

A. Operational Effectiveness

The technical and operational benefits of collaboration directly contribute to time savings in the lifecycle of a 9-1-1 call for service. The impact of that, as noted by FCC report cited above, is lives saved. Installations, particularly those in settings with a moderate or tight level of integration, are better equipped to meet the DoD mandate of providing the same level of emergency services on the installation that people enjoy outside the fence.

B. Information Sharing and Interoperability

Being on the same network as the surrounding jurisdictions inherently provides an information sharing capability, even in a loosely integrated environment. In moderate to tightly integrated environments, information sharing becomes increasingly seamless, particularly if the same CAD system is deployed. Likewise, systems sharing the same ESInet and other NG911 components will have a higher level of interoperability than do those using gateways or other workarounds.

C. Isolation from .Mil Networks

Although it is DoD policy to interface DoD systems with mission partner networks to share information as appropriate,[23] this can prove to be a difficult exercise in practice due to other DoD policies regarding information assurance. Having an installation's PSAP on the civilian ESInet in lieu of a military network, such as on Fort Carson, dramatically simplifies the PSAP's networking. As Figure 5-1 shows, none of the equipment in the PSAP touches the .mil network environment in this scenario, even though the PSAP itself sits on the installation.

[23] See DoD Instruction 8110.01, *Mission Partner Environment Information Sharing Capability Implementation for the DoD*, November 25, 2014. As per the policy, mission partners explicitly include state, local, and tribal governments.

By isolating the NG911 systems from the military networking environment, the need to comply with DoD's information assurance safeguards is reduced. As a result, the systems and the network interface do not have to be accredited in accordance with DoD practices, and civilian users do not need to be credentialed by DoD. NENA i3 security standards, which are common across all ESInets, are utilized in lieu of the DoD standards. These standards are strict and robust in themselves, as protected law enforcement information, health information covered by federal law, and personally identifiable information are all communicated over an ESInet.

This network model also increases the variety of systems available to the DoD public safety community. Few manufacturers opt to submit their public safety solutions for DoD certification given the relatively small size of the market and the costs that must be incurred. A similar model exists for JB CHS, which is connected via a network operated by the civilian jurisdiction.

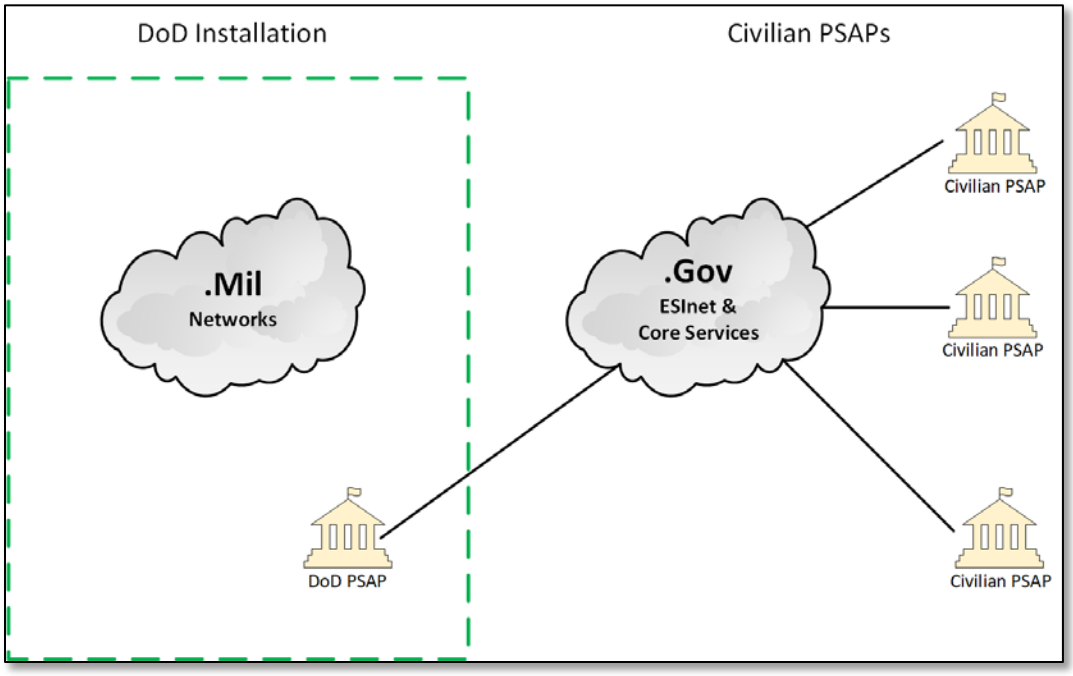


Figure 5-1. High-Level DoD-Civilian ESInet Architecture

D. Training

In the moderate and tightly integrated case studies, DoD personnel received the same training provided to their civilian counterparts. This ensures that all partners meet the same national training standards and facilitates joint operations and communications.

E. Policy Compliance

Closing the capability gap through collaboration assists the DoD first responder organizations in meeting the requirements of several DoD policies listed below, as well as relevant Component-specific policies:

- DoDI 6055.06, *DoD Fire and Emergency Services Program*, Change 1, August 31, 2018
- DoDI 6055.17. *DoD Emergency Management Program*, February 13, 2017
- DoD Instruction 8110.01, *Mission Partner Environment Information Sharing Capability Implementation for the DoD,* November 25, 2014
- DoDI 8130.01, *Installation Geospatial Information and Services,* April 9, 2015
- 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
- USNORTHCOM Instruction 10-222, *Force Protection Mission and Antiterrorism Program*

6. Summary and Recommendations

The historical capability gap between civilian first responder agencies and many DoD first responder agencies will be significantly exacerbated as civilian agencies across the U.S. migrate to NG911. Similar migrations are also happening in host nations housing DoD installations (i.e., NG112 migration in Europe). Should DoD be left behind, there will be a significant increase in risk to life and property.

To mitigate the effects of this capability gap, it will be necessary to address DoD policy and funding shortcomings. However, with some states looking to complete their NG911 migration as early as 2022, there will be insufficient time to rely on the traditional programming and budgeting process to close the gap.

Alternatively, or in addition to the programming and budgeting process, collaborations with civilian mission partners could facilitate a faster migration. This report examined various collaboration models existing today between DoD installations and local government first responder organizations and their impact on NG911 migration. These case studies highlight how various collaboration models can assist in solving the challenges that DoD first responder agencies face in migrating to the NG911 environment. As each region in the country is different, variations on these models is to be expected.

The collaborative relationship between Fort Carson and the EPTC 911 Authority is an exemplary tightly integrated partnership that is delivering significant benefits, not only to the first responders but to the entire population of the region. Due to this relationship, there is zero capability gap today between the DoD first responders and their civilian counterparts, and the Fort will migrate to NG911 in lockstep with the region. JB CHS also benefits from a strong partnership.

Even a loosely integrated relationship, such as connecting an installation to a civilian ESInet, could assist DoD in meeting the migration challenges. Regardless of the type of relationship, collaboration with civilian and regional initiatives will likely be required if DoD first responders are to be supported in the NG911 environment.

The case studies have highlighted a number of issues and lessons learned for other regions and decision makers to consider. We summarize these findings along with recommendations in Table 6-1.

Table 6-1. Findings and Recommendations

Name	Description	Impact	Recommendation
DoD Policy	DoD Components rely on policy to identify requirements and justify budget requests.	Lack of a DoD policy on NG911 could result in a future capability gap.	DoD should release formal guidance on adopting NG911.
Funding	Significant investments in networking, 9-1-1 call handling, and dispatching systems are required to achieve NG911. Much of this funding is being provided by state-administered 9-1-1 user fees and federal grants.	DoD does not, as a rule, benefit from these funding sources.	• The FCC and administrators of 9-1-1 user fees should examine ways of supporting DoD NG911 deployments from the 9-1-1 user fees. • Congress should examine the potential of making federal first responder organizations eligible for federal grants. • DoD Components should identify funding for NG911 migration.
Regionalization	The NG911 architecture facilitates regional approaches which are being adopted by most civilian jurisdictions.	Regional approaches save money while providing better support to every PSAP on the network and in mutual aid operations.	DoD installations should integrate with civilian mission partners' NG911 regional migration plans and governance bodies.
Geographic Information Systems (GIS)	NG911 systems rely on more exact location geocoding than legacy 9-1-1.	Better location information results in faster response times and situational awareness.	DoD installations should develop installation-level GIS data sets following National Emergency Number Association (NENA) "i3" standards to support NG911.

Appendix A.
Secretary of Defense Memorandum: Final Recommendations of the Ft. Hood Follow-on Review

THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

AUG 18 2010

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Final Recommendations of the Ft. Hood Follow-on Review

The tragic shooting of U.S. military personnel at Fort Hood in November 2009 underscored the need for the DoD to thoroughly review its approach to force protection and to broaden its force protection policies, programs, and procedures to go beyond their traditional focus on hostile external threats. I commissioned the DoD Independent Review Related to Fort Hood to assist the Department in identifying existing gaps and deficiencies, and also to help broaden the Department's force protection approach to reflect more effectively the challenging security environment in which we operate.

I have carefully considered the recommendations in the Independent Review's report, *Protecting the Force: Lessons Learned from Fort Hood*, and am directing that the Department respond to them by taking appropriate action, as specified in the attached final report of the DoD Follow-on Review to the Fort Hood incident. In a small number of cases, further study will be required before the Department can take additional steps. For the majority of recommendations, however, the Follow-on Review recommends concrete actions. The Department will make every effort to safeguard civil liberties as it develops these policies and programs.

These initiatives will significantly improve the Department's ability to mitigate internal threats, ensure force protection, enable emergency response, and provide care for victims and families. In particular, the Department will strengthen its policies, programs, and procedures in the following areas:

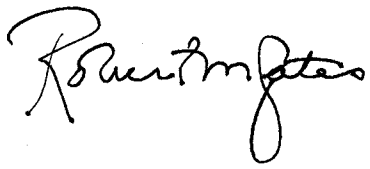
- Addressing workplace violence;
- Ensuring commander and supervisor access to appropriate information in personnel records;
- Improving information sharing with partner agencies and among installations;
- Expanding installations' emergency response capabilities;
- Integrating force protection policy, and clarifying force protection roles and responsibilities; and

OSD 07688-10

- Ensuring that we provide top quality health care to both our service members and our healthcare providers.

I expect Department leaders to place great priority on implementing these recommendations. To ensure the Department maintains an enduring focus on eliminating the gaps and deficiencies identified in *Protecting the Force*, I am directing that the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD&ASA)) continue to lead the Fort Hood Follow-on Review as it transitions its focus to monitoring implementation of the actions directed in this memorandum. The ASD(HD&ASA) will provide regular implementation progress reports to me, not only on those measures that I have approved, but also on progress by Military Department Secretaries and Combatant Commanders to mitigate issues identified in their independent internal reviews. The ASD(HD&ASA) will continue in this role until such point that he advises that implementation of each recommendation is sufficiently underway to render further monitoring unnecessary.

Force protection, although critical, is not a substitute for leadership. Leaders at every level in our military play a critical role. Leading forces is both a duty and a privilege, and it carries with it the clear responsibility to ensure good order and discipline. Leaders must be prepared to intervene when necessary; poor performance should never be ignored. The Department will continue to enable military leaders with the tools and discretion they need to take appropriate action to prevent and respond to potential problems, whatever their cause. As the Department takes steps to strengthen its approach to force protection, I ask leaders and commanders across the force to remain mindful of the unique requirements of the profession of arms – that military service is grounded in an oath to support and defend our Constitution, but also may necessitate the sacrifice of some of the very rights we defend. Our all-volunteer force reflects the strength of our national diversity and is composed of patriots who are first and foremost Soldiers, Sailors, Airmen, or Marines sworn to uphold our national values.



Attachment:
As stated

DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEFS OF THE MILITARY SERVICES
COMMANDERS OF THE COMBATANT COMMANDS
CHIEF OF THE NATIONAL GUARD BUREAU
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

Department of Defense Implementation of Recommendations

from the Independent Review Related to Fort Hood

Recommendation 2.1 a-d: Update Policies and Develop Programs to Identify Behavioral Indicators of Violence

The Independent Review found that DoD programs, policies, processes, and procedures that address identification of indicators for violence and radicalization are outdated, incomplete, and fail to include key indicators of potentially violent behaviors. There is no risk assessment system available to supervisors and commanders to help them identify and mitigate internal threats. Such a system must be developed to provide supervisors and commanders with better tools to identify internal threats, recognize when to intervene, and make judgment calls in disciplinary cases and when conducting performance and career counseling.

- **Future Action to Identify Behavioral Indicators of Violence:** The Department will take a 3-step approach to provide commanders and supervisors with the information and tools needed to identify and respond to internal threats. First, the Department will issue commanders and civilian supervisors interim guidance on how to identify internal threats.
- Second, the Department will conduct three formal studies to deepen our understanding of internal threats and refine the guidance contained in the interim message. By March 2011, the Defense Science Board (DSB) will identify behavioral indicators of violence and radicalization, develop threat assessment methodologies, and investigate optimal insider threat training delivery methods. In addition, OASD (HA) will conduct two scientific studies, one retrospective and one prospective, that will examine DoD populations and develop a scientifically based list of behavioral indicators of potential violence. The Follow-On Review Senior Steering Group will also coordinate with the FBI Behavioral Science Unit to further strengthen our understanding of insider threat.
- Third, the Under Secretary of Defense for Personnel and Readiness (USD (P&R)) and the Under Secretary of Defense for Intelligence (USD(I)) will integrate the Department's findings into existing programs no later than September 2011. Results from longer-term, ongoing studies will be integrated into policies and programs as appropriate upon study completion.

Recommendation 2.2 a-d: Review Personnel Policies for Access to Installations and Information

The Independent Review found that background checks on civilians entering the military or DoD civilian workforce may be incomplete, too limited in scope, or not conducted at all. The Independent Review also found that guidelines for adjudicating security clearances are vague, and training on how and to whom significant information reports are made is insufficient. Successful implementation of Homeland Security Presidential Directive-12 (HSPD-12), a government-wide standard for reliable identification verification, will mitigate current risk assumed by DoD. It mandates that all employees requiring a DoD Common Access Card (CAC) undergo, at a minimum, a National Agency Check with Inquiries prior to receiving a CAC. Some employee populations (i.e., temporary or seasonal hires) are not subject to mandatory

background investigations under HSPD-12. Further mitigating risk, the interagency Joint Reform Team (JRT) made recommendations to reform federal investigative standards, including revising the scope of the National Agency Check with Local Agency (NACLC) and aligning suitability for employment with national security.

The JRT effort to revise the scope of the NACLC renders unnecessary the Independent Review recommendation to review the appropriateness of the NACLC as a minimum background investigation for a DoD SECRET clearance. In addition, the Follow-on Review found no evidence that legal advisors lack understanding of the adjudicative guidelines or that the guidelines are vague, negating the need for additional specialized training.

- **Future Action to Strengthen Installation Access Policies:** The Under Secretary of Defense for Intelligence (USD(I)) , in consultation with the Under Secretary of Defense for Personnel and Readiness (USD(P&R), will revise DoDI 5200.02 and DoDM 5200.02 (currently both in draft form with the title *Personnel Security Program*) to comply with HSPD-12 mandates and JRT reform efforts no later than September 2011. Additionally, USD(I) will develop a plan to ensure the widest dissemination of *Roles and Responsibilities for Personnel Security: A Guide for Supervisors* throughout DoD so commanders and supervisors have access to this information. USD(P&R) will publish policy designating which individuals not covered by HSPD-12 should receive background investigations. USD(P&R) will also review current policy regarding expedited citizenship for certain classes of workers and make recommendations for updates by December 2010. The Department is projected to be in full HSPD-12 compliance by the end of CY 2012.

Recommendation 2.3: Recognition of Individuals as Ecclesiastical Endorsers of Chaplains

The Independent Review found that DoD standards for denying requests from organizations that want recognition as an ecclesiastical endorser are inadequate. An ecclesiastical endorser issues and withdraws credentials given to individuals to perform religious services in accordance with the practice of the granting organization. DoD Instruction (DoDI) 1304.28 (Guidance for the Appointment of Chaplains for the Military Departments) provides the Department with broad authority to deny recognition to individuals as ecclesiastical endorsers while also ensuring the ability of military members to exercise freedom of religion. Although this policy is appropriate, the Department will review and update existing policy to ensure effective implementation, including periodic reviews of religious organizations seeking to endorse religious ministry professionals as military chaplains.

- *The Under Secretary of the Defense for Personnel and Readiness will review DoDI 1304.28 to ensure it includes effective implementation procedures, and update the instruction as appropriate by September 2010.*

Recommendation 2.4: Establish Rigorous Procedures for Investigating Foreign National DoD Personnel

The Independent Review found that a number of populations presently granted physical access to DoD facilities overseas require some form of vetting for repeated access. Some notionally vetted populations have incomplete records, and large numbers of people with access to DoD facilities are not vetted at all under current procedures.

DoD's ability to investigate foreign national DoD employees who live outside of the U.S. and require access to DoD facilities is limited by available resources and agreements with the host nation. DoD is only able to conduct the FBI name check, fingerprint check, and a check of the known and suspected terrorist databases. The Government Accountability Office (GAO) Report 09-351, *Contingency Contract Management*, highlights issues in complying with DoD 5200.2-R (*Personnel Security Program*). Additionally, compliance with Homeland Security Presidential Directive 12 requires background investigations for foreign national hires, or the equivalent host nation review, for access to DoD installations.

- **Future Action to Investigate Foreign National Employees:** By September 2010, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), in collaboration with the Under Secretary of Defense for Intelligence (USD(I)), the Under Secretary of Defense for Policy (USD(P)), and the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) will comply with existing relevant policy issuances (DoD 5200.2-R, DTM 08-003, and DTM 06-006) by developing relevant programs or identifying policy issues for discussion and implementation. USD (AT&L), as the lead to develop a response to GAO Report 09-351, will provide a summary of possible improvements not later than December 2010. By February 2011, USD(I), USD (P&R), and USD (AT&L) will revise applicable policy issuances to reflect the agreed-upon process and improvements. The Fort Hood Follow-on Review Senior Steering Group will monitor responses and require reports in consultation with the DoD Inspector General.

Recommendation 2.5 a-c: Review Pre- and Post-Behavioral Screening

The Independent Review found that the policies and procedures governing assessment for pre- and post-deployment medical risks do not provide a comprehensive assessment of violence indicators. There is no global violence risk assessment performed during pre-deployment for service members not currently receiving healthcare.

Current post-deployment assessments rely primarily on self-report screening questionnaires to identify risk factors for post-traumatic stress, traumatic brain injury, substance abuse, depression, and suicide. These screening questionnaires often ask just one question to assess whether a service member has serious conflict with others.. A follow-up provider interview directs medical providers to conduct a risk assessment by asking whether members are considering harm to self or others. However, the assessments do not address all risk factors (e.g., financial, occupational) thought to be associated with the potential for violence. Research-based screening questions do not exist and there is no current ability to reliably predict violence or a proclivity towards radicalization.

- **Future Action to Improve Behavioral Screening:** The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) will conduct several studies to inform pre- and post-deployment assessments and refine DoD behavioral indicators ("Step 2" of Recommendation 2.1). Additionally, USD(P&R) reviewed scientific literature and conducted interviews with subject matter experts to identify indicators for measuring an individual's potential for future violence and to determine whether an evidence-based comprehensive risk assessment system exists. Based on the literature review, which was completed in June 2010, USD(P&R) will adjust the policy guidance for serial mental health assessments required by the National Defense Authorization Act 2010, to include an additional service member question relating

to factors that have been correlated with violence (i.e., work, home, financial, legal, and interpersonal stressors). In addition, the guidance for health care providers will include detailed follow-up questions for the assessment of violence risk and indications for referral.

- The final policy for implementing mental health assessments will be issued no later than August 2010; the final guidance for training and certifying providers to do the assessments will be issued no later than September 2010. USD(P&R) is also developing partnerships with organizations with expertise in risk management to determine any lessons that may apply to DoD.

Recommendation 2.5.d: Review Policies Governing Sharing Health Care Assessments with Commanders

The Independent Review found that appropriate commanders, supervisors, and other authorities do not always receive information about individuals who may commit violent acts because they may not have sufficient access to health care assessments. A significant body of policies already exists within DoD to ensure that commanders and supervisors do receive appropriate health care-related information about their subordinates. However, these policies are spread across multiple regulations, memoranda, and instructions. A number of these policies have not been reviewed in more than 10 years and may need to be updated.

- *The Under Secretary of Defense for Personnel and Readiness will review existing policies and guidance to evaluate their content, and update them as necessary by September 2010.*

Recommendation 2.6 a, b: Update Policies to Address Workplace Violence

The Independent Review found that the Services have programs and policies to address prevention and intervention for suicide, sexual assault, and family violence, but guidance concerning workplace violence and the potential for self-radicalization is insufficient. These programs may serve as useful resources for developing more comprehensive workplace violence prevention—including the potential for self-radicalization. Useful resources for violence prevention education and training also exist in other federal agencies but are dated and not integrated into DoD policies, procedures, or processes.

- **Future Action to Address Workplace Violence:** The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) will develop DoD policy and guidance on the prevention of workplace violence by January 2011. USD(P&R) will incorporate training on prevention of workplace violence into the Civilian Personnel Management Services' Managerial and Supervisory Training Framework in accordance with the requirements of the National Defense Authorization Act FY2010 Section 1113.

Recommendation 2.7: Update Policy to Clarify Guidelines for Religious Accommodation

The Independent Review found that DoD policy regarding religious accommodation lacks the clarity necessary to help commanders distinguish appropriate religious practices from those that might indicate a potential for violence or self-radicalization. DoDI 1300.17 (*Accommodation of Religious Practices within the Military Services*) outlines the terms upon which religious

accommodations should be granted, but it does not provide standards or record keeping procedures necessary to establish a baseline of traditional religious practice within faith groups. Therefore, Services have different policies and procedures for handling religious accommodation requests. Further, DoD has not issued clear guidance on the degree to which the Religious Freedom Restoration Act (RFRA) applies to the military. The Independent Review recommended the Department promptly establish standards and reporting procedures that clarify guidelines for religious accommodation.

- **Future Action to Establish Standards and Clarify Guidelines for Religious Accommodations:** The Independent Review raised an important, long-standing concern and the Department agrees there is a need for consistent and overarching policy to standardize the religious accommodation approval process. The Undersecretary of Defense for Personnel and Readiness will work with the Services to examine this issue in more detail and, when appropriate, will provide a recommendation to the Secretary.

Recommendation 2.8: Provide Guidance for Counterintelligence Awareness

The Independent Review found that DoDI 5240.6 (Counterintelligence (CI) Awareness, Briefing, and Reporting Programs) provides guidance to conduct defense CI and counter-terrorism awareness briefings to DoD personnel, but does not thoroughly address emerging threats, including self-radicalization, which may contribute to an individual's potential to commit violence.

- *By September 2010, the Under Secretary of Defense for Intelligence will begin formal coordination of DoDI 5240.6, updated with a list of potential behavioral indicators with a nexus to international terrorism and language directing CI entities to disseminate other reported behaviors to command authorities and/or to law enforcement agencies. By September 2010, the Under Secretary of Defense for Policy will work with the Defense Science Board to undertake a multi-disciplinary study to identify behavioral indicators of violence and self-radicalization and update DoDD 2000.12 (DoD Antiterrorism (AT) Program), DoDO 2000.12-H (DoD Antiterrorism Handbook), and DoDI 2000.16 (DoD Antiterrorism (AT) Standards) as appropriate.*

Recommendation 2.9 a, b: Update Policies to Ensure Commander and Supervisor Access to Information in Personnel Records

The Independent Review found that neither DoD nor Service guidance provides for the maintenance and transfer of all relevant information about service members' conduct throughout their careers. At present, only performance evaluations (the Official Military Personnel Folder (OMPF)) and medical records follow service members across all assignments. DoDI 1336.08 (*Military Human Resource Records Life Cycle Management*) governs the type of records to retain and DoDI 6040.43 (*Custody and Control of Outpatient Medical Records*) requires that all treatment records be maintained for medical, legal, and administration reasons. Gaining commanders and supervisors would benefit from additional visibility into service members' behavior, especially that which may undermine good order and discipline or indicate a potential insider threat to DoD and its personnel.

In March 2010, the Human Resources Management Community of Interest established the Military Personnel Records Information Management Task Force (MPRIMTF) to examine the need to maintain and share additional information in personnel records. In May 2010, MPRIMTF completed its review and concluded that no additional information should be added to the OMPF. Although the MPRIMTF found that the OMPF is not the appropriate vehicle to maintain and share additional information, the Task Force does affirm that the Department must ensure commanders have more visibility into service members' behavior.

Future Action to Ensure Access to Information in Personnel Records: The Secretary of Defense will issue a memorandum to the Chiefs of the Military Services, directing them to determine procedures for appropriate documentation of behaviors detrimental to good order and discipline, particularly those that could be associated with violence, prohibited activities, and potential harm to self or others. The procedures should increase engagement of unit commanders and supervisors to prevent potential acts of violence and ensure timely and appropriate support for military personnel in need. These new procedures must be consistent with the Privacy Act and DoDD 5400.11 (*DoD Privacy Program*). Service Chiefs are requested to inform the Secretary of their proposal within 30 days.

Recommendation 2.10: Establishment of Consolidated Law Enforcement Database

The Independent Review recommended establishing a consolidated database to enable organizations across the Department to query, retrieve, and post criminal investigation and law enforcement data in a single repository. In August 2008, the Secretary of Defense directed that the existing Naval Criminal Investigative Service system be used as the basis for establishing a consolidated Law Enforcement Defense Data Exchange (D-DEx). Each of DoD's thirteen law enforcement agencies are *participating in the development of D-DEx.*

- *The Under Secretary of Defense for Personnel and Readiness, in coordination with the Military Departments and other Defense Law Enforcement Agencies, will complete development of D-DEx and identify program funds to deploy D-DEx DoD-wide in FY2011.*

Recommendation 2.11: Establish Formal Information Sharing Agreements with Partner Agencies

The Independent Review found that existing DoD guidance on establishing information sharing agreements with Federal, State, and local law enforcement and criminal investigation organizations does not mandate action or provide clear standards. The Independent Review recommended the Department require the Military Departments and Defense Agencies to establish formal information sharing agreements with allied and partner agencies; Federal, State, and local law enforcement; and criminal investigation agencies, with clearly established standards regarding scope and timeliness. The report noted that a lack of information sharing with partners reduces commanders' and supervisors' visibility into service members' conduct off-installation and renders them less able to identify and respond to potential insider threats.

The Follow-On Review found that not all information sharing relationships will be improved through formal agreements. At the local and international level, current information sharing policies and procedures are adequate. Attempts to formalize these information sharing relationships will be counterproductive, since this approach would convey a lack of trust and

reduce partners' incentives to cooperate by increasing their administrative and legal burdens. Therefore, the Follow-On Review found that the Department could benefit from formal agreements for a limited set of force protection threat information sharing relationships.

- **Future Action to Strengthen Information Sharing with Partners:** By September 2011, the Follow-On Review Senior Steering Group will appoint a lead agency to develop DoD guidance requiring formal agreements with: (a) U.S. Federal Department or Agencies, or any subsidiary organization; (b) Office of the Director of National Intelligence or any subsidiary organization; and (c) U.S. State, Territorial, or Tribal governments.

Recommendation 2.12: Update Policies on the Release of Protected Health Information

The Independent Review found that Service policies governing release of protected health information do not reflect current DoD-level guidance. Release of protected health information in DoD is governed by Privacy Regulations issued under the Health Insurance Portability and Accountability Act, which balances confidentiality with the need to ensure operational readiness and is reflected in DoD- and Service-level policy. DoD has recently provided interim guidance that indicates the circumstances under which it is appropriate and required for a healthcare provider to release protected health information to commanders. However, not all current Service-level guidance has been updated to reflect the most recent DoD policy.

- **Future Action on Protected Health Information:** The Under Secretary of Defense for Personnel and Readiness will direct the Secretaries of the Military Departments to review existing policies and guidance and update them as necessary to reflect DoD policy on the release of protected health information by September 2010. The Services will ensure that updated policy reflects the anti-stigma DoDI to be placed into coordination by September 2010, currently under conversion from DTM 09-006 (*Revising Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Military Personnel*).

Recommendation 2.13: Adopt Policies to Ensure Timely Dissemination of Violence Risk Assessments from Civilian Health Professionals to Military Personnel

The Independent Review found that current policy does not require civilian health professionals who provide care to service members to notify military health treatment facilities or commanders of indicators of violence that are identified during treatment. This gap in visibility prevents military medical providers, commanders, and supervisors from assisting the service member or intervening until the risk indicators result in observable behaviors that trigger concern.

- **Future Action to Disseminate Violence Risk Assessments:** The Under Secretary of Defense for Personnel and Readiness will review policies and procedures to ensure that appropriate information (i.e., information on a service member's threat of harm to self or others, or a diagnosis that involves treatment requiring duty limitations) from civilian providers to whom service members have been referred from the Military Health System may be provided to commands and military medical personnel. Appropriate policy guidance to Services will be drafted and placed into coordination by September 2010.

Recommendation 2.14: Publish Cyberspace Policy for Identifying Potential Threats to DoD Personnel, Information, and Facilities

The Independent Review found that the Department does not have a comprehensive and interagency-coordinated cyberspace counterintelligence (CI) activities policy. DoD has started drafting DoDI 5240.mm to address this shortfall. This interagency coordinated policy will provide comprehensive guidance for CI activities in cyberspace to all Military Departments and Defense Agencies. This policy will not address law enforcement activities but will compel defense CI components to alert DoD investigative organizations of non-foreign intelligence threat information discovered during authorized CI activity.

- *The Under Secretary of Defense for Intelligence in coordination with all interagency partners will publish DoDI 5240.mm by August 2010 to ensure DoD CI activities in cyberspace effectively counter espionage and support force protection.*

Recommendation 2.15: Prohibited Activities

The Independent Review found that DoD policy governing prohibited activities is unclear and does not provide commanders and supervisors the guidance and authority to act on potential threats to good order and discipline. DoD policy on prohibited activities is limited and only addresses active participation in groups that may pose threats to good order and discipline. Current DoD policy on prohibited activities appropriately balances personal expression against actions that undermine good order and discipline. DoDI 1325.06 (Handling Dissident And Protest Activities Among Members of the Armed Forces) and Article 134, Uniform Code of Military Justice, define actions that are detrimental to good order and discipline and empowers commanders to act in these instance. However, further clarification is necessary to illustrate more effectively what constitutes associational, advocating, supremacist and extremist behavior.

- *The Under Secretary of the Defense for Personnel and Readiness will review DoDI 1325.06 to ensure guidance is actionable and to provide behavior examples, guidance on how to respond to uncertain situations, and update the instruction as appropriate by September 2010.*

Recommendation 2.16: Assess Commanders' Need for Additional Authorities to Identify Indicators of Potential Violence in Civilian Personnel More Effectively

The Independent Review found that authorities governing civilian personnel are insufficient to support commanders and supervisors as they attempt to identify indicators of violence or take actions to prevent violence.

The Follow-on Review found that any attempt to grant commanders and supervisors greater authorities would not be consistent with the employee's civil rights and liberties. However, the Follow-on Review also found that more could be done to provide training on the prevention of workplace violence, and to enhance supervisors' and managers' visibility into the authorities available to them to address workplace behavioral issues with regard to civilian personnel.

- **Future Action on Identifying Indicators of Violence in Civilian Personnel:** The Under Secretary of Defense for Personnel and Readiness will work with civilian Employee Relation Component representatives to develop a DoD policy on prevention of workplace violence.

Civilian supervisor training will be promulgated as part of the revision of DoDI 1400.25, Volume 412 (*Civilian Leader Development*) by January 2011.

Recommendation 3.1 a-c: Improving Force Protection Policy

The Independent Review found DoD lacks a senior official assigned overall responsibility for oversight and integration of force protection policy across the Department. Instead, several different Senior DoD officials are responsible for issuing policy in force protection-related subject areas. Additionally, there is a lack of clarity regarding the force protection roles and responsibilities between Geographic Combatant Commanders and the Military Departments, especially in the United States. Finally, clarity on command and control responsibility for force protection is essential for a rapid response to multiple near simultaneous events similar to the Fort Hood incident.

During the analysis by the Follow-On Review, an additional finding was identified. DoD has a long-standing lack of a senior official responsible for overall oversight and integration of law enforcement activities. Force protection and law enforcement activities are overlapping. To the extent that the Department needs better force protection integration, DoD also needs better integration of law enforcement.

- **Future Action to Integrate Force Protection Policy:** The integration of force protection policy and law enforcement policy across the Department urgently requires a more senior level oversight structure than what currently exists. However, the current programs and policy offices are so diverse that assigning a single senior official would require a major restructuring within the Department. Therefore, the Senior Steering Group of the Follow-On Review chaired by ASD(HD&ASA) will assume an additional and separate duty as a standing departmental body to meet not less than biannually to address Department-wide policy synchronization and integration issues related to force protection and law enforcement activities. This force protection and law enforcement steering group will report to the Deputy Secretary of Defense Advisory Working Group following each meeting.
- **Future Action to Clarify Service and Combatant Commander Roles for Force Protection:** The Secretary of Defense will issue a guidance memorandum to DoD Components clarifying the force protection responsibilities and authorities of the Geographic Combatant Commanders and other heads of DoD Components. The memorandum will emphasize the need for Military Departments' compliance with force protection reporting requirements to the appropriate Combatant Commander.

Recommendation 3.2 a-c: Integrate Force Protection Efforts against Internal Threats

The Independent Review found DoD force protection programs and policies are not focused on internal threats. Recommendations included: develop policy and procedures to defend against insider threats, commission a multidiscipline study to examine and evaluate threat assessment programs, and provide commanders with a multidiscipline capability focused on predicting and preventing insider attacks.

- **Future Action to Integrate Force Protection Efforts:** The Under Secretary of Defense for Acquisition, Technology, and Logistics will commission the Defense Science Board (DSB)

to examine and evaluate existing training, procedures, reporting requirements/mechanisms, threat assessment programs, and best practices for identifying predictive indicators of pending violence and managing emerging insider threats. The Defense Science Board will complete its study by March 2011. The Fort Hood Follow-on Review Senior Steering Group will appoint a lead agency to draw on these findings to develop policy and procedures to improve and integrate DoD programs to defend resources and personnel against internal threats. The Under Secretary of Defense for Personnel and Readiness will incorporate the DSB findings and tools developed under recommendations 2.9, 2.12, and 2.13 to provide a multidiscipline approach against insider threats for commanders.

Recommendation 3.3 (a, b, c): DoD Joint Terrorism Task Force Participation

The Independent Review found that DoD's commitment to Joint Terrorism Task Forces (JTTFs) is inadequate. Issues include the lack of a single agency appointed to lead DoD's efforts in JTTFs, inconsistent memoranda of understanding between FBI and DoD that govern activities of the Department and DoD Agencies, and a possible under commitment or misalignment of DoD resources supporting JTTFs.

- *The Under Secretary of Defense for Policy (USD(P)) will serve as the DoD lead for oversight, providing policy guidance and developing DoD-wide goals and objectives for JTFFs collaboration. By September 2011, USD(P) will begin drafting and coordinating one consolidated Memorandum of Understanding (MOU) between the FBI and DoD, including the DoD Inspector General's Defense Criminal Investigative Service, to clarify responsibilities and ensure consistency among all agencies. This JTTF MOU will be developed within the context of a January 2009, White House-directed, Under Secretary of Defense for Intelligence (USD(I))-drafted, Information Sharing MOU between DoD and FBI (staffing began in June 2010). Finally, USD(P) will review personnel and data from a resource study provided by the USD(I) to ensure the commitment of resources to JTTFs meets DoD requirements. Resource and organizational requirements, including requests for additional manpower, will be determined no later than October 2010, and the realignment plan, if required, will be completed by October 2012.*

Recommendation 3.4: Develop Guidance on Force Protection Threat Information Sharing

The Independent Review found DoD lacks guidance standardizing how to share Force Protection (FP) threat information across the Services or the Combatant Commands. The Independent Review recommended standardizing guidance regarding how military criminal investigative organizations and counterintelligence organizations will inform the operational chain of command.

To ensure the development of coherent policies spanning intelligence, counterintelligence, law enforcement, and investigative jurisdictions, the Under Secretary of Defense for Policy (USD(P)) is given a more proactive role in this area.

- **Future Action on Force Protection Information Sharing:** USD(P) will direct the development of standard guidance regarding how Defense Criminal Investigative Organizations, Counterintelligence Organizations, and Intelligence Organizations will inform

the operational chain of command as well as keep the Joint Intelligence Task Force for Combating Terrorism (JITF-CT) and Services informed.

- By October 2010, the Under Secretary of Defense for Intelligence (USD(I)) will designate JITF-CT as the lead for facilitating selective access to foreign-connected terrorism-related information to designated organizations.
- By May 2011, USD(P), in coordination with USD(I) and the Assistant to the Secretary of Defense for Intelligence Oversight, will establish FP threat information dissemination policy and procedures for Defense intelligence collection, counterintelligence, and criminal investigative organizations in response to Combatant Commander, Service, and Defense intelligence analytical agencies' requirements.
- By November 2011, DoD Antiterrorism, FP, counterintelligence, intelligence, and law enforcement components will begin reviewing and updating policies, procedures, and training to comply with the new USD(P) policies.

Recommendation 3.5.a: Adopt a Common Force Protection Threat Reporting System

The Independent Review found that DoD did not have direct access to a force protection threat reporting system for suspicious incident activity reports. DoD agrees with this finding. In an August 2007 memo, the Deputy Secretary directed termination of DoD's only Force Protection Threat Information (FPTI) Reporting system, which was called the Threat and Location Observation Notice (TALON) reporting system. He further directed the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs to propose a long-term solution for DoD suspicious activity reporting that ensures appropriate privacy protection.

- *After two years of analysis and a successful pilot program completed in June 2009, the Department has selected the Federal Bureau of Investigation's (FBI) eGuardian system for DoD unclassified threat reporting. The eGuardian system, which is FBI-owned and maintained, provides an unclassified, secure web-based, capability to report suspicious activity and will contribute to our overall force protection threat information structure. The eGuardian system will appropriately safeguard civil liberties, while enabling information sharing among Federal, State, local, and tribal law enforcement partners, including interagency fusion centers.*
- *The Under Secretary of Defense for Policy is establishing a plan and will issue policy and procedures for the implementation of the eGuardian system as DoD's unclassified suspicious activity reporting system. Use of eGuardian will begin no later than September 2010.*

Recommendation 3.5 b: Adopt a Common Force Protection Threat Reporting System

The Independent Review found that DoD lacks direct access to a force protection reporting system for suspicious activity reports. Recommendations included adopting a common force protection threat reporting system and appointing a single Executive Agent to oversee and manage the system.

The April 12, 2010 Interim Report addressed the first recommendation. This recommendation was implemented in May 2010, with the approval of using the eGuardian system. The

eGuardian system, which is FBI-owned and maintained, will incorporate appropriate safeguards for civil liberties, while enabling information sharing among Federal, State, local, and tribal law enforcement partners, including interagency fusion centers. DoD will begin using the eGuardian system no later than September 2010.

- **Future Action to Ensure Common Threat Reporting:** The Under Secretary of Defense for Policy (USD(P)) will recommend the appropriate management arrangement (e.g., Executive Agent or Lead Component) to the Deputy Secretary of Defense to implement and manage the Department's use of the eGuardian system by November 2010. USD(P) will incorporate those requirements within the final issuance governing *Law Enforcement Reporting of Suspicious Activity* by December 2010.

Recommendation 3.6: Create a Process for Sharing Real-Time Force Protection Event Information Among Installations

The Independent Review found that there are no force protection processes or procedures to share unclassified real-time event information among commands, installations, and components. In November 2009, Fort Hood, Texas went to Force Protection Condition (FPCON) Delta. There were no indications that the rest of the Continental United States DoD forces were immediately notified of the event. Most installations found out about the event through the news media. Events that are happening within one Area of Responsibility (AOR) should inform force protection decisions in another. The requirement for a process/system to share event information in near real-time is key for alerting the force that an attack is underway.

- **Future Action to Enable Real-Time Force Protection Information Sharing:** This recommendation is also being covered by new Secretary of Defense guidance to the Military Services and to Combatant Commanders under Recommendation 3.1. Additionally, the Joint Staff (JS) will evaluate the current incident reporting systems used by the National Military Command Center (NMCC) and update Chairman Joint Chiefs of Staff Manual (CJCSM) 3150.03C (*Joint Reporting Structure Event and Incident Reports*) or other appropriate CJCSM no later than April 2011. By January 2011, the Services will ensure that all organizations are trained in reporting systems used by the NMCC. By April 2011, Combatant Commands will ensure there is an unclassified means to notify all DoD facilities within their AOR of an FPCON change.

Recommendation 3.7 a, b: Review and Update Access Control Protocols to Detect Insider Threats

The Independent Review found that DoD installation access control systems and processes do not incorporate behavioral screening strategies and capabilities, and are not configured to detect an insider threat. DoD policy mandates 100-percent credentials inspection for access to DoD installations. A properly credentialed person has authorized access to an installation. Detecting a trusted insider's intention to commit a violent act requires observation of behavioral cues/anomalies. There are Federal programs that train personnel to observe individuals under routine conditions. These programs may be useful if employed by DoD security guards, police officers, supervisory personnel, and persons working in visitor control centers, or other common customer service contexts.

- **Future Action to Update Access Control Protocols:** DoD began reviewing best practices, technologies, procedures, and programs through the Physical Security Equipment Action Group-Defense Installation Access Control working group under the Deputy Assistant to the Secretary of Defense for Nuclear Matters. A feasibility analysis study on how behavior pattern recognition screening procedures and technology can detect anomalies of a potential insider threat will be completed by October 2010. The Office of the Under Secretary of Defense for Intelligence will review and assess the study findings by January 2011, and revise or develop policy guidance related to DoD 5200.08-R (*Physical Security Program*) or other DoD policies as appropriate by December 2011.

Recommendation 3.8: Review the Need for a DoD Privately Owned Weapons Policy

The Independent Review found that the Department does not have a policy governing Privately Owned Weapons. In the absence of such policy, the individual Services have established Privately Owned Weapons policies, which set minimum standards and task installation commanders to establish installation-specific requirements. These policies do not apply to personnel who live off installation.

- *The Under Secretary of Defense for Intelligence put into formal coordination a Secretary-issued Department-wide Interim Guidance Message. By early 2011, the interim guidance will be incorporated into a revision of DoD 5200.08-R (Physical Security Program).*

Recommendation 3.9 a-c: Develop Information Sharing Capabilities for Access Control to Installations

The Independent Review also found that the Services cannot share information on personnel and vehicles registered on installations, installation debarment lists, and other relevant information required to screen personnel and vehicles, and grant access. The Services do not have access to the National Crime Information Center (NCIC) or Terrorist Screening Database (TSDB) to obtain relevant information to screen visitors. The review also identified that automated systems should be able to authenticate against centralized authoritative databases on registered persons and share access control information among installations. This recommendation supports on-going efforts to survey installation and mission requirements and to coordinate and prioritize the use of automation to mitigate risk and threat.

- **Future Action to Share Information for Access Control:** Under existing DoD issuances, services are implementing automated access control capabilities that will enable authentication of various identification media against authoritative databases. Services will accelerate implementation of automated access control systems within resources constraints. Areas of acceleration may include, but are not limited to, improvements in enterprise architecture and technology associated with Physical Access Control System (PACS), improved access to law enforcement databases such as the NCIC or TSDB, and capabilities that enable information sharing across the DoD enterprise. A current Under Secretary of Defense for Intelligence (USD(I))-sponsored study of existing physical access control system capabilities and limitations, and a joint DOJ-DoD NCIC access test, will be completed by January 2011. USD(I) will evaluate and update physical security policy and issuances by December 2011.

Recommendation 4.1 a: Establish Milestones for Compliance with the Installation Emergency Management Program

The Independent Review found that the Military Departments are not fully interoperable with all military and civilian emergency management stakeholders. Additionally, some DoD installations have not implemented procedures that are consistent with the National Incident Management System (NIMS). DoD has instructed the Military Departments to develop Initial Operational Capability (IOC) by January 13, 2011, and to have Full Operational Capability (FOC) by January 13, 2014, for NIMS-consistent procedures. However, DoD guidance was unclear on what constitutes IOC and FOC consistency.

- *The Under Secretary of Defense for Acquisition, Technology and Logistics has issued interim guidance on tasks required for IOC and FOC, and initiated formal coordination of DoDI 6055.17 (DoD Installation Emergency Management Program).*

Recommendation 4.1 b: Assess the Potential for Accelerating the Timeline for Compliance with the Installation Emergency Management Program

The Independent Review found that Services are not fully interoperable with all military and civilian emergency management stakeholders. DoDI 6055.17 (*DoD Installation Emergency Management (IEM) Program*) directs the Services to adopt IEM programs consistent with the National Incident Management System (NIMS). The Under Secretary of Defense for Acquisition, Technology, and Logistics has instructed the Services to develop Initial Operational Capability (IOC) for IEM programs by January 2011 and Full Operational Capability (FOC) by January 2014.

To attain IOC and FOC, Services must implement a Common Operating Picture (COP) and Mass Notification and Warning Systems (MNWS). In addition, the Independent Review calls on Services to implement Enhanced 911 (E 911). The Independent Review recommends the Department assess the potential for accelerating the timeline for compliance with the IEM Program.

- **Future Action to Clarify Installation Emergency Management Program Requirements:** In June 2010, the Under Secretary of Defense for Acquisition, Technology, and Logistics initiated formal coordination of DODI 6055.17 (*DoD Installation Emergency Management (IEM) Program*) to clarify requirements for E 911, MNWS, and COP.
- **Future Action to Implement Installation Emergency Management Programs:** The Follow-On Review determined there is a need to implement certain IEM program elements as described below as soon as possible (see Recommendations 4.2, 4.4, and 4.5a).

Recommendation 4.2: Develop Policy to Implement Enhanced 911 Services

The Independent Review found that there is no DoD policy implementing public law requiring a 911 capability on DoD installations (Public Law 108-494, *Enhanced 911 Services*). The Independent Review recommended the Department develop policies that provide implementation guidance for Enhanced 911 (E 911) services. The two benefits of E 911 are that it automatically

notifies dispatchers of a caller's location, including cell phones, and that it has the capability to broadcast emergency notifications out to designated geographic locations. The two basic components of an E 911 capability are: (1) E 911 phone consoles that draw from a database that identifies caller location; and (2) trained dispatchers. Computer aided dispatcher systems contribute to a more sophisticated E 911 capability. Most civilian communities already have E 911 programs (funded through a national tax on phone services), but most DoD installations do not, because DoD installations were not part of the Congressionally mandated requirement.

- **Future Action to Implement Enhanced 911:** The Follow-On Review determined military personnel should receive the same emergency response services as their civilian counterparts. A DoD E 911 capability must be funded to meet Full Operational Capability (FOC), as outlined in DoDI 6055.17 (*DoD Installation Emergency Management (IEM) Program*), as soon as possible and no later than 2014. To meet FOC, E 911 systems should be commensurate with and supportable by E 911 systems in the surrounding local communities (or by comparable emergency notification systems in communities outside of North America). The Secretary places a high priority on this IEM program and directs the Services to work with Cost Analysis and Program Evaluation during the FY 2012-2016 Integrated Program/Budget Review to develop funding options to achieve FOC no later than 2014. Services should use the FY 2012-2016 Integrated Program/Budget Review process to determine how to prioritize and tailor IEM program implementation to maximize improvements to installation emergency preparedness using the minimum resources necessary, taking into account the unique requirements of installations of varying size and mission type.

Recommendation 4.3 a: Incorporate Law Enforcement Best Practices for Active Shooter Threat

The Independent Review found DoD does not currently take advantage of successful models for active shooter response for civilian and military law enforcement on DoD installations and facilities. More generally, the Department has no established process to identify and adopt quickly civilian law enforcement best practices. The Independent Review recommended the Department identify and incorporate civilian law enforcement best practices, including response to the active shooter threat, into training certifications for civilian police and security guards.

- **Future Action to Incorporate Best Practices:** In March 2010, DoD took several steps to specifically address the active shooter threat scenario. Moving forward, the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) will recast a joint Law Enforcement Training Standards Working Group to identify and incorporate a broad range of law enforcement best practices. By November 2010, USD(P&R) will update DoDI 5210.90 (*Minimum Training, Certification, And Physical Fitness Standards for Civilian Police and Security Guards (CP/SGs) In The Department of Defense)* or draft a new instruction accordingly.

Recommendation 4.3 (b, c, d): Develop Law Enforcement Practices for Active Shooter Threat

The Independent Review found that DoD policy does not currently take advantage of successful models for active shooter response, use the same minimum training standards for both civilian

and military law enforcement units on DoD installations, or incorporate Department of Homeland Security (DHS) best practices for workplace violence into DoD Antiterrorism Level 1 training. Responding officers at Fort Hood attributed their actions during the incident to a new active response training protocol instituted last year by the Fort Hood Department of Emergency Services.

Note: In March 2010, DoD incorporated a new training module addressing active shooter threats into the Antiterrorism Level 1 online training.

- *The Under Secretary of Defense for Acquisition Technology, & Logistics (USD(AT&L)) has updated and initiated formal coordination of DoDI 6055.17 (DoD Installation Emergency Management (IEM) Program). It directs commanders to incorporate the "Active Shooter" scenario, lessons learned from Fort Hood, and other workplace violence case studies into their Installation Emergency Management training programs. The Under Secretary of Defense for Personnel and Readiness has investigated the implementation of minimum standards for military police (and equivalents) and will draft a change to DoDI 5210.90 (Minimum Training, Certification, And Physical Fitness Standards For Civilian Policy And Security Guards (CP/SGs) In The Department Of Defense) or draft a new instruction by November 2010.*

Recommendation 4.4: Examine and Incorporate State-of-the-Art Mass Warning Systems into Emergency Response Plans

Based on Joint Staff Integrated Vulnerability Assessments, the Independent Review found that many DoD installations lack mass notification capabilities. The Independent Review recommended the Department examine the feasibility of advancing the procurement and deployment of state-of-the-art Mass Notification and Warning Systems (MNWS) and incorporate these technologies into emergency response plans. The purpose of MNWS is to provide warning and response direction for all personnel within 10 minutes of incident notification and verification. MNWS has four elements: (1) Giant Voice for outdoor areas; (2) Indoor Voice for indoor facilities; (3) Telephone Alert System for phone call/text alerts; and (4) Software Alert Systems for computer alerts. Depending on the installation, different combinations of components may be required to meet FOC for mass notification. All installations have some MNWS in place, but the systems are not robust. A state-of-the-art MNWS automates guidance (e.g., evacuation orders for certain areas) to help emergency responders manage a crisis.

- **Future Action to Implement Mass Notification Warning Systems:** The Follow-On Review determined there is a need to implement MNWS. Each Service should determine the combination of elements most appropriate to meet FOC requirements for mass notification. MNWS programs must be funded to meet Full Operational Capability (FOC), as outlined in DoDI 6055.17 (*DoD Installation Emergency Management (IEM) Program*), no later than 2014. To meet FOC, MNWS must notify all installation personnel within ten minutes of incident verification. The Secretary places a high priority on this IEM program and directs the Services to work with Cost Assessment and Program Evaluation during the FY 2012-2016 Integrated Program/Budget Review to develop funding options to achieve FOC no later than 2014. Services should use the FY 2012-2016 Integrated Program/Budget Review process to determine how to prioritize and tailor IEM program implementation to maximize improvements to installation emergency preparedness using the minimum resources

necessary, taking into account the unique requirements of installations of varying size and mission type.

Recommendation 4.5 a: Accelerate Deployment of Common Operating Picture Capability into Installation Emergency Operations Centers

The Independent Review found that Services have not widely deployed or integrated a Common Operating Picture (COP) capability into Installation Emergency Operations Centers (IEOCs) per direction from the Under Secretary of Defense for Acquisition, Technology, and Logistics. The Independent Review recommended the Department examine the feasibility of accelerating the deployment of state-of-the-art COP to support IEOCs. COP is a web-based software system and there are many commercially available software packages, such as Web-EOC and E-Team. COP enables coordination between emergency responders on- and off-installation, allowing them to share the exact same information in real time over the course of an incident. COP also improves installations' capacity to report force protection information to the Combatant Commands.

- **Future Action to Implement a Common Operating Picture:** The Follow-On Review determined installations require COP capability, particularly given its benefits to force protection and emergency management for a relatively low resource requirement. COP capability must be funded to meet Full Operational Capability (FOC), as outlined in DoDI 6055.17 (*Installation Emergency Management (IEM) Programs*) no later than 2014. To meet FOC, the COP capability must share real-time information among first responders. The Secretary places a high priority on this IEM program and directs the Services to work with Cost Analysis and Program Evaluation during the FY 2012-2016 Integrated Program/Budget Review to develop funding options to achieve FOC no later than 2014. Services should use the FY 2012-2016 Integrated Program/Budget Review process to determine how to prioritize and tailor IEM program implementation to maximize improvements to installation emergency preparedness using the minimum resources necessary, taking into account the unique requirements of installations of varying size and mission type.

Recommendation 4.5 b: Develop an Operational Approach that Sets Force Protection Condition Appropriately

The Independent Review recommended the Department develop an operational approach that raises the Force Protection Condition in response to a scenario appropriately and returns to normal while considering both the nature of the threat and the implications for force recovery and healthcare readiness in the aftermath of the incident.

- **Future Action to Set Force Protection Condition Appropriately:** The previous recommendation on creating a process for sharing real-time force protection event information among installations (3.6) addresses the development of an operational approach to raise Force Protection Condition. By April 2011, Combatant Commands will ensure there is an unclassified means to notify all DoD facilities within their AOR of an FPCON change.

Recommendation 4.6 a, b: Review and Establish Policies for Synchronizing Installation Emergency Management Procedures

The Independent Review found that DoD Installation Emergency Management (IEM) program stakeholders have not yet synchronized their applicable programs, policies, processes, and procedures. Better synchronization and coordination would remove redundant planning requirements, identify seams in policy, focus programmed resources, and streamline procedures to achieve unity of effort.

- **Future Action to Synchronize Installation Emergency Management:** The Follow-on Review developed a Policy Architecture Analysis. This Analysis recommended the Department publish a new Directive to synchronize IEM and related programs, policies, processes, and procedures across the Department. To address this recommendation, the Under Secretary of Defense for Policy has established a stakeholders working group, with the goal of placing draft synchronizing policy in coordination by January 2011.

Recommendation 4.7: Review Installation Emergency Management Programs to Ensure Appropriate Interaction with Mutual Aid Agreements

The Independent Review found that the Mutual Aid Agreements (MAAs) between DoD installations and civilian support agencies are not current and need to be updated. There is no overarching guidance regarding the maintenance, frequency of review, and tracking of MAAs. DoDI 6055.17 (DoD Installation Emergency Management Program) tasks installations to develop resource management objectives that address partnership agreements essential to Installation Emergency Management.

- *The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) has initiated formal coordination of DoDI 6055.17 to clarify oversight and exercise requirements, including annual reviews, integrating tracking, exercising, and inspections of MAAs.*

Recommendation 4.8.a: Develop Core Service Elements of a Family Assistance Center

The Independent Review found that lessons from the terrorist attacks in 2001 resulted in sufficient policy guidance for implementing day-to-day support programs and baseline family support services. However, the policy guidance has not been updated nor does it clearly delineate a specific structure for how these services integrate in support of a crisis or mass casualty incident. As a result, Military Department-level planning lacks consistency and specificity, which leads to variation in the delivery of victim and family care.

- *The Under Secretary of Defense for Personnel and Readiness reviewed the Pentagon 9/11 After Action Report and all applicable Military Department regulations, and identified best practices that will be incorporated into the draft revision of DoDI 1342.22 (Family Centers) by December 2010.*

Recommendation 4.8 b, c: Develop Core Service Elements of a Family Assistance Center

The Independent Review found that the Department of Defense has not produced guidance to develop family assistance plans for mass casualty and crisis response. As a result, Service-level planning lacks consistency and specificity, which leads to variation in the delivery of victim and family care.

- **Future Action to Develop Family Assistance Centers:** In June 2010, the Under Secretary of Defense for Acquisition, Technology, and Logistics initiated formal coordination of DoDI 6055.17 (*DoD Installation Emergency Management (IEM) Program*) to ensure Family Assistance Center crisis and mass casualty response plans become integral elements of the IEM program. The Family Assistance Center crisis and mass casualty response will "establish procedures to integrate victim and family services in response to the full spectrum of crisis or catastrophic events." The Under Secretary of Defense for Personnel and Readiness will review and identify Service best practices and revise DoDI 1342.22 (*Family Readiness Program*) to incorporate a best practices model for a family assistance center by December 2010.

Recommendation 4.9 (a, b): Ensure Religious Support in Mass Casualty Incidents

The Independent Review found no comprehensive instructions that address religious support, planning, or integration requirements in response to a mass casualty incident. This results in inconsistencies in Military Department policies on integrating religious support into emergency management, and could lead to inadequate planning and coordination for religious support resources.

- *The Under Secretary of Defense for Personnel and Readiness, with the advice and assistance of the Armed Forces Chaplains Board and the Armed Forces Chaplains Center, reviewed Military Department policies and civilian sector programs and identified best practices for religious support to mass casualty incidents. USD(P&R) will begin to update guidance for policy additions or revisions to applicable policy governing installation emergency management and response to disasters or incidents by September 2010.*

Recommendation 4.10: Review Mass Casualty Incident Response Training in the Chaplain Basic Officer Courses

The Independent Review found inconsistencies among Military Department entry-level chaplain training programs, which can result in inadequate religious support during a mass casualty incident. The newly established Armed Forces Chaplaincy Center (AFCC) is comprised of the Army, Navy, and Air Force Chaplain Schools. The Department will obtain advice from the AFCC and the Armed Forces Chaplains Board on an optimal manner of introducing mass casualty incident training into the basic course and/or other training opportunities for newly commissioned chaplains can develop enhance counseling and care skills consistent with their knowledge, skills, and abilities.

- *The Under Secretary of Defense for Personnel and Readiness has put into formal coordination DoDI 6055.17, which will require that new chaplains get mass casualty incident training at the earliest point.*

Recommendation 4.11: Develop Standardized Policy Guidance on Memorial Service Entitlements

The Independent Review found that DoD has not published guidance regarding memorial service travel and transportation benefits authorized for certain survivors of deceased service members enacted in section 631 of Public law 111-84, the national Defense Authorization Act for Fiscal Year 2010. DoD guidance is necessary to ensure this benefit is administered consistently throughout the Department.

- *The Under Secretary of Defense for Personnel and Readiness established interim guidance (DTM 10-008 – Travel and Transportation for Survivors of Deceased Members of the Uniformed Services to Attend Memorial Ceremonies) and will incorporate its content into the pending revision of DoDD 1300.22 (Mortuary Affairs Policy), which will be published as a new DoDI with the same title, Mortuary Affairs Policy, during calendar year 2010.*

Recommendation 4.12 a, b: Review Mortuary Affairs Policies for Application to Private Citizens within the Continental United States

The Independent Review found that DoD and Service casualty policies revealed no guidance, at any level, that was sufficient to address the full range of issues pertaining to private citizens who become casualties on a CONUS military installation. In the area of DoD and Service mortuary affairs policies, the review revealed a similar absence of guidance regarding mortuary entitlements and services.

- **Future Action to Update Mortuary Affairs Policies:** The Under Secretary of Defense for Personnel and Readiness will coordinate with the Defense Human Resource Activity Law Enforcement and the Office of the Assistant Secretary of Defense for Health Affairs to establish policy and draft guidance to revise DoDI 1300.18 *(Department of Defense (DoD) Personnel Casualty Matters, Policies and Procedures*), DoDI 1300.22 (*Mortuary Affairs Policy*), and other applicable issuances no later than September 2010.

Recommendation 5.1 a-c: Optimize Mental Healthcare for Domestic Mass Casualty Incident

The Independent Review found that DoD installations have not consistently planned for mental health support after domestic mass casualty incidents for victims and their families. Current DoD medical policy regarding combat stress does not specifically address an appropriate traumatic stress response in a domestic mass casualty incident. Several DoD programs and initiatives are currently working to address this shortcoming.

- **Future Action to Optimize Mental Healthcare:** The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) completed a review of existing policies, guidance, and evidence-based practices inside and outside of DoD, and, in June 2010, recommended

the development of a DoDI on post-disaster mental health response. USD(P&R) will draft and place into coordination interim guidance on disaster response strategies by December 2010.

Recommendations 5.2 (a, b, d): Create Policies to Measure Health Care Provider Readiness

The Independent Review found that the Department does not endorse a program encompassing all of the desired attributes of a health care provider readiness strategy. Although the Independent Review found the Department has evolving collaborations between DoD entities and civilian organizations to support health care providers, it suggested that DoD should further develop formal collaboration relationships with the civilian sector to share best practices and ongoing research outcomes.

Note: This finding is partially approved for parts "a" and "b" because the necessary policies to ensure health care provider readiness already exist. They are not, however, fully integrated and current.

- *The Under Secretary of Defense for Personnel and Readiness will review existing policies and guidance, establish a Directive-Type Memorandum related to civilian resiliency resources, and update and integrate policies as necessary by September 2010.*

Recommendation 5.2 c: Create Policies to Measure Health Care Provider Readiness

The Independent Review found that DoD does not have comprehensive policies that recognize, define, integrate, and synchronize monitoring and intervention efforts to assess and build health care provider readiness. DoD does not have readiness sustainment models, with requisite resources, for the health provider force that are similar to readiness sustainment models for combat and combat support forces.

The Follow-on Review found that DoD does have readiness sustainment models inclusive of health care providers. However, the demand for support from caregivers in general, and from mental health care providers in particular, is increasing and appears likely to continue to increase due to the stress on military personnel and their families from our high operational tempo and repeated assignments in combat areas.

- **Future Action to Assess and Build Health Care Provider Readiness:** In accordance with approved recommendations from the Follow-on Review's Interim Report, the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) is currently conducting a review of existing policies, guidance, and current initiatives/programs that specifically target health care providers, especially mental health providers, to evaluate their content, and will draft and place into coordination updates by September 2010. Based on the results of the review, by November 2010 USD(P&R) will also prepare the business case for additional mental health providers, specifying the number of providers needed as well as the resources required to reach that number of providers. In accordance with the business case, USD(P&R) will then develop new policies to assess and build health care provider readiness.

Recommendation 5.3 (a, c): Ensure Integrated Policies to Sustain High Quality Care and De-stigmatize Health Care Providers Who Seek Treatment

The Independent Review found that increasing demands on health care support will make it difficult to sustain high-quality care due to the high operational tempo and work-related stress on caregivers. The Department needs to develop a deployment model that provides sufficient recovery and sustainment for health care providers, and de-stigmatizes health care providers who seek treatment for stress. DoD also needs to integrate the existing body of policies, processes, procedures, and programs to ensure consistency and a comprehensive approach.

- *The Under Secretary of Defense for Personnel and Readiness will review and update existing policies and guidance, to ensure they are integrated and provide appropriate guidance to sustain high quality care, and complete the conversion of an anti-stigma DoDI based on DTM 09-006 (Revising Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Military Personnel), by September 2010.*

Recommendation 5.3 b: Ensure Integrated Policies to Sustain High Quality Care and De-stigmatize Health Care Providers Who Seek Treatment

The Independent Review found that the lack of a readiness sustainment model for the health provider force, the unique stressors that healthcare providers experience, and the increasing demand for support combine to undermine force readiness. The Independent Review recommended that DoD develop integrated policies, processes, procedures, and properly resourced programs to sustain high quality care.

The June 2007 Report of the DoD Task Force on Mental Health noted the importance of enhancing the resiliency and recovery of combatants due to the emotional pathology of combat. The Services have robust programs for pre- and post-deployment care for their members, but some have only recently initiated similar programs for healthcare providers. It is equally important to enhance the resilience and recovery of healthcare providers.

- **Future Action to Support Health Care Providers:** The Under Secretary of Defense for Personnel and Readiness developed a strategy to enhance resilience that addresses the total health and comprehensive well-being of healthcare providers. It accounts for various factors, including deployment length, post-deployment reconstitution, and dwell time, and assesses the advantages and disadvantages of using temporary providers to fill shortfalls. The strategy incorporates a new resilience model, which will be drafted and placed into coordination by September 2010.

Recommendation 5.4: Provide Mentor Relationships Among Healthcare Providers

The Independent Review found that senior caregivers are not consistently functioning as clinical peers and mentors to junior caregivers. It also raised concerns regarding the retention rate of experienced physicians. The Independent Review recommended a review of Senior Medical Corps officer requirements to determine optimal roles, utilization, and assignments.

The Follow-on Review found that current assignment processes in the Medical Departments of each Service are unique to the specific mission requirements of each Department, and are already responsive to those requirements.

- **Future Action to Improve Mentoring:** The Army, Navy, and Air Force will maintain the current assignment process developed by each Service, and expand them as they deem necessary to ensure that Senior Medical Officers are assigned to clinical positions.

Appendix B.
City of Virginia Beach Request for Proposals

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**
PLEASE FILL IN COMPANY NAME & ADDRESS IN THE SPACES PROVIDED BELOW: _____ _____ _____	**RETURN THIS COPY** ***THIS IS NOT AN ORDER***	CLOSING TIME **3:00 PM EST**
		PROCUREMENT OFFICER **Darla Smith**

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

I. Purpose 1

II. Background 1

III. Scope of Work 2

A. General Requirements 2

1. Project Knowledge 2
2. Offeror Vision of NG9-1-1 2
3. Single Point of Contact 3
4. Information Provided By the Offeror 3

B. Technical Requirements 3

1. Capacity 3
2. Standards 4
3. Network 5
4. Interconnection to Legacy Selective Routers 7
5. Interconnection to Other ESInets 8
6. Interoperability with State Police, Military Bases, and Other Federal Entities, Colleges and Universities 9
7. Data Centers 9
8. Security 11
9. Network Operations Center/Security Operations Center 13
10. NG9-1-1 Core Services Elements 20
11. Service Level Agreements 42
12. PSAP Interfaces and Backroom Equipment Requirements 47
13. Migration Plan Options 48
14. Project Management and Ongoing Client Management Services 49
15. Training 50
16. Service, Repair and Advance Replacement 51
17. Software Release Policy 51
18. Scheduled Releases 51
19. Maintenance Releases 52
20. Documentation 53

IV. General Terms and Conditions 53

A. Licensing, Support, and Maintenance PERIOD 53
B. Renewal 53
C. Termination with Cause/Default/Cancellation 54
D. Nondiscrimination 54
E. Drug Free Workplace 54
F. Faith Based Organizations 55
G. Compliance with Immigration Laws 55
H. Business Entity Registration 55
I. Compliance with All Laws 55
J. Venue 55
K. Agreement Interpreted under Laws of Virginia 55

L. Business License Requirement 55
M. Independent Contractor 55
N. Representation Regarding City Employment; Conflict of Interest: 56
O. Integration/Merger 56
P. Severability 56
Q. Waiver 56
R. Interpretation 56
S. Descriptive Headings 56
T. Non-appropriation 56
U. Assignment of Agreement 57
v Termination without Cause 57
w Hold Harmless/Indemnification 57
X Insurance 57
Y Notice 58
Z Offset/Setoff 58
AA. Audits 58
BB. Cooperative Procurement 59
CC. Submission and Disposition of Contractual Claims 59
DD. Payments to Subcontractors 59
EE. Subcontractors 60

V. Special Terms and Conditions 60

A. Payment Schedule 60
B. Modification 60
C. Company Personnel Standards 60
D. Claims for Extra Compensation 60
E. Copyright/Patent Indemnity 61
F. License 61
G. Warranty 62
H. Standards 62
I. Subcontractors 62
J. Project Team Members 62
K. Security 63
L. Product Documentation 64
M. Product Modifications 64
N. Product Training 64
O. Product Testing 64
P. Production Deployment 65
Q. Post Installation Support/Reliability Test Period 65
R. Final System Acceptance 65
S. Product On-going Support and Maintenance 66

VI. Special Instructions to the Offeror 66

A. Contract Administrator 66
B. Pre-Proposal Conference 66

VII. General Submittal Terms and COnditions 67

A. Definitions of Terms 67
B. Submittal of Proposals 67
C. Examination 67
D. Questions 67

E. Conditions of Work 68
F. Anticollusion/Nondiscrimination//Drug-Free Workplace Form 68
G. Subcontracting Participation Plan Form 68
H. Good-Faith Efforts – Certified Small, Woman, Minority, Service Disabled Veteran or Employment Services Organization 68
I. Proposal Binding for One Hundred Twenty (120) Days 68
J. Proprietary Information 68
K. Proposal Costs 69
L. Exceptions 69
M. Award 69
N. Fraud, Waste and/or Abuse 69
O. Public Notice of Award or Decision to Award 69
P. Preparation Guidelines 69
Q. Proposal Opening 72
R. Evaluation 73
S. Presentation/Demonstration 73
T. Negotiations 73
U. Submittal 73

Attachment A – City of Virginia Beach Government Organizational Structure 74

Attachment B – City of Virginia Beach Computing Environment and Information Technology Standards 75

Attachment C - City of Virginia Beach PSAPs with List of Preferred Interoperable Agencies 85

Attachment D - Specification Of Environment Hardware and System Software 87

Attachment E – Database Questionnaire 88

Attachment F – ESInet Services and Software Investment Summary 92

Attachment G – Confidentiality Agreement 95

Attachment H: Requirements Compliance Summary Matrix 96

List of Tables

Table 1. Third Party NOC/SOC Support 19
Table 2. ESRP Functional Requirements 31

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

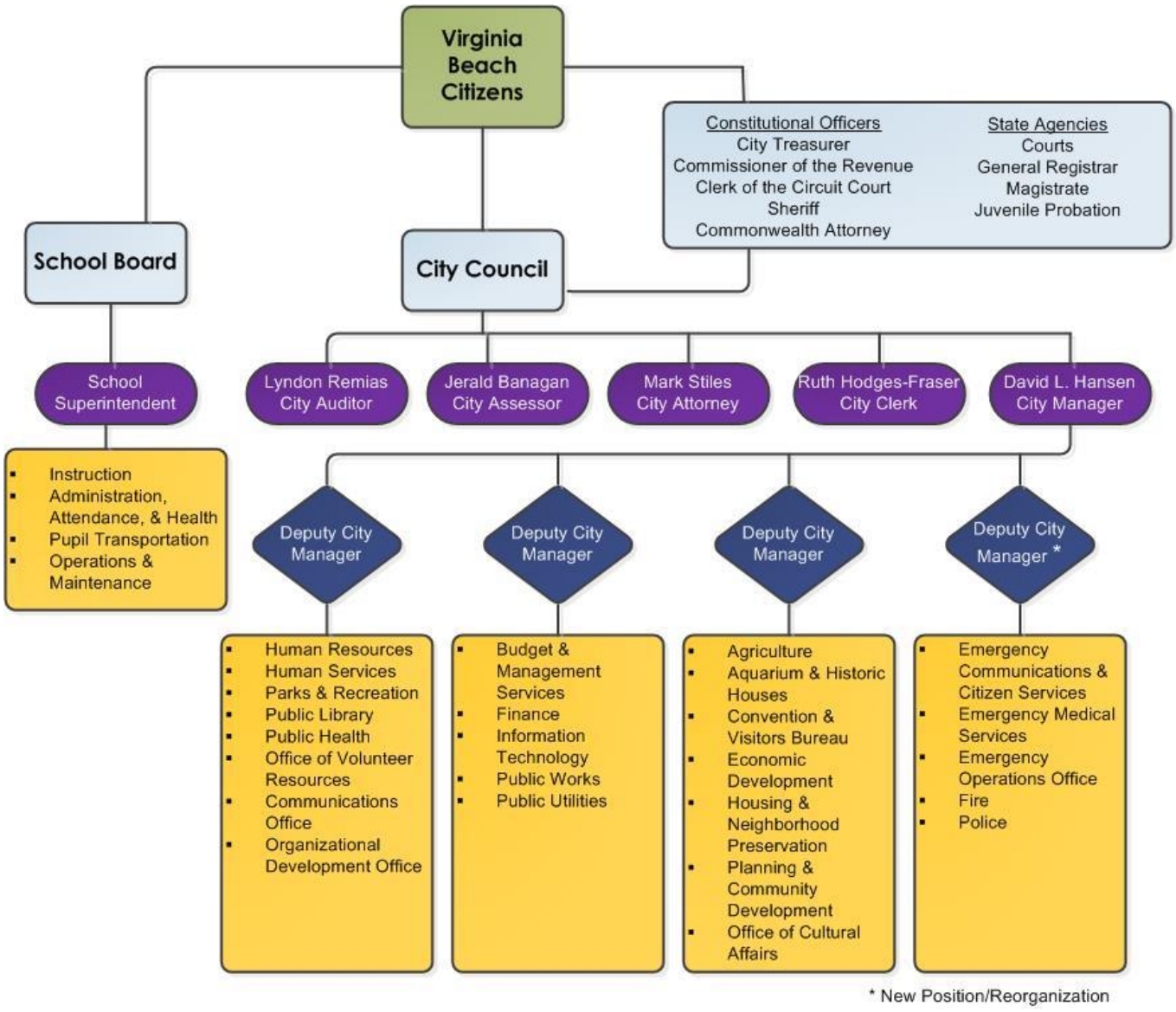
Negotiations shall then be conducted with each of the Offerors so selected. Price shall be considered, but need not be the sole determining factor. After negotiations have been conducted with each Offeror so selected, the City shall select the Offeror, which in its opinion, has made the best proposal, 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						

Appendix C.
Memorandum of Agreement Between Charleston County and Joint Base Charleston

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 [signature]
Michelle Buell

02-17-17

K Bustraan (Seal)
Keith Bustraan, County Administrator

DATE: 2/17/17

FOR JOINT BASE CHARLESTON:

WITNESSES

Vivica N. Bryant
Vivica N. Bryant

02-~~22~~ 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.

The information herein is For Official Use Only (FOUO) which must be protected under the Freedom of Information Act of 1966 and Privacy Act of 1974, as amended. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in criminal and-or civil penalties

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

Department of Defense

INSTRUCTION

NUMBER 6055.17
January 13, 2009
Incorporating Change 1, November 19, 2010

USD(AT&L)

SUBJECT: DoD Installation Emergency Management (IEM) Program

References: See Enclosure 1

1. PURPOSE. This Instruction, under the authority of DoD Directive (DoDD) 5134.01 (Reference (a)):

a. Establishes policy, assigns responsibilities, and prescribes procedures for developing, implementing, and sustaining IEM programs at DoD installations worldwide for "all hazards" as defined in the glossary.

b. Establishes the goals of the DoD IEM Program as follows:

(1) Prepare DoD installations for emergencies.

(2) Respond appropriately to protect personnel and save lives.

(3) Recover and restore operations after an emergency.

c. Aligns DoD emergency management (EM) activities with the National Incident Management System (NIMS), the National Preparedness Guidelines (NPG), and the National Response Framework (NRF) (References (b), (c), and (d)).

d. Establishes the DoD EM Steering Group (EMSG).

e. Authorizes other publications such as manuals to provide specific information on the DoD IEM Program.

2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other

(e) Crisis and mass casualty response that integrates religious support in response to the full spectrum of crisis or catastrophic events.

(f) Appropriate dynamic protocols to allow non-DoD first responders to access the installation in an emergency.

(5) Recovery planning that provides short-term and long-term priorities for restoration of functions, services, resources, facilities, programs, and infrastructure.

(6) Communications through all phases of an emergency that address communication capability and operation of major communication nodes ~~such as~~ *to include, but not be limited to,* dispatch centers, mobile command posts, *and* incident command*s* ~~vehicles and services with recording capability for each installation either direct support (government owned and operated) or in general support from another organization off installation~~.

c. IEM Plan Structure. The IEM Plan structure should be written to address the three phases of incident management per the NRF: prepare, respond, and recover. The annexes should address the hazards that threaten the installation.

5. ENHANCED 911. All installations shall have:

a. The availability of enhanced 911 services with recording capability at domestic installations through either direct support (Government-owned and -operated) or support from State and local authorities off the installation.

b. Requirements to subscribe for enhanced 911 services for Voice-Over Internet Protocol users and emergency dispatch capabilities for nondomestic installations.

Appendix
Hazard Identification List

awareness level. The ability to recognize that an incident is occurring and to initiate an emergency response sequence by notifying proper authorities. Awareness level requires no further action beyond notifying the authorities.

capability assessment. A DoD, command, or unit-level evaluation (assessment) to identify capabilities for responding to a natural or manmade disaster or hazard.

casualty management. A process by which coherent and interrelated sets of procedures, policies, and plans are developed in order to optimize the baseline capability to deal with patient populations expected in a mass casualty incident. Effective casualty management includes the efficiency to increase capacity during the response to a mass casualty incident.

common operating picture. A continuously updated overview of an incident compiled throughout an incident's life cycle from *standard data (meaning standard data elements, definitions, etc.) shared between integrated and compatible* systems *(meaning systems that can talk to each other)* for communication, information management, and intelligence and information sharing. The common operating picture ~~allows incident managers at all levels to make effective, consistent, and timely decisions~~ *facilitates collaborative planning and assists all echelons to achieve situational awareness*. The common operating picture ~~also helps ensure~~ *provides* consistency at all levels of incident management across jurisdictions, as well as between various governmental jurisdictions and private-sector and nongovernmental entities ~~that are engaged~~.

consequence management. As defined in Reference (~~aq~~*ar*).

continuity of operations. As defined in Reference (~~aq~~*ar*).

criticality assessment. As defined in Reference (~~aq~~*ar*).

critical personnel. Personnel deemed necessary for ensuring that a military mission identified as being "critical" is performed.

DCIP. A DoD risk management program that seeks to ensure the availability of networked assets critical to DoD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the national military strategy.

DSCA. Support provided by U.S. Federal military forces, National Guard forces performing duty under Reference (~~ad~~*ah*), DoD civilians, DoD contract personnel, and DoD Component assets, in response to requests for assistance from civil authorities for special events, domestic emergencies, designated law enforcement support, and other domestic activities. Support provided by National Guard forces performing duty under Reference (~~ad~~*ah*) is considered DSCA but is conducted as a State-directed action.

EM. See Introduction, Framework Unpacked, page 5 of Reference (d).

enhanced 911 capability. 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.

ESFs. Used by the Federal Government and many State governments as the primary mechanism at the operational level to organize and provide assistance. ESFs align categories of resources and provide strategic objectives for their use. ESFs use standardized resource management concepts such as typing, inventorying, and tracking to facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident. DoD is considered a support agency to all ESFs.

essential personnel. Personnel deemed necessary for ensuring that a military mission identified as being "essential" is performed.

evacuation management. Organized, phased, and supervised withdrawal, dispersal, or removal of civilians from dangerous or potentially dangerous areas, and their reception and care in safe areas.

FCM. As defined in Reference (~~aq~~*ar*).

first receivers. Employees at a hospital engaged in decontamination and treatment of victims during an emergency incident occurring at a site other than the hospital. These employees are a subset of first responders.

first responders. Firefighters, law enforcement and/or security personnel, emergency medical technicians, and explosive ordnance disposal personnel who provide the initial, immediate response to an all-hazards incident.

full-scale exercise. Full-scale exercises simulate a real event as closely as possible. They are exercises designed to evaluate the operational capability of EM systems in a highly stressful environment that simulates actual response conditions. To accomplish this realism, they require the mobilization and actual movement of emergency personnel, equipment, and resources as outlined in the IEM Plan. Full-scale exercises incorporate the EOC and installation support functions.

functional exercise. Functional exercises are designed to validate and evaluate individual capabilities, multiple functions, activities within a function, or interdependent groups of functions. Events are projected through an exercise scenario with event updates that drive activity at the management level. Functional exercises simulate the reality of operations in a functional area by presenting complex and realistic problems that require rapid and effective responses by trained personnel in a highly stressful time-constrained environment.

hazard assessment. A DoD, command, or unit-level evaluation (assessment) to identify hazards and associated risk to person, property, and structures and to improve protection from natural or manmade disasters or hazards. Hazard assessments serve as one of the foundational components for effective EM activities including planning, resource management, capability development, public education, and training and exercises.

Appendix D.
El Paso-Teller County Authority
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:

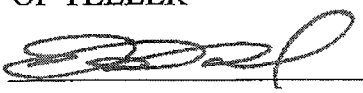
COUNTY OF EL PASO

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: [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: [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: _____

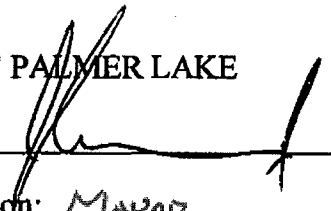
TOWN OF MONUMENT

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: _____

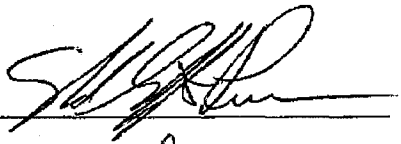
BLACK FOREST FIRE PROTECTION DISTRICT

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: _____

Aug 01 17 11:27a Broadmoor Fire Dept 1-719-633-1069 p.1

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 Kohlman

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: _____

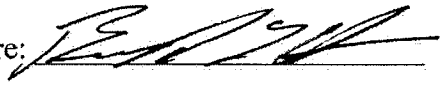
DONALD WESCOTT FIRE PROTECTION DISTRICT

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: _____

Download Show email Edit and reply

Word Online Second Amended Restated IGA(004563 Accessibility Mode Print Find Translate ...

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 G 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:

HELP IMPROVE OFFICE 100%

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: [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 E.
2019 Fort Carson PSAP Funding Agreement

2019 RESTATED PSAP FUNDING AGREEMENT

This 2019 Restated PSAP Funding Agreement ("Agreement") is entered into this 1 day of June 2019, by and between the United States Army Garrison, Fort Carson, hereinafter referred to as "the Public Agency", and the El Paso-Teller County Emergency Telephone Service Authority, hereinafter referred to as "the Authority" (the Public Agency and the Authority being referred to individually as "Party" or jointly as "Parties").

DEFINITIONS

The definitions contained in the Emergency Telephone Service Statutes shall apply to the terms used herein. The following terms shall have the following meanings unless the context requires otherwise.

A. Authority Creation Agreement. The Second Amended and Restated Intergovernmental Agreement continuing the Authority.

B. Authority Funded Equipment. Equipment requested by the Public Agency and approved and purchased by the Authority with Authority funds for use by the Public Agency related to its operation of the PSAP. The Authority Funded Equipment as of the date of this Agreement is listed on Exhibit A attached hereto and incorporated herein. Additional equipment requested by the Public Agency and approved by the Authority shall also constitute Authority Funded Equipment as provided herein.

C. Authority Funded Personnel and Services. Services or personnel costs related to a Public Agency's operation of its PSAP, requested by the Public Agency and approved by the Authority to be paid for with Authority funds. Personnel costs shall generally be funded by the Authority by making funds available to the Public Agency in advance for expenditure by the Public Agency for the personnel costs, and may, at the Authority's sole discretion, be paid for by the Authority reimbursing the costs to the Public Agency after they have been initially paid by the Public Agency. Costs of services funded by the Authority shall only be paid for directly by the Authority to the entity or person providing the services.

D. Authority Gifted Equipment. Equipment that has little or no operational or economic value and which has been transferred or gifted to the Public Agency by the Authority pursuant to the Authority's property disposal policy.

E. Emergency Telephone Service Statutes. Article 11, Title 29, C.R.S.

F. PSAP. Public Safety Answering Point, or the local 9-1-1 staff that the Public Agency maintains to provide emergency telephone service, and which meets the requirements of Section 29-11-101(6.5), C.R.S.

G. Transferred Authority Funded Equipment. Authority Funded Equipment, the ownership of which has been transferred to the Public Agency upon its request and approval by the Authority. The Transferred Authority Funded Equipment as of the date of this Agreement is listed on Exhibit B attached hereto and incorporated herein. Additional Transferred Authority Funded Equipment requested by the Public Agency and approved by the Authority shall also constitute Transferred Authority Funded Equipment as provided herein. Transferred Authority Funded Equipment generally consists of equipment that is no longer supported by the Authority or which because of Public Agency's policy or practice the Public Agency desires to own and continue using for its PSAP purposes, subject to the terms of this Agreement.

RECITALS

WHEREAS, the Authority is a separate legal entity that is a political subdivision and public corporation of the state, separate from the parties to the Authority Creation Agreement, organized pursuant to 29-1-203.5 C.R.S., and the Emergency Telephone Service Statutes for the purpose of providing emergency telephone service, and providing for its organization, administration and operation within El Paso and Teller counties; and

WHEREAS, the Public Agency is a Party to the Authority Creation Agreement, and operates a PSAP located on Fort Carson Army Base that provides enhanced emergency telephone service within its jurisdiction; and

WHEREAS, the Authority is authorized by the Emergency Telephone Service Statutes and the Colorado Public Utilities Commission to collect an emergency telephone charge from all telecommunications users who receive emergency telephone service and use the revenues to purchase equipment necessary to provide emergency telephone service; and

WHEREAS, as approved by its Board of Directors, the Authority funds Authority Funded Equipment, Transferred Authority Funded Equipment, and Authority Funded Personnel and Services directly related to the continued operation of the Public Agency's emergency telephone service and emergency notification service; and

WHEREAS, the Authority, in its sole discretion, has previously approved requests from the Public Agency for Authority Funded Equipment which is described on Exhibit A attached hereto and incorporated herein, and Transferred Authority Funded Equipment which is described on Exhibit B attached hereto and incorporated herein; and

WHEREAS, the Public Agency may in the future request, and the Authority may, in its sole discretion approve additional Authority Funded Equipment and Transferred Authority Funded Equipment; and

WHEREAS, the Parties have previously defined and agreed to the conditions associated with the Authority's approval and the Public Agency's acceptance and use of Authority Funded Equipment and Transferred Authority Funded Equipment; and

WHEREAS, in 2006 the Parties entered into the PSAP Funding Agreement and in 2015 entered into the Addendum to PSAP Funding Agreement, and wish by this Agreement to terminate these prior agreements and enter into this 2019 Restated PSAP Funding Agreement;

NOW THEREFORE, in consideration of the mutual covenants and promises contained herein, the Parties hereby agree as follows:

1. Incorporation of Definitions and Recitals. The definitions and recitals set forth above are incorporated into the covenants and agreements agreed to by the Parties.

2. Termination of Prior Agreements. All prior agreements between the Parties related to the Authority Funded Equipment, including but not limited to the 2006 PSAP Funding Agreement and the 2015 Addendum to PSAP Funding Agreement, are hereby terminated.

3. Conditions of Authority Funding. All Authority Funded Equipment as listed on Exhibit A and Transferred Authority Funded Equipment as listed on Exhibit B, and as may be in the future requested by the Public Agency and approved by the Authority, and its continued use by the Public Agency shall be subject to all terms and conditions of this Agreement.

4. Additional Authority Funded Equipment. From time to time the Public Agency may request, and the Authority in its sole discretion may approve additional Authority Funded Equipment for use by the Public Agency. Approval of any additional Authority Funded Equipment shall be contingent upon sufficient funds being appropriated and budgeted by the Authority in the year of the proposed expenditure. Any additional Authority Funded Equipment shall be subject to the terms of this Agreement unless the Parties agree otherwise in writing. Upon approval by the Authority of additional Authority Funded Equipment, the Parties shall execute a written addendum to this Agreement substantially in the same format of Exhibit A, and specifying any special conditions, requirements or restrictions associated with the approval, if any. Failure of the Parties to execute such addendum shall not except the additional Authority Funded Equipment from the terms of this Agreement.

5. Compliance with Authority Policies. The Public Agency agrees to comply with the written Policies and Procedures of the Authority associated with receipt, use, operation, maintenance, licensing, return and disposal of Authority Funded Equipment and Transferred Authority Funded Equipment and operation of the Public Agency's PSAP, as approved by its Board of Directors, as they currently exist and as adopted or

amended from time to time. At such time as Authority adopts or amends its Policies and Procedures, copies shall be provided to the Public Agency, which may be done by posting on the Authority's website. At the request of the Public Agency, the Authority's Chief Executive Officer shall provide a certified copy of the Authority's Policies and Procedures which are the subject of this paragraph in effect at the time of the request. The Authority Policies and Procedures which are the subject of this paragraph at the time of execution of this Agreement are as follows:

(a) Policy No. 4.14 Supplies and Equipment

(b) Policy No. 5.0 Emergency Medical Dispatch Policy

(c) Policy No. 5.1 Emergency Medical Dispatch Quality Assurance and Improvement Process

6. Ownership and Maintenance of Authority Funded Equipment. All Authority Funded Equipment shall be and remain the property of the Authority, unless otherwise agreed to by the Authority. Unless the Authority agrees in writing and appropriates sufficient funds for payment in the year of the proposed expenditure, costs associated with operation of the Authority Funded Equipment shall be paid by the Public Agency. Such agreement and appropriation shall not be unreasonably withheld. The Public Agency agrees to operate Authority Funded Equipment in the manner for which it was designed. To the extent reasonably possible, the Authority shall insure against general property casualty and theft at its replacement value, and such insurance shall provide primary coverage, and maintain in good and working condition all Authority Funded Equipment. The Authority hereby waives all claims against the Public Agency for property loss or damage to the Authority Funded Equipment except in the case of gross negligence or willful or wanton actions of the Public Agency. In the event of any loss or damage to Authority Funded Equipment, the Public Agency shall immediately notify the Authority, shall take such steps as are required of the Authority by the Authority's insurer, and shall fully cooperate in good faith with any investigation conducted by such insurer. The Public Agency, at the Public Agency's sole discretion, may insure Authority Funded Equipment, and in such event the Authority insurance shall provide secondary coverage. Each Party shall at the request of the other Party provide a certificate of insurance evidencing this insurance coverage. Should the Public Agency no longer desire the use of the Authority Funded Equipment for the purposes provided for in this Agreement, it shall immediately transfer possession of the equipment back to the Authority at no cost to the Authority, free and clear of liens or encumbrances, and subject to the Authority's policies on use and disposal of assets.

7. Transferred Authority Funded Equipment. All Transferred Authority Funded Equipment as listed on Exhibit B and as may in the future be requested to be classified as Transferred Authority Funded Equipment by the Public Agency and approved by the Authority, shall continue to be subject to the terms of this Agreement

including those concerning Authority Funded Equipment, subject to the following, specific and additional terms and conditions.

(a) The Public Agency will own, license and insure all Transferred Authority Funded Equipment.

(b) If the Public Agency wishes to discontinue use of the Transferred Authority Funded Equipment for the purposes provided for in this Agreement, or otherwise wishes to dispose of it, it shall be transferred at no cost to the Authority, free and clear of liens or encumbrances, and subject to the Authority's policies on use and disposal of assets.

(c) Any additional special conditions related to transfer of ownership of Transferred Authority Funded Equipment to the Public Agency, or its operation, use, maintenance or disposal, shall be noted on Exhibit B.

8. Limitations on Authority Funded Equipment, Transferred Authority Funded Equipment, and Authority Funded Personnel and Services. Use by the Public Agency of Authority Funded Equipment, Transferred Authority Funded Equipment, and Authority Funded Personnel or Services shall comply at all times with the requirements and limitations of the Emergency Telephone Service Statutes, the Authority's Policies and Procedures noted in paragraph 5, and this Agreement, and be directly related to operation of the Public Agency's PSAP. Authority Funded Equipment, Transferred Authority Funded Equipment, and Authority Funded Personnel and Services are not intended for the general use of the Public Agency or its departments or personnel. Funding for Authority Funded Personnel may only be used for compensation, benefits, and training for emergency call-takers and dispatchers employed to take emergency telephone calls and dispatch them. At all times the Public Agency shall continue to operate a PSAP. Should the Public Agency fail to operate a PSAP, or if its emergency telephone service fails to qualify as a PSAP, or the Public Agency otherwise fails to meet its obligations under this Agreement, the Authority may, in its sole discretion, retake possession of any and all Authority Funded Equipment and Transferred Authority Funded Equipment or dispose of the same consistent with the Authority's Policies and Procedures, and the Authority may also require the Public Agency to reimburse the Authority for all unexpended funds or the amounts previously paid by the Authority for Authority Funded Personnel and Services associated with the time following the failure. So long as the Public Agency shall comply with the terms of this Agreement, it shall be allowed the use of the Authority Funded Equipment, Transferred Authority Funded Equipment, and Authority Funded Personnel and Services without interruption or interference by the Authority.

9. Authority Gifted Equipment. From time to time the Authority may, based on its property disposal policies, gift to the Agency equipment that has little or no economic or operational value. Authority Gifted Equipment is not subject to the terms of

this Agreement or the Authority's Policies and Procedures and may be used, maintained, insured and disposed of in the sole discretion of the Agency. At the time Authority Funded Equipment or Transferred Authority Funded Equipment is placed with or transferred to the Agency and added to either Exhibit A or Exhibit B it may be assigned an end of life date, in which case as of the specified end of life date the Authority Funded Equipment or Transferred Authority Funded Equipment shall be automatically and without further action of the Parties converted to Authority Gifted Equipment. If not otherwise specified on Exhibit B, all technical Transferred Authority Funded Equipment, such as servers, loggers and monitors, shall have an end of life date that is five (5) years from the date it is originally transferred to the Public Agency and all non-technical Transferred Authority Funded Equipment, such as desks, shelves, and chairs, shall have an end of life date that is seven (7) years from the date it is originally transferred.

10. Additional Requirements and Limitations Associated with Authority Funding Commitments. All funds provided by the Authority to the Public Agency for Authority Funded Personnel shall be restricted and encumbered by the Public Agency for the limited purposes set forth in the previous Section of this Agreement and must be returned to the Authority at the end of the fiscal year following the fiscal year in which they are paid by the Authority to the Public Agency, if not expended for the intended purposes. All funds approved by the Authority to provide Authority Funded Equipment or Authority Funded Services for the benefit of the Public Agency must be expended within the fiscal year in which they are budgeted and appropriated by the Authority, and if not, the funds will be returned to the Authority's unexpended surplus and available for budgeting, appropriation and expenditure by the Authority in the following fiscal year in the sole discretion of the Authority.

11. Confidentiality. As regards any and all documents of either Party that may come into the possession of the other Party, the Parties agree to follow the Colorado Public Records laws, contained primarily in Part 2, Article 72, Title 24. The Parties recognize that certain documents of the Parties related to funding and services provided by the Authority to the Public Agency are or may be confidential. The Authority will keep confidential the personnel records of Public Agency personnel. The Public Agency agrees that it shall not make available for public inspection or copying the personnel records generated or maintained by the Authority, including training records of Public Agency personnel, documents marked by the Authority as "Confidential," documents containing specialized details of security arrangements, and documents required by state or federal laws to be kept confidential, including HIPAA. The Parties agree that any such documents that come into the possession of the other Party shall, to the extent possible, be clearly marked as to their originating source and with the word "confidential" on the front page. The Parties agree to take all reasonable steps to redirect requests for such documentation to the originating party. This paragraph shall not be construed, however, as license to disobey a valid court or administrative order, or as establishing a breach-of-contract claim for complying with such an order.

12. Future Authority Funding. The Authority's funding in any given year of Authority Funded Equipment, Transferred Authority Funded Equipment, or Authority Funded Personnel and Services shall not obligate the Authority to continue providing such funding in future years. The Public Agency may not act in reliance on funding being budgeted, appropriated or authorized for such purpose by the Authority in future years.

13. Term. This Agreement shall remain in effect so long as the Public Agency retains Authority Funded Equipment or Transferred Authority Funded Equipment. The Public Agency may terminate this Agreement upon sixty (60) days written notice to the Authority and by returning all Authority Funded Equipment and Transferred Authority Funded Equipment. The Authority shall not unilaterally terminate this Agreement so long as the Public Agency remains in compliance with its terms.

14. Notices. All notices, demands, requests or other communications to be sent by one Party to the other hereunder or required by law shall be in writing and shall be deemed to have been validly given or served by delivery of same in person to the addressee or by courier, delivery via Federal Express or other nationally recognized overnight courier service or by depositing same in the United States mail, postage prepaid, addressed as follows:

To Authority:	Chief Executive Officer El Paso-Teller County Emergency Telephone Service Authority 2350 Airport Road Colorado Springs, Colorado 80910
To the Public Agency:	Garrison Commander BLDG 1118 1626 Ellis Street Fort Carson, Colorado 80913

15. Integration. This Agreement represents the entire agreement between the Parties and there are no oral or collateral agreements or understandings. This Agreement may be amended only by an instrument in writing signed by the Parties. If any other provision of this Agreement is held invalid or unenforceable, no other provisions shall be affected by such holding, and all of the remaining provisions of this Agreement shall continue in full force and effect.

16. Choice of Law and Venue. This Agreement and the provisions hereof shall be governed by and construed in accordance with the laws, rules and regulations of the State of Colorado, without regard to principles of conflicts of law. The Parties agree that the proper venue for resolution of any disputes arising out of this Agreement shall be in the District Courts of the Fourth Judicial District, El Paso County, Colorado. Any

provision of this Agreement, whether or not incorporated herein by reference, which provides for arbitration by any extra-judicial body or person or which is otherwise in conflict with said laws, rules and regulations shall be considered null and void. Nothing contained in any provision incorporated herein by reference which purports to negate this or any other special provision in whole or in part shall be valid or enforceable or available in any action at law, whether by way of complaint, defense or otherwise. Any provision rendered null and void by the operation of this provision shall not invalidate the remainder of this Agreement to the extent that this Agreement is capable of execution.

17. Amendments. This Agreement may be amended only by a written instrument, executed by all of the Parties hereto. Variances to the obligations, limitations and requirement set forth above may only be provided by written amendment or separate, written agreement signed by the parties.

18. Headings. The headings in this Agreement are inserted for convenience only and are in no way intended to describe, interpret, define or limit the scope, extent or intent of this Agreement or any provisions hereof.

19. Default/Remedies. In the event of a breach or default of this Agreement by either Party, the non-defaulting Party shall be entitled to exercise all remedies available at law or in equity, including without limitation specific performance. In the event of a breach or default by the Public Agency, the Authority may, with or without terminating this Agreement, retake any and all Authority Funded Equipment. In the event of any litigation or other proceeding to enforce the terms, covenants or conditions hereof, the prevailing Party in such litigation or other proceeding may be entitled to an award of its reasonable attorneys' fees.

20. Waivers. The failure of any party to seek redress for violation of or to insist upon the strict performance of any covenant or condition of this Agreement shall not prevent a subsequent act, which would have originally constituted a violation, from having the effect of an original violation. Any provision contained herein allowing for a waiver of conditions shall require the waiver of all Parties, unless specifically otherwise indicated.

21. Severability. If any provision of this Agreement or the application thereof to any party or circumstance shall be invalid, illegal or unenforceable to any extent, the remainder of this Agreement and the application thereof shall not be affected and shall be enforceable to the fullest extent permitted by law. However, in the event that the severance of an invalid or enforceable provision materially impairs the consideration expected by a Party, then such Party may terminate this Agreement.

22. Assignment. Neither Party shall assign any of its rights or delegate any of its duties hereunder to any person or entity without having first obtained the prior written consent of the other Party, which consent shall not be unreasonably withheld. Any

assignment or delegation in violation of the provisions hereof shall be void and ineffectual. Each of the terms, covenants and conditions hereof shall be binding upon and inure to the benefit of the Parties and their duly authorized successors and assigns.

23. Counterparts. This Agreement may be executed in counterparts, each of which shall be deemed an original but all of which shall constitute one and the same instrument.

24. Indemnity. The Public Agency shall indemnify, defend and hold harmless, to the extent allowed by law, the Authority, its members, agents, officers, directors, and employees from any and all liability, claims, losses, demands, actions, causes of action and expenses whatsoever, including, without limitation, costs of litigation and reasonable attorney's fees, arising out of or in any way related to this Agreement, including, without limitation, the Public Agency's negligent, intentional, or grossly negligent acts, and the installation, operation, maintenance, use and/or existence of Authority Funded Equipment. The Authority shall indemnify, defend and hold harmless, to the extent allowed by law, the Public Agency, its members, agents, officers, directors and employees from any and all liability, claims, losses, demands, actions, causes of action and expenses whatsoever, including, without limitation, costs of litigation and reasonable attorney's fees, arising out of or in any way related to the Authority's actions, errors or omissions with respect to this Agreement, including without limitation, the Authority's negligent, intentional, or grossly negligent acts related to the installation, operation, maintenance, use and/or existence of Authority Funded Equipment.

25. Compliance with Laws. At all times during the performance of this Agreement, the Parties shall strictly adhere to all applicable federal, state and local laws, rules and regulations that have been or may hereafter be established.

26. Relationship of the Parties. Nothing in this Agreement creates or shall be construed or deemed to create a partnership or joint venture or principal-agent or employment relationship between any of the Parties to this Agreement. Nothing in this Agreement creates or vests, and nothing in this Agreement shall be construed or deemed to create or vest, in the Authority any right, title or interest in the equipment purchased pursuant to this Agreement. Each Party is responsible for all costs of its personnel including pay and benefits, support, and travel. Each Party is responsible for supervision and management of its personnel. This Agreement does not document nor provide for the exchange of funds between the Parties.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement the day and year first above written. This Agreement will expire 1 June 2029.

Public Agency:
FORT CARSON GARRISON

By: _____ 20190708
BRIAN K. WORTINGER (Date)
COL, AR
Garrison Commander

ATTEST:

_____
Clerk

EL PASO-TELLER COUNTY E-911 AUTHORITY

By: _____ Chair
7/24/2019 (Date)

ATTEST:

_____
Secretary

References & Resources

Colorado Next Generation 9-1-1 System Review Report, Colorado 9-1-1 Resource Center, August 2011
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*, April 9, 2015
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 8540.01, *Cross Domain Policy*, Change 1, August 28, 2017
DoD Strategic Management Plan, July 2013
A Plan for the Continued Implementation of 9-1-1 in the State of Colorado, Colorado 9-1-1 Resource Center, January 16, 2015
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*

AR 525-27, *Army Emergency Management Program*
Army Network Campaign Plan, ver. 1.1, February 2015
El Paso Teller County 911 Authority, http://www.elpasoteller911.org/
El Paso Teller County 911 Authority 2017-2018 Authority Strategic Plan
FCC 14-13, PS Docket No. 07-114, Proposed Rulemaking
FCC Task Force on Optimal PSAP Architecture, *Adopted Final Report*, January 29, 2016
FCC, *Tenth Annual Report to Congress on the State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, December 17, 2018
FCC TFOPA, *Working Group 2: Optimal Approach to MG91-1-1 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, review 04/05/2018

Acronyms and Abbreviations

CAD	Computer-aided dispatch
CDC	Consolidated dispatch center
CIO	Chief information officer
COP	Common operating picture
COOP	Continuity of operations
CHE	Call-handling equipment
DoDI	Department of Defense Instruction
DOT	Department of Transportation
E911	Enhanced 911
ECC	Emergency Communications Center
EMS	Emergency Medical Service
EPTC	El Paso and Teller Counties
ESInet	Emergency Services IP Network
F&ES	Fire and Emergency Services
FCC	Federal Communications Commission
FCF&ES	Fort Carson Fire and Emergency Services
FY	Fiscal Year
GIS	Geographic information systems
IGA	Intergovernmental agreement
IP	Internet protocol
JB CHS	Joint Base Charleston
MCAS	Marine Corps Air Station
MoA	Memorandum of agreement
NENA	National Emergency Number Association
NG911	Next-generation 9-1-1
NGCS	Next-generation core services
PCMS	Piñon Canyon Maneuver Site
PSAP	Public safety answering point
RFP	Request for Proposals
TFOPA	Task Force on Optimal PSAP Architecture

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-07-19	Draft Final	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Military and Civilian Collaborations in Deploying Next-Generation 9-1-1	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-10771

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Katherine Brennan, Deputy, Law Enforcement Division Headquarters Department of the Army, Office of the Provost Marshal General 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

DoD 9-1-1 emergency call centers, known as public safety answering points, are challenged in making the necessary migration from the legacy, analog-based 9-1-1 environment to the digital, IP-based next-generation 9-1-1 (NG911) environment. Civilian agencies are increasingly deploying NG911 solutions at the state and regional levels. Maintaining parity with the surrounding civilian agencies is critical as telecommunications providers will be retiring their entire legacy 9-1-1 infrastructure. This document highlights a few collaborative approaches between military installations and their abutting civilian jurisdictions that can be adopted by others in the near-term to minimize or avoid a NG911 capability gap. Collaboration provides substantial benefits to each partner and reflects the strong economic, human capital, and operational bonds between the DoD installations and the communities where they reside.

15. SUBJECT TERMS

Next Generation 9-1-1, Public Safety Answering Point, military, civilian, collaboration

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, Deputy, Law Enforcement Division
Unclassified	Unclassified	Unclassified	Unlimited	237	19b. TELEPHONE NUMBER (Include Area Code) 703-692-6721