



INSTITUTE FOR DEFENSE ANALYSES

Computer Aided Dispatch Interoperability Case Studies

Serena Chan, *Project Leader*

John W. Bailey
Ronald A. Enlow
Clyde G. Roby

December 15, 2017

Approved for public release;
distribution is unlimited.

IDA Document
D-8778

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 Enterprise Mass Warning & Notification," for DoD CIO. 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

Francisco L. Loaiza-Lemos, Michael T. Hernon, Russell J. Smith

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

© 2017 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-8778

Computer Aided Dispatch Interoperability Case Studies

Serena Chan, *Project Leader*

John W. Bailey
Ronald A. Enlow
Clyde G. Roby

Executive Summary

This document reports on work done by the Institute for Defense Analyses (IDA) for the Office of the Deputy Chief Information Officer (DCIO) for Command, Control, Communications, and Computers and Information Infrastructure Capabilities (C4&IIC), Department of Defense (DoD) Chief Information Officer (CIO).

This document addresses the interoperability of Computer Aided Dispatch (CAD) systems. CAD systems are used by Public Safety Answering Points (PSAPs) to dispatch first responders to answer Calls For Service (CFS) (9-1-1 calls or alarms). The premise of this document is that neighboring jurisdictions, whether military, civilian, or mixed, can benefit from interoperable CAD systems. This document examined case studies of several implementations of interoperable CAD systems and describes their path toward interoperability with surrounding jurisdictions. These illustrative case studies serve to initiate discussions about whether a DoD-wide policy standard for implementation of interoperable military-civilian CAD systems is viable.

The four case studies discussed include:

1. U.S. Navy Regional Dispatch Centers and the Public Safety Network;
2. Charleston County, South Carolina, and Joint Base Charleston;
3. National Capital Region Fire and EMS Interoperable Communications;
4. FATPOT Technologies, Inc.: Lake County, Illinois, and Boston, Massachusetts.

General Observations

1. The CAD market is fractionated. There are at least 21 primary CAD vendors and over 100 secondary vendors. This complicates the process of implementing even a small-scale interoperable, multi-jurisdiction/multi-agency CAD system.
2. In the majority of the case studies, an Internet-capable bearer network spanning the area already was in existence. This not only facilitated the technical implementation of interoperable CAD but significantly reduced the costs attributable to that implementation. Bearer networks ranged from national in scope to single counties.
3. Anecdotal evidence indicates that cooperation between multiple vendors of CAD systems is often needed but difficult to achieve (requiring proprietary software). This has been overcome by the selection of a single vendor or use of

multiple application program interfaces (APIs) to implement a hub-and-spoke architecture.

4. Decisions to implement interoperable CAD systems are typically local ones. Each locality will have unique aspects: the CAD systems already in use, the local communities to be included, jurisdictional boundaries, the total population involved, the types of first response organizations selected to participate (one case study included fire and EMS but not police), and budgetary constraints.
5. When mobile devices are used on a military installation to make 9-1-1 calls, the call does not necessarily go to base operators but is routed to a civilian 9-1-1 call center. Eliminating the “call forwarding” delay was a motivating factor in multiple case studies.

Contents

Executive Summary	i
Contents	iii
1. Introduction	1-1
A. Background	1-1
B. Methodology	1-2
1. CAD Vendor Survey	1-3
C. Scope and Approach – Case Study.....	1-4
2. CAD Interoperability Case Studies	2-1
A. Case Study A: USN Regional Dispatch Centers and the Public Safety Network	2-2
1. Context	2-2
2. Interoperability Path	2-4
B. Case Study B: Charleston County, South Carolina, and Joint Base Charleston 2- 6	
1. Context	2-6
2. Interoperability Path	2-8
3. Charleston CAD Vendor Selection Task List	2-10
4. Interagency Network Diagram	2-14
5. Charleston 9-1-1 Center Details	2-16
C. Case Study C: National Capitol Region Fire and EMS Interoperable Communications.....	2-19
1. Context	2-19
2. Interoperability Path	2-21
D. Case Study D: FATPOT Technologies, Inc., Lake County, Illinois, and Boston, Massachusetts	2-29
1. Context	2-29
2. Interoperability Path Examples	2-30
3. Discussion.....	3-1
A. General Observations	3-2
Appendix A CAD Vendor List	A-1
Acronyms and Abbreviations	1

Figures and Tables

Figure 2-1. PSNet Regional Dispatch Center	2-4
Figure 2-2. Example Base Architecture.....	2-5
Figure 2-3. JB Charleston and the Tri-County Area.....	2-7

Figure 2-4. Charleston Interagency Network Diagram.....	2-15
Figure 2-5. NCRnet Link Map.....	2-23
Figure 2-6. Interconnections Required Among Four Partner Systems	2-26
Figure 2-7. Partner System Interconnection Using the DEH.....	2-27
Figure 2-8. Generic Diagram of FATPOT Fusion PLATFORM Connectivity.....	2-31
Figure 2-9. Lake County, Illinois, FATPOT Architecture Diagram.....	2-32
Figure 2-10. FATPOT Implementation Architecture for Boston Region.....	2-34
Table 2-1. Call and Incident Volumes	2-10
Table 2-2. Metrics and Standards	2-10
Table 2-3. Charleston Personnel Titles and Numbers of Employees	2-16

1. Introduction

This document reports on work done by the Institute for Defense Analyses (IDA) for the Office of the Deputy Chief Information Officer (DCIO) for Command, Control, Communications, and Computers and Information Infrastructure Capabilities (C4&IIC), Department of Defense (DoD) Chief Information Officer (CIO).

This document addresses the interoperability of Computer Aided Dispatch (CAD) systems. CAD systems are used by Public Safety Answering Points (PSAPs) to dispatch first responders to answer Calls For Service (CFS) (9-1-1 calls or alarms). The premise of this document is that neighboring jurisdictions, whether military, civilian, or mixed, can benefit from interoperable CAD systems. This document examined case studies of several implementations of interoperable CAD systems and describes their path toward interoperability with surrounding jurisdictions. These illustrative case studies serve to initiate discussions about whether a DoD-wide policy standard for implementation of interoperable military-civilian CAD systems is viable.

A. Background

The historical antecedents of Computer Aided Dispatch (CAD) reach back over a hundred years to the invention of the telegraph in 1844. Not surprisingly, the original agencies driving the development of alarm systems were fire departments. The first municipal fire alarm system, based on the Morse telegraph and installed in Boston, Massachusetts, in 1851,¹ was considered revolutionary at the time. However, these alarm boxes were prone to false alarms and pranks, and with the invention of the telephone, they were replaced by Emergency Response Service boxes that enabled a direct telephonic link to a fire department response facility. This technology enabled direct person-to-person communications with a central dispatcher, with the additional virtue of including a primitive false alarm determination. Call boxes were still in use during the 1950s, but their use in recent times has been virtually eliminated. With the introduction of mainframe computers in the 1960s, the initial application of automation was in fire service administrative functions—not emergency response.

However, data shows that to a great extent, police departments, particularly in large urban areas, have more calls to answer and more units to dispatch than fire departments.

¹ *Computer aided dispatch technology: A study of the evolution and expectations of CAD and a comparative survey of CAD in the U.S. Fire Service and the Clark County Fire Department*, Kenneth E. Morgan, University of Nevada, Las Vegas, 2003.

Consequently, the next advances in the application of automation were developed by police departments. Police departments followed the examples of the automation of military command and control systems. The police use of direct computer aided emergency response increased rapidly. In the 1970s, police applications were enabled by funding from the Law Enforcement Assistance Administration. The Los Angeles, California, police department teamed with Jet Propulsion Laboratory in 1972 to develop a computerized dispatch system with Mobile Data Terminals (MDT) in police vehicles. Their system was dubbed the Emergency Command and Control Communications System (ECCCS).

In the 1980s, predecessors of today's CAD systems began to be implemented in the larger emergency response departments. The primary limiting factor to their spread was cost since they were custom-engineered systems. In 1980, the Fire Department of New York (FDNY) entered the computer age with STARFIRE. At a cost of \$15 million (1980 dollars), it connected 14 computers, 12 microcomputers, and 500 terminals and covered just one of five boroughs. This effort was considered a major undertaking, even for a large city with a substantial emergency response budget. Ultimately, the STARFIRE system was expanded to all boroughs and 250 fire houses. New York City replaced the system under the Emergency Communications Transformation Program, which was initiated in the early 2000s, and work to upgrade the system continues today.

The modern CAD system is generally integrated into a larger administrative unit, the Public Safety Answering Point (PSAP). The PSAP dispatches first responders to answer Calls for Service (CFS) (9-1-1 calls or alarms). The integrated CAD system becomes the link between virtually all initial emergency communications, status reporting, and response actions. As such, it can be thought of as a civilian analog of military command and control (C2) systems. Like military C2 systems, civilian CAD systems track responses to emergencies and provide an operating picture or situational awareness as the emergency response evolves.

A CAD system can potentially share the emergency operating picture laterally between jurisdictions if interoperability and data sharing have been implemented. If this is the case, then jurisdictions have the capability to request additional resources from those jurisdictions. The premise of this document is that neighboring jurisdictions, whether military, civilian, or mixed, will benefit from interoperable CAD systems if a solution to interoperability can be found. To investigate the feasibility of CAD interoperability, CAD vendors were surveyed and asked to describe existing solutions.

B. Methodology

In beginning our research, the IDA team sent out Requests for Information (RFI) to 28 CAD vendors, selected from over 75 CAD vendors that we discovered in the United States. Respondents were invited to provide documentation, discuss their CAD systems with the IDA team, and visit IDA to provide face-to-face technical interchanges.

CAD Vendor Survey

The IDA team received RFI responses from three CAD vendors: Caliber Public Safety,² Motorola,³ and FATPOT Technologies, Inc.⁴ In addition, the IDA team separately received a description of the U.S. Navy (USN) Regional Centers approach to CAD interoperability.

The response from Caliber described an Internet-based approach that relies heavily on national data standards. Their solution involves standards-based cooperation between vendors to ensure that systems from different vendors can interoperate.

The documents from Motorola reinforced the IDA team's initial assumption that, short of using one vendor across all cooperating entities or else ensuring that the various vendors share a single messaging language, CAD-to-CAD interoperability could be supported only by writing and using application programming interfaces (APIs) for each pairing of systems for them to be able to pass messages. It then became clear to the IDA team that there were two additional and very different architectural approaches to achieving interoperability, neither depend either on message standards or on pairing-unique API developments.

The responses from FATPOT and from the USN broadened our understanding by illustrating two other solution paths. First, the FATPOT response explained that they have developed a hub-and-spoke architecture that enables CAD interoperability by using a proprietary central fusion engine as a hub. This allows disparate CAD systems to connect by spokes to this hub and, although APIs may have to be written by FATPOT, the connection architecture remains transparent to the interoperating CAD systems; all connected systems can send and receive messages in their own format just as though they were interfacing with other instances of their same system. This independence among systems means that there is no requirement to share message standards between any of the interoperating CAD systems, nor is there a requirement to write one-off translations from one vendor's message standard to another's.

An example of the second new solution path was described in a briefing we received outlining the USN Regional Dispatch architecture. This architecture incorporates a highly distributed functionality based on an AT&T Corporation (AT&T) telecommunications backbone and yields a fourth solution in addition to those suggested by Caliber, FATPOT, or Motorola.

Significantly, little emphasis was given to compliance with data standards except when mandatory, as required by state regulations. The capability to share data was often

² Caliber Public Safety, 2429 Military Road, Niagara Falls, NY 14304, www.caliberpublicsafety.com

³ Motorola Solutions, Inc., 500 W Monroe Street, Chicago, IL 60661, www.motorolasolutions.com

⁴ FATPOT Technologies, Inc., 655 Medical Dr., # 100, Bountiful, UT 84010, www.fatpot.com

advertised in the marketing materials of CAD vendors, but it is difficult to know whether this referred to the vendor's internal data warehouse or the real-time sharing of incidents and resources with external systems. Generally, any real-time sharing was assured only among agencies with identical suites of CAD software. We were able to discuss approaches to CAD interoperability with IDA employees with relevant experience and with consultants in the Washington area. Their experiences confirmed that interfaces among disparate CAD systems almost always required the development of custom software. Developing such custom software, even when using an API, is time-consuming and expensive, and requires the cooperation among vendors of proprietary and potentially competitive software products.

Given the diversity of approaches in the four CAD interoperability solutions that we became aware of, it seemed desirable to reach out to more of the major CAD providers to ensure that we captured an even wider scope of interoperability paths. However, an additional RFI was impractical given the time and resources available. Instead, the IDA team shifted its approach to concentrate on examining a representative sample of interoperability solutions using a case study approach.

C. Scope and Approach – Case Study

After receiving vendor responses and learning of the four CAD interoperability solutions (same vendor, regional PSAP, hub-and-spoke architecture, and telecommunications backbone), the IDA team attempted to examine individual DoD and civilian communities to learn what CAD interoperability solutions were presently in use. Example DoD–community emergency dispatch implementations were selected based on historical contacts and knowledge of Joint Bases that require interoperability with civilian jurisdictions. Two examples of the sites we identified are Kirtland AFB, which shares its facilities with the Albuquerque, New Mexico, civilian airfield, and Joint Base Charleston, South Carolina, which straddles the border between the counties of Charleston and Berkeley.

The results of the case study approach are described in the next chapter. Each case study has two sections. The first section provides context, e.g., the description of a county with multiple jurisdictions, including a military installation, and which has decided to enable their CAD systems to interoperate. The second section describes the interoperability implementation path, e.g., the selection of a CAD interoperability vendor and how it achieved the required interoperability or the development of an in-house solution to directly connect different CAD systems.

2. CAD Interoperability Case Studies

The IDA team used several resources to understand the magnitude of need for emergency dispatch interoperability between DoD installations and surrounding communities. A Base Realignment and Closure (BRAC) report⁵ from 1998 cited 259 bases that were identified by the Military Departments as “major installations.” The list consisted of 74 Army, 103 Navy and Marine Corps, 76 Air Force, and 6 Defense Logistics Agency installations. However, Appendix J of the same report lists 390 installations with 300 or more civilian authorizations, the method used by the BRAC study to identify the most sizeable installations. This list consisted of 125 Army, 128 Navy, 14 Marine Corps, 75 Air Force, and 48 Defense Agency and Field Activity installations.⁶

An even more comprehensive list of DoD bases, posts, camps, and stations was obtained from the National Geospatial-Intelligence Agency (NGA) map “U.S. Military Installations Map.jpg,” also available on Wikipedia.⁷ This map shows the locations of 483 DoD installations, ranges, and training areas, all bordering on civilian jurisdictions of one kind or another. We assume this number of co-located DoD installations and civilian communities could be considered a proxy for the potential number of CAD interoperability implementations in DoD.

For a case study approach, however, an exhaustive list of DoD installations and their surrounding communities was not necessary. Instead, the IDA team examined a small sample of installations and locations to learn about different methods used at these facilities to coordinate the emergency responses of the military installation’s assets with those of the nearby civilian jurisdictions. The IDA team chose the following list either because they had already identified a relevant DoD point of contact or because of a perceived need for CAD interoperability at the locations involved.

1. USN Regional Centers;
2. National Capital Region (NCR);
3. Joint Base Charleston/Charleston County, South Carolina;

⁵ <http://archive.defense.gov/pubs/brac040298.pdf>, accessed September 29, 2017.

⁶ Ibid, page 135.

⁷ https://www1.nga.mil/ProductsServices/TopographicalTerrestrial/PublishingImages/8205XMILINST_049.jpg, accessed from Wikipedia, September 29, 2017, which includes the further footnote, “U.S. Military Installations Map (CONUS). This is a map of the major U.S. military installations, ranges and training areas in the continental United States. It is used by military and government contacts to assist in Federal communication to state and local governments.”

4. Great Lakes Naval Station, Lake County, Illinois;
5. Joint Base McGuire-Dix-Lakehurst, New Jersey;
6. McDill AFB, Tampa, Florida;
7. Kirtland AFB, Albuquerque, New Mexico;
8. Peterson AFB/Fort Carson, Colorado Springs, Colorado;
9. Joint Base Pearl Harbor-Hickam, Hawaii;
10. Fort Bragg, North Carolina.

The IDA team made several attempts to contact the facilities on this list but was only partially successful. Case studies were possible for only the first four locations on the list. The remaining locations either did not use CAD systems (Kirtland AFB and Joint Base Pearl Harbor-Hickam) or did not return our calls (Joint Base McGuire-Dix-Lakehurst, McDill AFB, Peterson AFB, and Fort Bragg).

The remainder of this chapter is devoted to descriptions of the four successful case studies, each organized into the two sections as previously described: (a) Context and (b) Interoperability Path. The fourth case study, FATPOT, incorporates a discussion of CAD interoperability within Lake County, Illinois, and the Boston, Massachusetts area.

A. Case Study A: USN Regional Dispatch Centers and the Public Safety Network

1. Context

The Commander, Navy Installations Command (CNIC) Office of the Command Information Officer (N6) delivers common, business and operational Information Technology (IT) services as part of the overall Service IT activity. N61 – Control, Communications and Protection (C3P) Ashore provides IT solutions and support services to global network transport via the Public Safety Network (PSNet). PSNet services include Navy Emergency Response Management System (NERMS), Enterprise Land Mobile Radio (ELMR), Navy Port Operations Management (POMS), Navy Access Control Management System (NACMS), Automated Vehicle Gates (AVG), Advanced Metering Infrastructure (AMI), and Industrial Control Systems (ICS). Through PSNet, the USN supports first responders, emergency management, and the monitoring of critical infrastructure.

The availability of PSNet enabled the USN to move to its original regional approach to emergency services dispatch. The PSNet began to evolve in 2005 as a result of the inability of the Navy–Marine Corps Intranet to meet quality-of-service requirements (driven by Land Mobile Radio (LMR) network requirements for packet loss, jitter, and

latency). In 2006, the Defense Information Systems Agency (DISA) ordered the installation of PSNet circuits. Two firms were selected: AT&T for Multiprotocol Layer Switching and Verizon for point-to-point communications (supporting ELMR). The PSNet evolution included PSNet 1.0, in August 2007, and PSNet 2.0, in August 2008. PSNet 1.0 was a closed network without any external connections. PSNet 2.0 implemented Non-Classified Internet Protocol Router Network (NIPRNet) connections. An Authority to Operate (ATO) was issued in May 2013 and a migration to the Defense Information Systems Network (DISN) Defense Security Service Wide Area Network followed, which is the current state.

Within the Continental United States (CONUS) are five Regional Dispatch Centers (RDCs) or Regional Operations Centers (ROCs): Northwest RDC, Southwest RDC/ROC, Midwest ROC, Mid-Atlantic ROC, and Southeast RDC/ROC. The RDC is the Public Safety Answering Point (PSAP) for that region. At the present time, each region is independent. Each region uses Northrop Grumman Command Point CAD software. Although the capability is present, PSAP-to-PSAP communications do not occur.

The ROC serves as the civilian analog of an Emergency Operations Center, providing situational awareness to an echelon above RDC. The ROC uses the C4I Suite software for situational awareness (see IDA document D-8388 for a description of C4I Suite)⁸ and provides video feeds. The ROC also has access to the Emergency Management Network. Both types of centers use a central data bus connection to a PSNet Point of Presence (POP) for access to the PSNet cloud. Figure 2-1 illustrates the RDC connection to PSNet.

Both types of centers exist outside of CONUS (Europe, Hawaii, Japan, Joint Region Marianas – Guam) but they are outside the scope of this analysis. In addition to the RDCs and ROCs, two Service Delivery Points (San Diego, California, and Norfolk, Virginia) are used as hot data backups.

⁸ IDA Document D-8388, *A Survey of Mass Warning and Notification Systems*, S. Chan et al, March 2017.

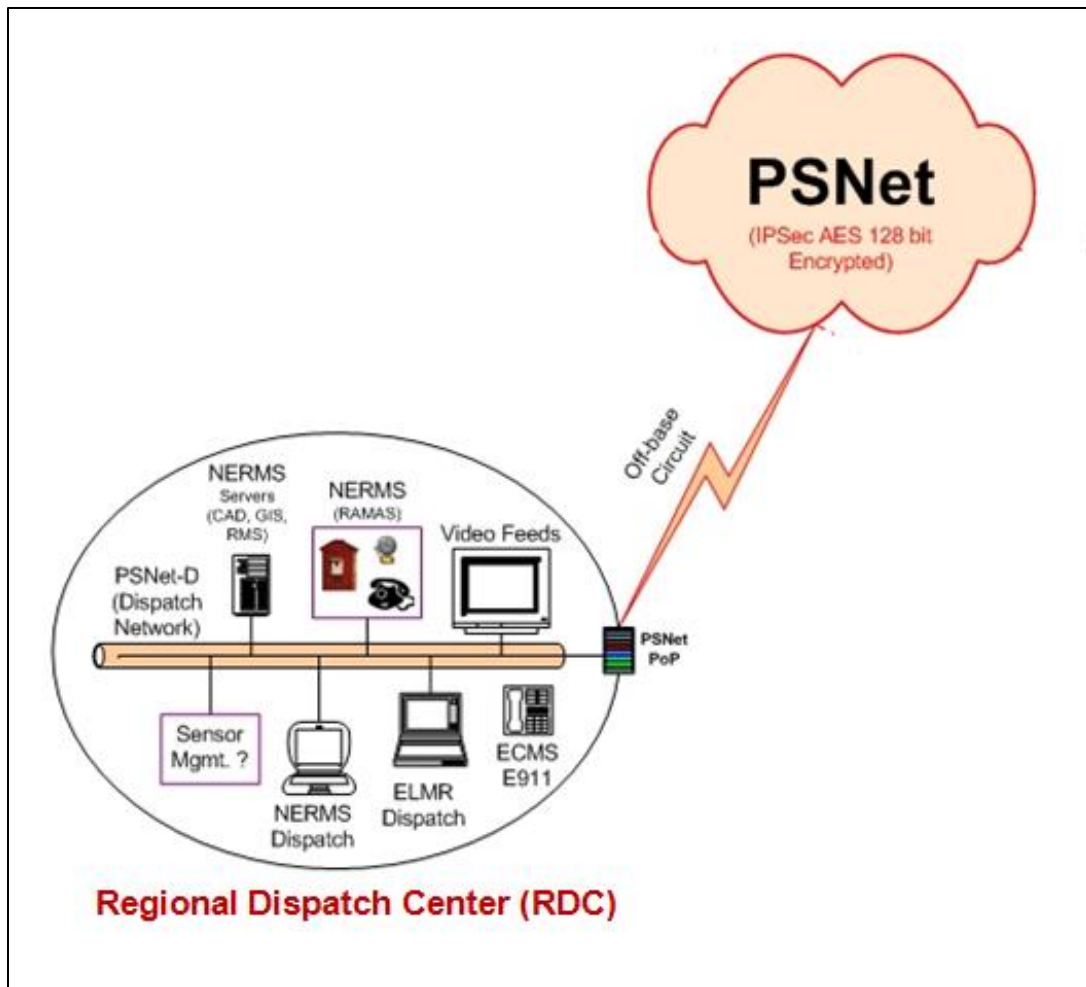


Figure 2-1. PSNet Regional Dispatch Center

2. Interoperability Path

The RDC is typically connected to multiple USN/U.S. Marine Corps bases via the PSNet and its functionality can support CAD, Geographic Information System (GIS), Records Management System (RMS), video feeds, Enhanced Crisis Management System (ECMS), Enhanced 911, and ELMR dispatch. A single bus connects the terminals and consoles with a PSNet POP providing connectivity.

Connectivity between the RDC and the remote bases is through the PSNet cloud, which currently employs an Advanced Encryption Standard 128 bit encryption. A PSNet POP is employed at each base to enable local circuit connections to the Regional Centers.

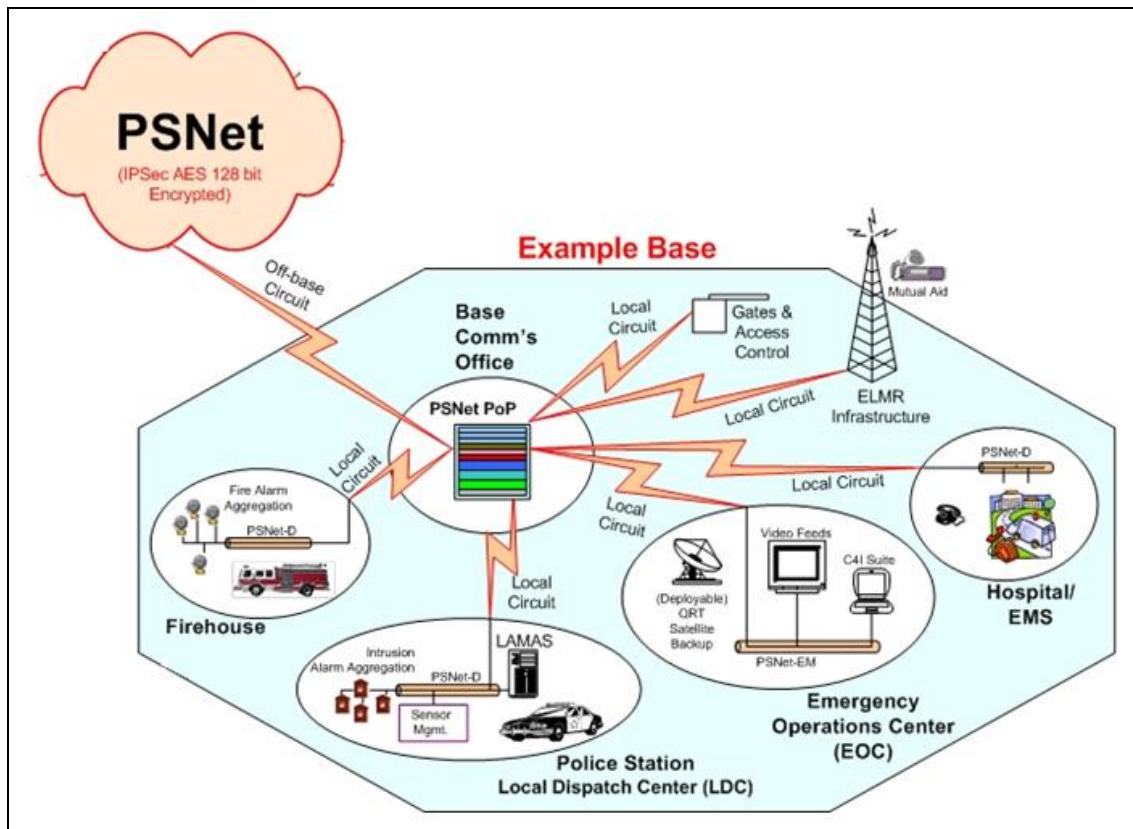


Figure 2-2. Example Base Architecture

In the example base architecture given in Figure 2-2, the Firehouse, Police Station/local dispatch center, Emergency Operations Center, Hospital/EMS, ELMR Infrastructure, Gates and Access Control, and mutual aid resources outside the fence are all represented. Note that the Location and Movement Analysis System (LAMAS) may be available at some police stations.

The USN's regional architecture does not address interoperability with local civilian emergency services. See Figure 2-9 for an example of a naval facility (Naval Station Great Lakes), which is located in Lake County but does not interoperate with adjoining jurisdictions. It is unknown whether interfaces with adjoining civilian jurisdictions and agencies will be implemented or whether they will all simply remain independent.

B. Case Study B: Charleston County, South Carolina, and Joint Base Charleston

1. Context

Charleston County, South Carolina, is located along the Atlantic coast. As of the 2010 census, its population was 350,209, making it the third most populous county in South Carolina. Immediately to the north and contiguous is Berkeley County. As of the 2010 census, Berkeley County's population was 177,843. Joint Base Charleston is a United States military facility located partly in the City of North Charleston, South Carolina, and partly in the City of Goose Creek, South Carolina. The facility is under the jurisdiction of the United States Air Force (USAF) 628th Air Base Wing, Air Mobility Command. The facility is an amalgamation of the USAF Charleston Air Force Base and the United States Navy's Naval Support Activity Charleston (which were merged as a Joint Base on October 1, 2010). It is illuminating to note that not only does the Joint Base (JB) Charleston response area overlap into two counties (Charleston and Berkeley) but the Charleston County Response area also overlaps into two other counties (Dorchester and Berkeley).

A joint civil–military airport, JB Charleston shares runways with Charleston International Airport for commercial airline operations on the south side of the airfield and general aviation aircraft operations on the east side. North Charleston is located within Charleston County, and Goose Creek is located within Berkeley County. The Naval Weapons Station Charleston and the 841st Transportation Battalion, Charleston are located in Berkeley County.

The geography is a bit complex, so a graphical representation of the tri-county area and the JB Charleston response area is given as Figure 2-3.

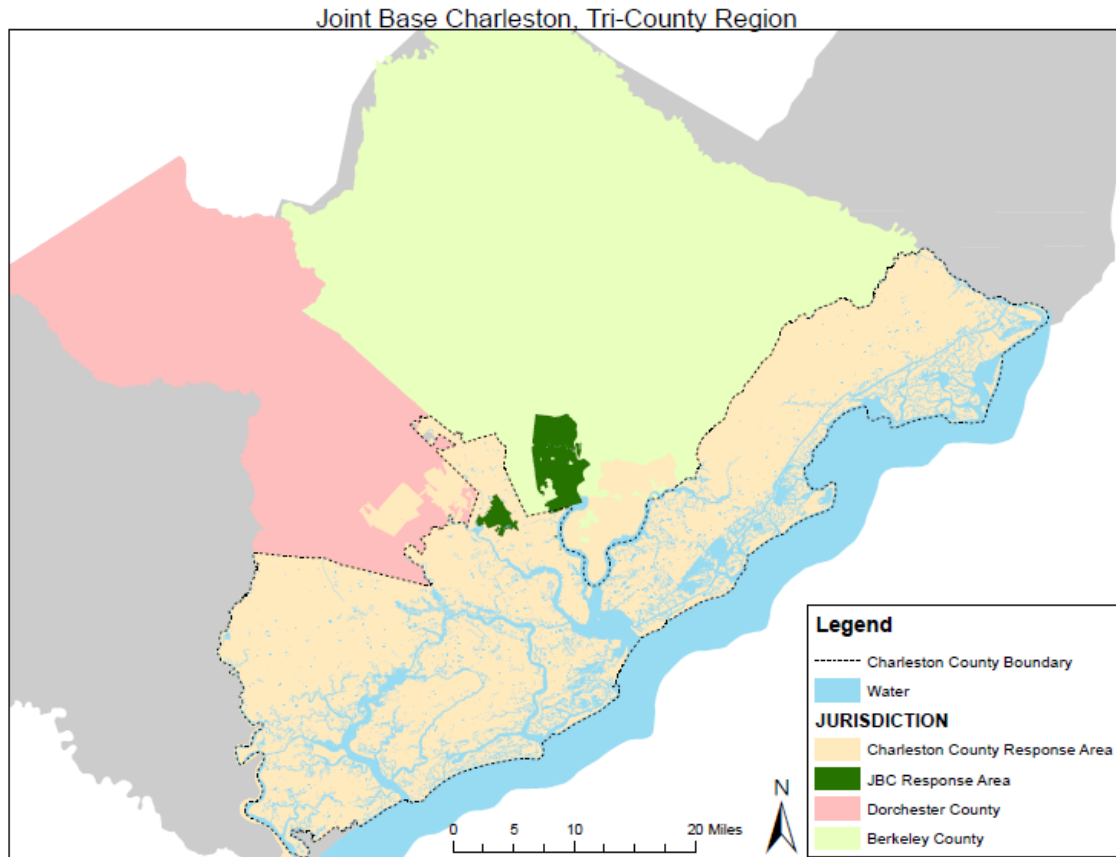


Figure 2-3. JB Charleston and the Tri-County Area

The Fort Hood shooting was the event that initiated the consolidation described below.⁹ At that time, USAF Lt. Col. Warren Brainard, Commander of the 628th Security Forces Squadron (Lt. Col. Clouse is now the Commander) initiated the conversation as part of his goal to increase information sharing and communication. Lt. Col. Brainard believed that the USAF was exceptional at performing their missions, however, 9-1-1 services are not what the USAF typically provides. He thought that these services should be handled by professional 9-1-1 communicators. From its beginnings, this consolidation evolved into the current project.

A Memorandum of Agreement (MOA) between Charleston County and Joint Base Charleston (JB CHS) to establish shared services, including the transition of an Enhanced 9-1-1 Primary Public Safety Answering Point (PSAP), was signed on February 17, 2017. The emergency call situation prior to implementing the terms of the MOA was not optimal since JB CHS could receive only wire line (land line) 9-1-1 calls. Other modes of communication, e.g., wireless and text, were routed to the Charleston County Consolidated

⁹ On November 5, 2009, a mass shooting took place at Fort Hood, near Killeen, Texas. Thirteen persons were killed and more than 30 injured.

Dispatch Center (CDC) or, depending upon the location of origin, to Berkeley County 9-1-1 operators.

In implementing the MOA, the PSAP functions and responsibilities of the JB CHS transferred to the CDC PSAP. The CDC PSAP was designated and authorized to receive emergency 9-1-1 calls requesting public safety services (e.g., law enforcement, fire, medical, etc.) placed within the jurisdiction of JB CHS, including areas of JB CHS located within both Charleston and Berkeley Counties. Specifically excluded from this transition were the dispatch functions of JB CHS fire emergency services and Security Forces. These remained with the JB CHS Emergency Communications Center (ECC).

2. Interoperability Path

Just prior to consolidation, the participating agencies owned five different CAD systems. Three of the five were Tier 1 systems. (Note: tiers are roughly based on the population served. Tier 1 systems generally serve 250,000 to 2 million individuals, Tier 2 systems serve fewer than 250,000 individuals, and if used, Tier 0 systems serve over 2 million individuals.) The County decided that it would first examine existing systems to determine whether any one system was suitable. Three CAD systems were subsequently evaluated: TriTech, Smart Public Safety Software, and VisionAIR. A consulting firm was used to assist in the decision-making process. The factors examined were installation timeline, cost, ability to interface to existing applications, training, and mobile data capability. After a five-month evaluation period, the results were presented to the Consolidated Dispatch Board. Their decision was to continue using TriTech CAD and to “rebuild” it to meet the needs of the consolidated agencies. The TriTech CAD system was already being used by Charleston County EMS Dispatch for EMS and some small Fire Agencies. It was rebuilt to meet the needs of Law Enforcement and the consolidation of agencies. Section 3 shows the task listing used in the evaluation.

There are four sites: Site #1 is the Charleston County Consolidated 9-1-1 Center (with both a primary and backup server), Site # 2 is a backup Center (a backup server), Site #3 is located at the JB CHS primary location, and Site #4 is located at the JB CHS backup location.

AT&T is the Local Exchange Carrier in Charleston County. The County maintains a Master Agreement Contract, which allows the County to purchase services directly from AT&T. As the primary provider of network services in the area and with the associated ability to provide Smart-Ring Diverse Technology, AT&T was chosen to provide an interagency network, which enables multi-jurisdiction communications. Consequently an AT&T Switched Ethernet Service (ASE) was implemented as the Charleston County Interagency Network, configured with secure, encrypted 10 Mbps (megabits per second) capacity links. Routers and firewalls are installed at each side of a connection. The network connects the CDC to JB CHS and to all law, fire, and EMS agencies in Charleston County.

The complete interagency network architecture is shown in Figure 2-4. Currently in the planning stages are connections to other agencies outside of Charleston County (e.g., Berkeley County). In addition, Advanced Technology International's ALASTAR system was selected to support information sharing and situational awareness. The ALASTAR software provides a common operational picture incorporating real-time inputs (e.g., 9-1-1 calls, automatic vehicle location, weather, infrastructure status, and video feeds).

The administration of the CAD and GIS systems is provided by the Charleston 9-1-1 CDC. The CDC staff also provides training for JB CHS dispatch center personnel. The base commander has a requirement for logging all calls that base security receives. This activity is currently not integrated into the CAD system.

The flow of calls originating in the JB CHS response area has been consolidated, and all wireline 9-1-1, wireless 9-1-1, and text-to-911 calls are routed to the CDC. The CDC call taker receiving a call uses the Priority Dispatch Protocol software to question the caller. The Priority Dispatch protocol software is interfaced to the TriTech CAD system so that the call taker has to enter the information only once. If the location of the incident is within the JB CHS response area, then the initial incident report will be sent to the JB CHS TriTech CAD system via the AT&T ASE connection. If a medical incident occurs within the boundary of the JB CHS response area and in the jurisdiction of Berkeley County, the CDC will communicate the incident information to JB CHS via TriTech CAD and call the Berkeley County dispatch center. If a medical incident occurs within the boundaries of the JB CHS response area and the jurisdiction of Charleston County, a Charleston County EMS response will be generated by the CDC at the same time that JB CHS is notified via the TriTech CAD.

The Charleston County Call and Incident Volumes for 2016 are listed in Table 2-1. The Performance Metrics and Standards for the CDC as of June 30, 2017, are listed in Table 2-2. Note the references to the National Emergency Number Association (NENA), International Academy of Emergency Dispatch (IAED), Emergency Fire Dispatch (EFD), Emergency Medical Dispatch (EMD), and National Fire Protection Act (NFPA) standards.

Table 2-1. Call and Incident Volumes

Call and Incident Volumes	Totals For 2016
9-1-1 Wireline and Wireless Calls	327,643
Seven-digit Inbound Calls	396,821
Seven-digit Outbound Calls	312,346
Total Call Volumes	1,036,810
EMS/Fire/Rescue Incidents	73,445
Law Incidents	763,397
Total Incident Volumes	836,842

Table 2-2. Metrics and Standards

Metrics and Standards	Quarter Ending 6/30/2017
Answer 90% of Emergency Calls within 10 seconds During Busiest Hour (NENA)	88%
Answer 80% of Emergency Calls within 10 seconds (SC State)	88%
Answer 95% of Emergency Calls Within 15 seconds (NFPA v.2016)	92%
Answer 95% of Emergency Calls Within 20 seconds (NENA)	95%
Answer 99% of Emergency Calls Within 40 seconds (NFPA v.2016)	99%
Fractal Call Processing Time (Call pickup to dispatch) - EMS/Fire/Rescue	
90% in 64 seconds NFPA 7.4.2 (v.2016)	89%
95% in 106 seconds NFPA 7.4.2 (v.2016)	98%
90% in 90 seconds NFPA 7.4.2.2 (v.2016)	89%
99% in 120 seconds NFPA 7.4.2.2 (v.2016)	96%
Call Taker Average Quality Assurance Score for EFD (IAED)	99%
Call Taker Average Quality Assurance Score for EMD (IAED)	100%

A comprehensive Listing of Consolidated 9-1-1 Center Personnel, Agencies Served, Information and Technology Sharing, and Training appears in the next section.



3. Charleston CAD Vendor Selection Task List

The following pages show the planned effort to implement CAD interoperability at Charleston. “Rip and Run” refers to the generation of a written (printed) emergency response report.

MSProj11		
ID	Task Name	Duration
1	Charleston SC CAD Analysis	9 days
2	On-site analysis requirements	1 day
3	Review Agency background and analysis data	1 day
4	Review available analysis data and reports	8 hrs
5	Create Schedule based on task list and Client feedback	6 hrs
6	Collect call volume data for hardware sizing	8 hrs
7	Determine RMS interface requirements of all agencies	4 hrs
8	Review CAD functionality requirements	0.38 days
9	Tritech	0.38 days
10	Mandatory Functionality	2 hrs
11	Set-up requirements for mandatory functionality	0.38 days
12	Time	0.5 hrs
13	File Structure	3 hrs
14	Map Integration/Linking requirements	1 hr
15	Available Modules	1 hr
16	Numbering requirements	0.5 hrs
17	Smart Public Safety Software	0.38 days
18	Mandatory Functionality	2 hrs
19	Set-up requirements for mandatory functionality	0.38 days
20	Time	0.5 hrs
21	File Structure	3 hrs
22	Map Integration/Linking requirements	1 hr
23	Available Modules	1 hr
24	Numbering requirements	0.5 hrs
25	VisionAIR	0.38 days
26	Mandatory Functionality	2 hrs
27	Set-up requirements for mandatory functionality	0.38 days
28	Time	0.5 hrs
29	File Structure	3 hrs
30	Map Integration/Linking requirements	1 hr
31	Available Modules	1 hr
32	Numbering requirements	0.5 hrs
33	Determine CAD Interface requirements	0.25 days
34	Tritech	0.25 days
35	CAD to ancilliary systems and hardware	0.06 days
36	Mobile	0.5 hrs
37	Toning	0.25 hrs
38	Radio Systems Interfacing	0.25 hrs
39	Paging	0.25 hrs
40	Rip and Run	0.5 hrs
41	Logging Recorder	0.25 hrs
42	NCIC	0.25 hrs
43	Emergency Medical dispatch software	0.25 hrs
44	Mapping/GIS	0.5 hrs
45	CAD to RMS	0.5 hrs
46	CAD to Other Systems	0.25 days
47	EOC software/processes	0.25 hrs
48	Data Sharing (CAD neutral)	0.25 hrs
49	Other (i.e. Towing, 'Shot Spotter', etc)	2 hrs
50	Smart Public Safety Software	0.25 days
51	CAD to ancilliary systems and hardware	0.06 days
52	Mobile	0.5 hrs
53	Toning	0.25 hrs
54	Radio Systems Interfacing	0.25 hrs
55	Paging	0.25 hrs
56	Rip and Run	0.5 hrs
57	Logging Recorder	0.25 hrs
58	NCIC	0.25 hrs
59	Emergency Medical dispatch software	0.25 hrs
60	Mapping/GIS	0.5 hrs
61	CAD to RMS	0.5 hrs
62	CAD to Other Systems	0.25 days
63	EOC software/processes	0.25 hrs
64	Data Sharing (CAD neutral)	0.25 hrs
65	Other (i.e. Towing, 'Shot Spotter', etc)	2 hrs
66	VisionAIR	0.25 days

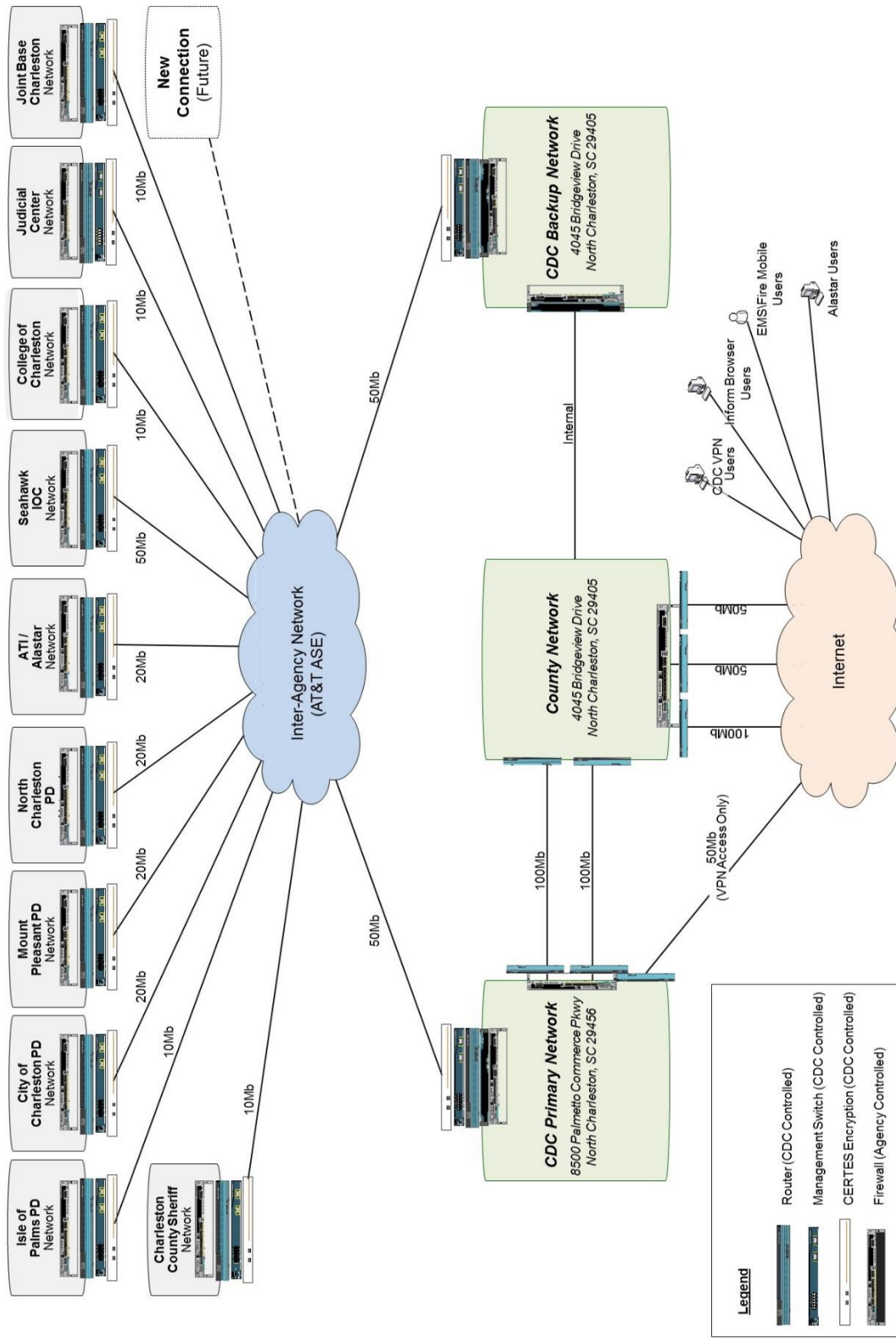
MSProj11		
ID	Task Name	Duration
67	CAD to ancilliary systems and hardware	0.06 days
68	Mobile	0.5 hrs
69	Toning	0.25 hrs
70	Radio Systems Interfacing	0.25 hrs
71	Paging	0.25 hrs
72	Rip and Run	0.5 hrs
73	Logging Recorder	0.25 hrs
74	NCIC	0.25 hrs
75	Emergency Medical dispatch software	0.25 hrs
76	Mapping/GIS	0.5 hrs
77	CAD to RMS	0.5 hrs
78	CAD to Other Systems	0.25 days
79	EOC software/processes	0.25 hrs
80	Data Sharing (CAD neutral)	0.25 hrs
81	Other (i.e. Towing, 'Shot Spotter', etc)	2 hrs
82	Determine Data Conversion requirements	0.06 days
83	Tritech	0.06 days
84	Rolodex/Contact information	0.25 hrs
85	CAD Incident data	0.5 hrs
86	Location/Hazard Alert information	0.25 hrs
87	Master Name Index	0.25 hrs
88	Unit data	0.25 hrs
89	Run Card data	0.25 hrs
90	Personnel data	0.25 hrs
91	Other	0.5 hrs
92	Smart Public Safety Software	0.06 days
93	Rolodex/Contact information	0.25 hrs
94	CAD Incident data	0.5 hrs
95	Location/Hazard Alert information	0.25 hrs
96	Master Name Index	0.25 hrs
97	Unit data	0.25 hrs
98	Run Card data	0.25 hrs
99	Personnel data	0.25 hrs
100	Other	0.5 hrs
101	VisionAIR	0.06 days
102	Rolodex/Contact information	0.25 hrs
103	CAD Incident data	0.5 hrs
104	Location/Hazard Alert information	0.25 hrs
105	Master Name Index	0.25 hrs
106	Unit data	0.25 hrs
107	Run Card data	0.25 hrs
108	Personnel data	0.25 hrs
109	Other	0.5 hrs
110	CAD System Hardware requirements	0.13 days
111	Tritech	0.13 days
112	Platform	0.25 hrs
113	Hardware scaling analysis	1 hr
114	Future Viability	0.25 hrs
115	Licensing mechanism	0.25 hrs
116	Technical Support availability/preference	0.25 hrs
117	Smart Public Safety Software	0.13 days
118	Platform	0.25 hrs
119	Hardware scaling analysis	1 hr
120	Future Viability	0.25 hrs
121	Licensing mechanism	0.25 hrs
122	Technical Support availability/preference	0.25 hrs
123	VisionAIR	0.13 days
124	Platform	0.25 hrs
125	Hardware scaling analysis	1 hr
126	Future Viability	0.25 hrs
127	Licensing mechanism	0.25 hrs
128	Technical Support availability/preference	0.25 hrs
129	Client/Project Assumptions Definition and Signoff	2 hrs
130	CAD Vendor analysis requirements	1 day
131	Collect Vendor data	1 day
132	Tritech	1 day

MSPProj11			
ID	Task Name	Duration	
133	Contact information	0.5 hrs	
134	Customer/Reference information	4 hrs	
135	Company profile	0.5 days	
136	History	4 hrs	
137	Standing	2 hrs	
138	Financial	2 hrs	
139	Vendor market research	8 hrs	
140	Smart Public Safety Software	1 day	
141	Contact information	0.5 hrs	
142	Customer/Reference information	4 hrs	
143	Company profile	0.5 days	
144	History	4 hrs	
145	Standing	2 hrs	
146	Financial	2 hrs	
147	Vendor market research	8 hrs	
148	VisionAIR	1 day	
149	Contact information	0.5 hrs	
150	Customer/Reference information	4 hrs	
151	Company profile	0.5 days	
152	History	4 hrs	
153	Standing	2 hrs	
154	Financial	2 hrs	
155	Vendor market research	8 hrs	
156	Research Vendor capabilities	0.5 days	
157	Tritech	0.5 days	
158	Determine ability to meet functional requirements & cross comparison and anal	4 hrs	
159	Determine prior history of similar projects & cross comparison and analysis	4 hrs	
160	Determine data conversion history & cross comparison and analysis	0.13 days	
161	Interview vendor/technical staff	1 hr	
162	Check vendor references	1 hr	
163	Determine vendor interface capability & cross comparison and analysis	0.25 days	
164	Interview vendor/technical staff	2 hrs	
165	Check vendor references	1 hr	
166	Determine vendor multi-jurisdictional capabilities & cross comparison an	0.25 days	
167	Interview vendor/technical staff	2 hrs	
168	Check vendor references and market perception	1 hr	
169	Determine vendor commitment to facilitate process & cross comparison a	0.25 days	
170	Interview vendor/technical staff	1 hr	
171	Price quote (vendor)	1 hr	
172	Schedule estimate (vendor)	1 hr	
173	Training estimate (vendor/Kimball)	2 hrs	
174	Migration plan (vendor)	1 hr	
175	Smart Public Safety Software	0.5 days	
176	Determine ability to meet functional requirements & cross comparison analysis	4 hrs	
177	Determine prior history of similar projects & cross comparison and analysis	4 hrs	
178	Determine data conversion history & cross comparison and analysis	0.13 days	
179	Interview vendor/technical staff	1 hr	
180	Check vendor references	1 hr	
181	Determine vendor interface capability & cross comparison and analysis	0.25 days	
182	Interview vendor/technical staff	2 hrs	
183	Check vendor references	1 hr	
184	Determine vendor multi-jurisdictional capabilities & cross comparison an	0.25 days	
185	Interview vendor/technical staff	2 hrs	
186	Check vendor references and market perception	1 hr	
187	Determine vendor commitment to facilitate process & cross comparison a	0.25 days	
188	Interview vendor/technical staff	1 hr	
189	Price quote (vendor)	1 hr	
190	Schedule estimate (vendor)	1 hr	
191	Training estimate (vendor/Kimball)	2 hrs	
192	Migration plan (vendor)	1 hr	
193	VisionAIR	0.5 days	
194	Determine ability to meet functional requirements & cross comparison and anal	4 hrs	
195	Determine prior history of similar projects & cross comparison and analysis	4 hrs	
196	Determine data conversion history & cross comparison and analysis	0.13 days	
197	Interview vendor/technical staff	1 hr	
198	Check vendor references	1 hr	

MSProj11			
ID		Task Name	Duration
199		Determine vendor interface capability & cross comparison and analysis	0.25 days
200		Interview vendor/technical staff	2 hrs
201		Check vendor references	1 hr
202		Determine vendor multi-jurisdictional capabilities & cross comparison an	0.25 days
203		Interview vendor/technical staff	2 hrs
204		Check vendor references and market perception	1 hr
205		Determine vendor commitment to facilitate process & cross comparison a	0.25 days
206		Interview vendor/technical staff	1 hr
207		Price quote (vendor)	1 hr
208		Schedule estimate (vendor)	1 hr
209		Training estimate (vendor/Kimball)	2 hrs
210		Migration plan (vendor)	1 hr
211		Analysis and Recommendation	9 days
212		Analyze data from all data collection activities	40 hrs
213		Review findings with Charleston Stakeholders	8 hrs
214		Create final recommendation	24 hrs

4. Interagency Network Diagram

Figure 2-4, on the following page, is a diagram of the Charleston interagency network.



Charleston County Consolidated Dispatch Center (CDC)
Inter-Agency & Internet Network Connectivity
(Current as of 09/19/2017)

This document is the property of Charleston County Consolidated Dispatch Center. Any reproduction, distribution or modification without the consent of Charleston County Consolidated Dispatch Management is strictly prohibited. For further information about this document, you may contact (843) 529-3710.

Figure 2-4. Charleston Interagency Network Diagram

5. Charleston 9-1-1 Center Details

Table 2-3 shows the number of employees at the Charleston County 9-1-1 center.

a. Employees

Table 2-3. Charleston Personnel Titles and Numbers of Employees

Department Personnel	Current Number of Employees
Management (Director & Deputy Director)	2
Managers (Operations, Support, Administrative, IT)	4
Project Coordinator	1
Call-takers	40
Law Enforcement Dispatchers	40
EMS/Fire/Rescue Dispatchers	20
Multi-Function Telecommunicators	17
Administrative Call Takers	6
Shift Supervisors	12
Floor Supervisors	4
Training Coordinator	1.5
Quality Assurance Supervisor & Technicians	4
IT Supervisors	2
IT Staff (Geographic Information Systems, Mobile Data, Computer Aided Dispatch, Records Management, Telephony, Computer Technician)	6
Public Education	1.5
Support (Recordings, Accreditation, NCIC Terminal Agency Coordinator)	4
Administrative (Assistants, Recruiter, Accountant, Grants, Human Resources, Research)	7.0
Total Personnel	172.0

b. Agencies Served

The agencies served are listed in this subsection. First, the Consolidated 9-1-1 Center takes emergency and non-emergency calls for service and/or dispatches for:

- 10 Law Enforcement Agencies,
- 13 Fire Agencies,
- 1 EMS Agency,
- 1 Emergency Management Agency.

The following are agencies served by discipline and name:

Law Agencies:

- Charleston County Sheriff's Office,
- Charleston County Coroner's Office,
- Charleston County Solicitor's Office,
- City of Charleston Police Department,
- Isle of Palms Police Department,
- Joint Base Charleston Security Forces,
- Mount Pleasant Police Department,
- National Park Service,
- North Charleston Police Department,
- Sullivan's Island Police Department.

Fire Departments:

- Awendaw Fire District,
- Charleston County Rescue Squad,
- City of Charleston Fire Department,
- Isle of Palms Fire Department,
- James Island Fire District,
- Joint Base Charleston Fire,
- Lincolnville Fire & Rescue,
- Mount Pleasant Fire Department,
- North Charleston Fire Department,
- St Andrews Fire District,
- St John's Fire District,
- St Paul's Fire Department,
- Sullivan's Island Fire Department.

Medical Services:

- Charleston County EMS.

Emergency Management:

- Charleston County Emergency Management.

c. Information & Technology Sharing

The Consolidated 9-1-1 Center shares information and technology with the following agencies:

- U.S. Coast Guard,
- DHS Seahawk IOC,
- College of Charleston Public Safety,
- Charleston County Parks & Recreation Commission,
- State Law Enforcement Division,
- Department of Natural Resources,
- South Carolina Department of Health and Environmental Control (DHEC).

d. Training

The classroom training period lasts approximately 12 weeks and includes scenario-based practice sessions. Trainees then move to the 9-1-1 Center under the training of a Certified Training Officer for approximately 8 to 12 weeks of practical application and learning.

The Telecommunicators hold the following certifications:

- International Academies of Emergency Dispatch Emergency Telecommunicator Certification,
- International Academies of Emergency Dispatch Emergency Fire Dispatch Certification,
- International Academies of Emergency Dispatch Emergency Medical Dispatch Certification,
- International Academies of Emergency Dispatch Emergency Police Dispatch Certification,
- National Crime Information Center Certification,
- Cardio-Pulmonary Resuscitation Certification,
- National Incident Management System Incident Command System 100,
- National Incident Management System Incident Command System 200,
- National Incident Management System Incident Command System 700,

- National Incident Management System Incident Command System 800,
- National Center for Missing and Exploited Children Amber Alert Certification,
- Federal Emergency Management Agency Active Assailant-907,
- Department of Homeland Security Suspicious Activity Reporting.

C. Case Study C: National Capitol Region Fire and EMS Interoperable Communications

1. Context

Geographically, the National Capital Region (NCR) was defined by the National Capital Region Planning Act of 1952 as the District of Columbia, two Maryland counties, and four Virginia counties. The Maryland components are Montgomery and Prince George's counties, and the municipalities of Bowie, College Park, Gaithersburg, Greenbelt, Rockville, and Takoma Park. In Virginia, Arlington, Fairfax, Loudon, and Prince William counties are included, as are the cities of Alexandria, Fairfax, Falls Church, Manassas, and Manassas Park. The Washington metropolitan area is one of the most educated and most affluent metropolitan areas in the United States. The metro area anchors the southern end of the densely populated Northeast megalopolis, with an estimated total population of 6,097,684 as of the 2014 U.S. census.

This case study provides an overview of the NCR Interoperability Communications Infrastructure (ICI) program and how it has evolved to support Fire and EMS cooperation and communications.

In the period following 9/11, the local jurisdictions in the NCR came together to address the severe interoperability issues that had become apparent in the public safety response following that tragedy. The jurisdictions developed a vision for a crucial new public safety communications network to connect community leaders and first responders across the NCR. The goal of the newly envisioned NCR Interoperability Program (NCRIP) was to enhance the region's public safety and emergency response communications and systems interoperability through the establishment of a new fiber optic digital network. Through the NCRIP, the region applied for funding from the Department of Homeland Security (DHS). Funding was awarded and NCRnet—a collaborative work of 19 jurisdictions—was begun.

Designed and deployed with a range of innovative digital networking technologies and IT security measures, NCRnet represents one of the most sophisticated approaches to regional interoperability currently in use in the United States. In 2005, the NCRIP assessed requirements for the network and piloted an initial interconnection between the District of Columbia and Montgomery County, Maryland. The needs assessment demonstrated

conclusively that local first responders and emergency support personnel needed a secure, reliable, regional communications infrastructure—in particular, regional video streaming and videoconferencing, applications that can best be supported over fiber optics.

The assessment established a number of design principles in consultation with stakeholders and on the basis of the needs assessment results. Among these are:

- The ability to support a diverse community of potential users (first responders, public health, local, state, federal government, education) without conflict between the users;
- A robust, scalable, survivable network infrastructure that connects with each participant's own fiber optic network;
- The need to operate independently of leased carrier infrastructure, the Internet, the public switched telephone network, and the Intergovernmental Network (I-Net) electronics of individual jurisdictions;
- The ability to interface with different network devices, models, and brands used by jurisdictions, using industry best practices and federal communications and security standards; and
- A platform for real-time interoperable data exchange between different users regardless of native applications and formats.

These design principles ensured not only that the developing network fulfilled regional needs but that this would be achieved in a cost-effective manner.

Local government internets and various agreements for access to fiber optic cable are enormously valuable resources in designing a cost-effective, inter-jurisdictional, fiber-optic network. While some of the governing agreements underlying the I-Nets restrict the use of fiber, acceptable use is defined in a manner consistent with public safety usage.

I-Nets are well suited to public safety communications. Their independence from commercial carrier lines ensures a survivable network when commercial options are saturated. In addition, local government control allows flexible network design and end-to-end risk and security management.

Previous work developing many of the jurisdictions' I-Nets formed the basis for NCRnet due to spare fiber in existing I-Nets and provisions for rack space at potential hub sites, which allowed NCRnet to re-use existing assets. In addition, the NCR jurisdictions' agreements with cable providers typically had provisions for building out and extending I-Net footprints at advantageous cost (often to the mutual benefit of government and cable providers).

The NCRnet was designed for flexibility and local control. Its flexibility reduced the need for future redesign or complicated network governance. The current implementation

treats NCRnet as a “semi-trusted cloud”—a private intranet. Jurisdictions protect themselves with a firewall, and manage communications into their own networks with an extranet router. On the NCRnet side of the demarcation sits an edge router that handles traffic within the NCRnet cloud. NCRnet monitors only the equipment on its side of the demarcation, while the jurisdictions are responsible for the equipment that controls access within their own networks.

The NCRnet project, now part of NCR Interoperable Communications Infrastructure (ICI), provides network infrastructure to the participant jurisdictions to enable secure, non-commercial, local government-controlled access to Regional Systems and Applications. NCRnet was created to enhance Emergency Support Functions (ESFs) ability to succeed in their mission of building and sustaining an integrated effort to prepare for, prevent, protect against, respond to, and recover from all-hazards, threats, and events.

The NCR ICI, is led by the Metropolitan Washington Council of Governments (MWCOG) Chief Information Officer (CIO) Committee. Founded in 1957, the MWCOG is a regional organization of 21 Washington-area local governments, as well as area members of the Maryland and Virginia state legislatures, the U.S. Senate, and the U.S. House of Representatives. The MWCOG provides a forum for discussion and the development of regional responses to issues regarding the environment, transportation, public safety, homeland security, affordable housing, community planning, and economic development.

The NCR ICI established a foundational communications infrastructure that leverages the assets of the local governments and NCR partners. It follows established and regionally approved guidelines, standards, policies, and procedures, and it is compliant with National Information Exchange Model (NIEM) and National Institute of Standards and Technology (NIST) standards.

2. Interoperability Path

The Core Components of the NCR ICI include:

- NCRnet – Physical, fiber network interconnection of local I-Nets and other private network infrastructures.
- Data Exchange Hub (DEH) – A central hub comprising servers, exchange service software, and standards and policies that facilitates the authorized enablement of exchange and use of data between partners and supports specific interoperability goals. Applications are developed as directed by sponsors such as for CAD-to-CAD (CAD2CAD).
- Government Data Exchange (GDX) – Interconnection of spatial data assets of the NCR partners’ Geographic Information Systems (GIS) databases that allows

discovery, authorized access, and sharing of real-time GIS data regardless of a participating entity's GIS platform.

- NCR Identity and Access Management Service (IAMS) – Enables trusted access authentication using NCR partner entity credentials for gaining access to participating regional applications.

a. National Capital Region Network

NCRnet is a private, high-speed network that interconnects MWCOG jurisdictions and other entities. It provides a secure, critical communications infrastructure that can support secure voice, data, and video transmission supporting emergency response functions. NCRnet is not dependent on independent commercial service-provider networks across the states.

NCRnet has been operational since 2005. It is a resilient carrier-class network using state-of-the-art equipment and fiber optics. It is redundant including three geographically distinct Potomac River crossings. It has (as of early 2017) approximately 70 network devices (routers and switches) that transmit at high speed (10GB/s). It connects to a secure commercial third-party data center host for regional applications. Operation policies, agreements, and procedures are in place, and they have all been published. NCRnet has maintained minimum uptime performance of 99.9% during this time. Its design uses existing jurisdictional I-Nets; thus it reduces regional costs overhead by eliminating the need to lease independent, commercial communications services.

All MWCOG jurisdictions/entities connect to NCRnet. Metropolitan Washington Airports Authority (MWAA), MWCOG, Virginia Department of Transportation (VDOT), Washington Metropolitan Area Transit Authority (WMATA), and Washington Suburban Sanitary Commission (WSSC) all connect to NCRnet. NCRnet also pairs with networkMaryland¹⁰ and can interconnect with any agencies connected to networkMaryland. Authorized organizations can interconnect through connections with the locality's I-Net.

During the 2017 Presidential Inauguration, the NCR ICI provided NCRnet connectivity for the Federal Bureau of Investigation's Closed Circuit Television (CCTV) network, facilitated by Washington, D.C.'s fiber optic network DC-NET. Many other incident, situational awareness, video-sharing applications, and participants were also active for that inauguration. The NCR link map is shown in Figure 2-5.

¹⁰ networkMaryland is Maryland's statewide high-speed data network for public sector use, operated by the Department of Information Technology.

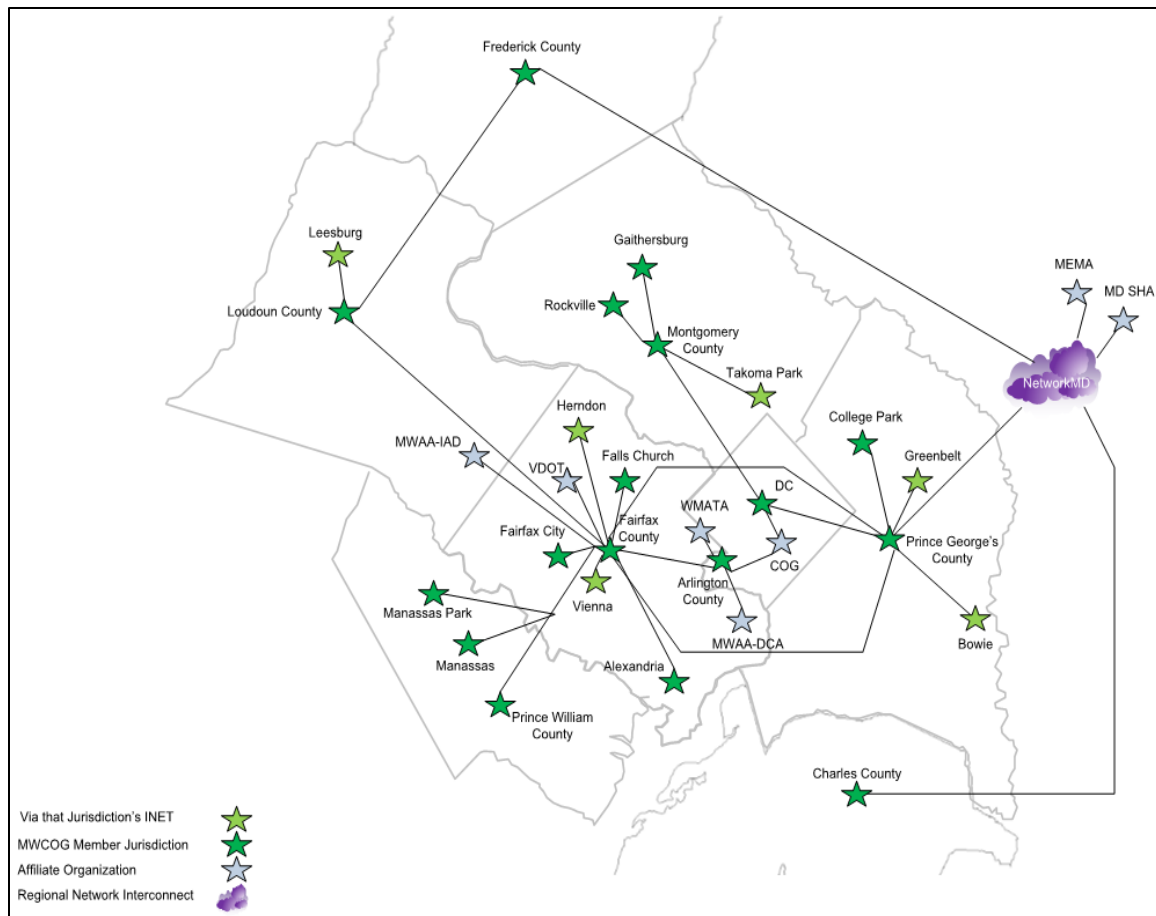


Figure 2-5. NCRnet Link Map

For cybersecurity protection, NCRnet uses sophisticated tools to detect malicious or suspicious traffic, with pre-authorization for staff to take immediate action to avert threats and minimize impact. The advantages of this are:

- It provides insulation from denial of service attacks.
- Exposure to the public Internet is limited.
- No Internet of Things (IoT) devices are connected to NCRnet.
- Users are authenticated (see IAMS, below).
- It can segment data traffic for specific applications as required.

In addition to possessing a high level of security controls, NCRnet maintains independence from commercially switched networks. Companies specialized in IT security practices perform independent security-vulnerability assessments and 24/7 real-time monitoring of the network.

Applications currently transmitting via NCRnet include:

- Automated Fingerprint Identification System (AFIS) – Mobile AFIS, Northern Virginia Regional Identification System (NOVARIS), RAFIS;
- Closed Circuit Television (CCTV): video feed (MView);
- Computer Aided Dispatch (CAD2CAD) Fire and EMS Data Exchange: CAD2CAD unit and incident data;
- Geospatial Data Exchange (GDX) (plus Internet): GIS data integration with local tools;
- Inter RF Subsystem Interface (ISSI) feature (Prince William County and Fairfax County);
- License Plate Reader (LPR): Permits searches across systems;
- MugShots (new version): User interface with single sign-on;
- NCR Situational Dashboard: User access to tool;
- Prince George's Sheriff Warrants (shares with WMATA);
- Video Conferencing System (VTC): video/audio transmission;
- WebEOC Fusion: Backend data communications.

Current Emergency Support Functions (ESFs) in use are:

- ESF-1–Transportation: CCTV;
- ESF-2–Communications: GDX, ISSI feature, DEH;
- ESF-4–Fire: CAD2CAD;
- ESF-5–Emergency Management: Situational Dashboard, VTC, WebEOC;
- ESF-13–Public Safety and Security: AFIS, LPR, Mugshots, PGC's Sheriff Warrants.

The Identity and Access Management Service (IAMS) allows authorized use of local-entity-issued credentials to access regional applications without changing existing architecture or protocols. No special training is needed. It has been operating since June 2013 and was awarded the Commonwealth of Virginia's Information Technology Symposium (COVITS) Governor's Technology Award in 2014. It is available to any authorized local/state/federal employee, or external user.

Application Functionality includes:

- Broker's identity information between jurisdictions and regional applications,
- Users authenticate using locality-managed email addresses/passwords,

- Workflow engine supports application access request/approval process,
- External users can register and request access,
- Self-service portal (<https://getaccess.ncrnet.us>).

The host location for IAMS is a secure commercial hosting provider. It is accessible via both the Internet and NCRnet.

b. Identity and Access Management Service (IAMS)

IAMS has a single sign-on with zero impact to the existing enterprise. It can authenticate end users to applications in less than 5 seconds. It collects metrics about regional public-safety applications use, which allows for better planning. IAMS operates 24/7 with several layers of redundancy. It supports advanced forms of identification as application needs expand. The deployment of IAMS with NCR partners continues.

In Virginia, IAMS is connected to Arlington County, the City of Alexandria, the City of Fairfax, the City of Fairfax Police, the City of Falls Church, the City of Manassas, Fairfax County, Loudoun County, Prince William County, and the Town of Vienna. IAMS is in the process of being connected to the Town of Leesburg, Virginia.

In Maryland, IAMS is connected to the City of Gaithersburg, Frederick County, Montgomery County, and Prince George's County.

IAMS is also connected to MWCOG and Northern Virginia Emergency Response System (NVERS) and Northern Virginia Hospital Alliance (NVHA) (via Google).

The following have been informed: MWAA, District of Columbia, Charles County (MD), and Montgomery Park Police.

In addition, the Federal Government, partners, and other non-profits are integrated with Office of Management and Budget (OMB) MAX and pursuing National Identity Exchange Federation (NIEF) Certification.

What remains to be done is connection to several smaller cities and towns, the Commonwealth of Virginia, and the State of Maryland.

c. Data Exchange Hub (DEH)

In strategic and tactical realities, ESF functions and local partners need a data interoperability architecture to support regional response, mutual aid, and situational awareness. Data Exchange Hub is the answer.

The DEH established guidance, policies, and approaches for data exchange are:

- Avoid non-standard-compliant data exchanges because they require costly, customized interfaces, as well as costly rewriting as connected applications and systems change.
- Adopt a DEH because it allows access to mutually agreed-upon data within independent, proprietary applications.
- Adopt a DEH because it uses non-proprietary approaches to establish data services and contracts between systems that share similar data definitions, including what will be shared and how the sharing is governed.
- Follow Department of Homeland Security (DHS) United States of America Standards Institute (USASI)—now the American National Standards Institute (ANSI)—guidance, which specifies the use of the National Information Exchange Model (NIEM).
- Adopt flexible mechanisms because they are easier to interface with, maintain, and expand as needs and data sources evolve.

Figure 2-6 shows a generic example of four interconnected partner systems.

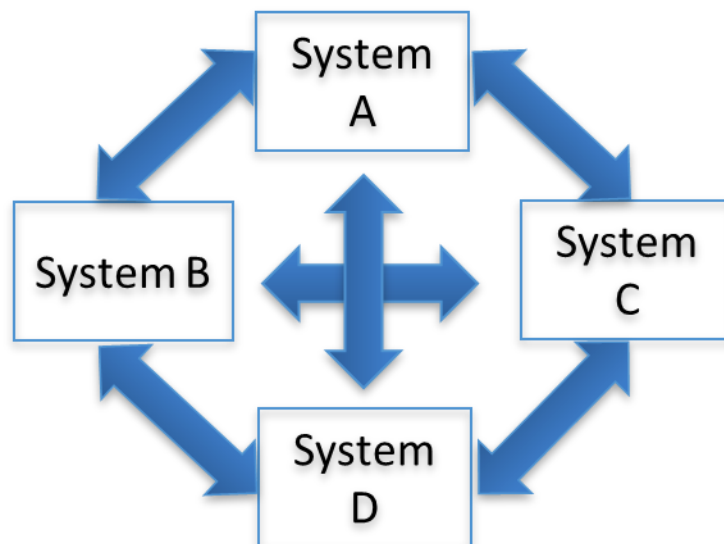


Figure 2-6. Interconnections Required Among Four Partner Systems

Without the DEH:

- Each system maintains three interfaces.
- Adding a new system requires work by all existing systems.
- If one system makes a change, then it ripples through all three of its interfaces.

Figure 2-7 shows how partner systems can interconnect more easily using the DEH. With the DEH:

- One interface is maintained by each system.
- It can scale with new systems.

DEH defines the method, data specification and format (e.g., “how to speak, words and language”), i.e., it translates between “languages.”

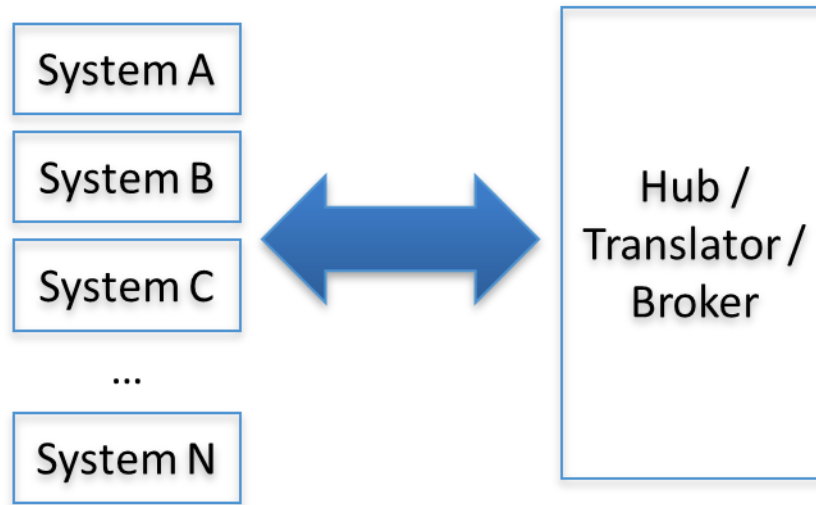


Figure 2-7. Partner System Interconnection Using the DEH

d. CAD2CAD Data Exchange for Fire and EMS

A number of regional systems and applications are currently using NCRnet. The CAD2CAD Data Exchange between Fairfax County, Arlington County, City of Alexandria, and City of Fairfax allows for mutual resource sharing and dispatch between the fire departments of those jurisdictions.

The CAD2CAD data exchange handles real-time resource requests between Computer Aided Dispatch (CAD) systems with unit status/location awareness.

- This enables CAD systems to perform closest unit routing of First Response Disaster (FRD) resources across locality boundaries for daily and catastrophic events.
- It was implemented in 2010, replacing manual phone calls. This results in a near simultaneous dispatch from all jurisdictions, reducing response times by up to 90 seconds.
- It operates exclusively on NCRnet and uses DHS UASI-stipulated NIEM approaches for data exchange.

Data Exchange Hub shares a feed of real-time unit status data with NCR GDX for consumption by situational awareness tools and viewers. Incident Details is a future, planned service.

The Fire CAD2CAD Data Exchange, within the existing dispatcher interface, recommends the closest units and requests units from other jurisdictions in less than 10 seconds. It also maintains awareness of the units and their locations as the event unfolds.

Benefits include: (1) reduction of response time, (2) dispatch of closest unit, (3) situational awareness data is shared, and (4) there is only one interface for each vendor/locality.

However, there are some challenges: (1) differences in fire-fighting operations, (2) differences in data maintenance procedures, and (3) varying quantities of event types and unit status types.

Existing CAD2CAD data exchanges are the Fairfax County CAD, City of Alexandria CAD, Arlington County CAD, and MWAA CAD. In the future, it is expected that data exchanges will exist for the Prince William County CAD, Loudoun County CAD, Prince George's County CAD, and Montgomery County CAD. At the present time, no public safety (police) jurisdictions participate.

e. Government Data Exchange (GDX)

GDX enables partners in the NCR to securely share a wide range of geospatially referenced data through dynamic web map services in support of coordinated, regional responses to emergency events and on-going regional planning. It supports response operations and planning, situational awareness, and mitigation activities.

Through CAD to GIS (CAD2GIS), GDX creates a regional live view of locations of all fire and rescue/public safety vehicles and the incidents they are responding to. CAD2GIS is for local operations use, mutual aid, emergency management, and area command functions. CAD2GIS puts the real-time location of all units into a map service that can be consumed by situation viewers around the region to support a common operating picture for regional events. A map layer of CAD incidents can be developed to complement vehicle locations.

NCR GDX is a common, known location for geographic data exchange among GISs for several Emergency Operations Centers (EOC) in the area. These include: the Fairfax County EOC GIS, Loudoun County EOC GIS, Prince William County EOC GIS, Arlington County EOC GIS, and the City of Alexandria EOC GIS in Virginia; the District of Columbia EOC GIS, Maryland Emergency Management Agency/Virginia Department of Emergency Management, and the Frederick County EOC GIS, Montgomery County EOC GIS, and Prince George's County EOC GIS in Maryland.

The exchange is not limited to EOC entities. It also includes Federal Emergency Management Agency (FEMA), Military District of Washington, Regional Information Centers, and Principal Federal Official's Representative (PFOR) (U.S. FEMA).

GDX serves to populate situation viewers with incident and contextual information throughout the region.

D. Case Study D: FATPOT Technologies, Inc., Lake County, Illinois, and Boston, Massachusetts

1. Context

FATPOT Technologies, Inc. develops public safety software solutions for data integration and real-time information sharing across dissimilar systems. The company was founded in 2002 and is located at 655 Medical Drive, Bountiful, Utah 84010. Additional company background may be obtained online at <https://www.fatpot.com/>.

FATPOT Technologies has additional offices in Marianna, Doral, Naples, Punta Gorda, Rockledge, and Tampa, Florida; and Goldsboro, North Carolina. The name FATPOT is the acronym from FATPOT World, which once stood for For All The People Of The World, a phrase coined by the firm's founder in an enterprise unrelated to CAD.

The company offers several products/solutions:

- Peer Intelligence-Virtual DATAfusion – A peer intelligence messaging framework that addresses various methods and protocols required to access and distribute information;
- FATPOT CADfusion – A tool for sharing data among various CAD systems;
- FATPOT RMSfusion – A tool that enables sharing of secure record management system information among authorized parties;
- FATPOT GPSfusion – A system that uses peer intelligence to collect and integrate location data in real-time from GPS-enabled mobile units across various interconnected agencies and jurisdictions;
- FATPOT MOBILEfusion-PortalONE – A mobile client desktop environment that provides a framework in which the tools, functional components, and applications needed to perform jobs are integrated for one-click access;
- FATPOT MAPPINGFusion – A tool that provides public safety departments with a real-time picture of their operational environments by aggregating data from information systems in multiple jurisdictions and plotting the data on a detailed real-time digital map;

- FATPOT REPORTfusion – A reporting system that offers automated reporting for mobile users; and
- FATPOT Web Instant Notification System – A notification system that enables public safety agencies to distribute critical alerts and other information to designated parties.

FATPOT software has been implemented by law enforcement, fire, rescue, EMS, homeland security, justice, defense, and 9-1-1 dispatch organizations.

As of January 4, 2011, FATPOT Technologies, Inc., operates as a subsidiary of Communications International, Inc. Communications International, Inc., founded in 1975, is a system integration and software company providing custom communication solutions for public safety and mission critical communications, federal, transit, and utility clients worldwide. The company also handles dispatch center construction activities ranging from facility planning and building construction to renovations, as well as coordination with technology experts for retrofits and console system installations.

Communications International, Inc., has strategic partnerships with Harris, Spectracom, EFJohnson, Otto, Zetron, Raytheon, Icom, KENWOOD, Microwave Networks, Bird Technologies, Impact, Alcatel-Lucent, Midland, and Axell Wireless.

2. Interoperability Path Examples

The FATPOT interoperability approach uses a hub-and-spoke architecture. The hub can be thought of as a “fusion” engine that provides interfaces with disparate CAD systems. The hub handles all of the setup, configuration, translation, and rules for information sharing. Local PSAPs continue to use their native CAD applications, but with the added capability of sharing information and resources across jurisdictional boundaries. Functionally, this approach requires that every connected CAD system publishes to the hub all critical information about all active incidents in real time. This includes continuous updates as changes are made to active incidents. Subscribers must be able to consume basic incident transfer requests, requests for resources, and ongoing updates to shared incident and resource data. These transactions are sent only when a business rule in the hub has triggered the sharing of information. FATPOT uses industry standards for information exchange, such as the National Information Exchange Model (NIEM) and the NIEM XML Schema definitions, which provide data structures for the exchange of basic incident elements. Figure 2-8 shows the connections from the FusionPLATFORM hub to various external entities via spokes.

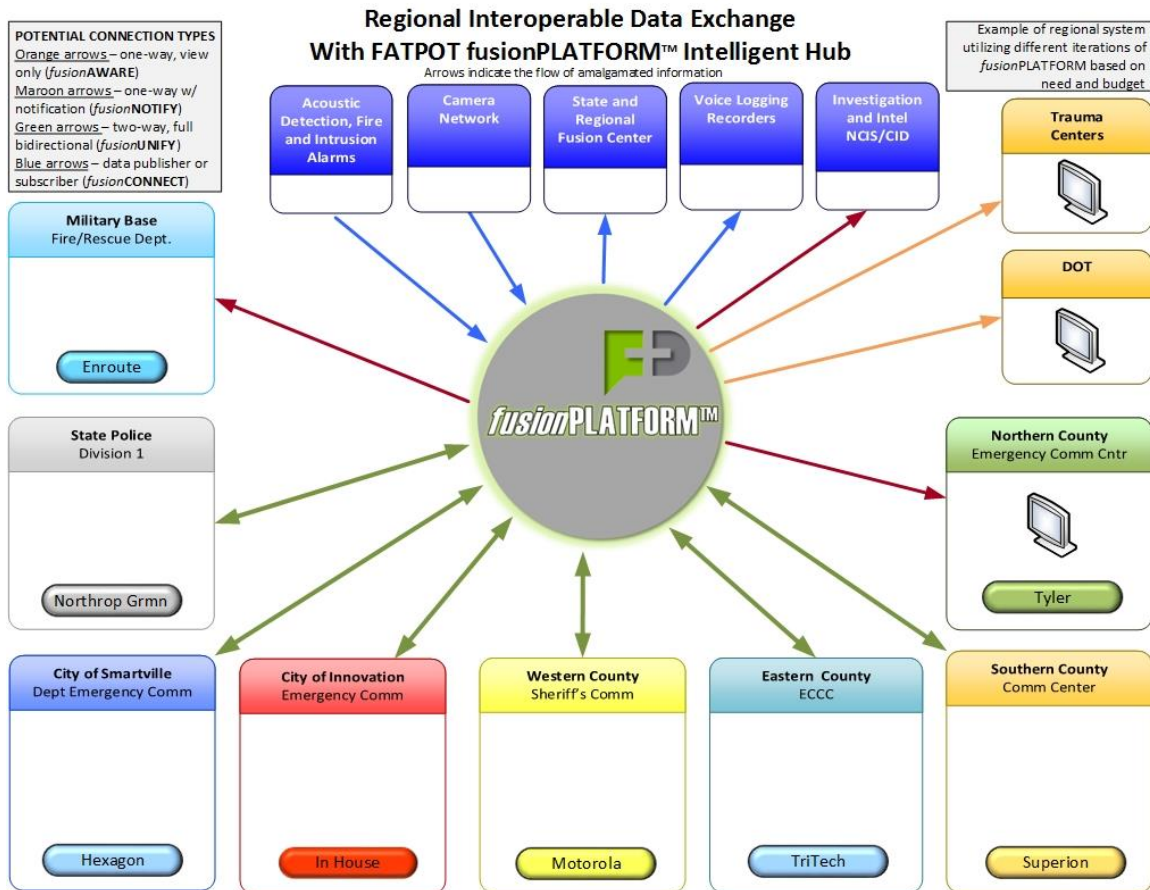


Figure 2-8. Generic Diagram of FATPOT Fusion PLATFORM Connectivity

The Naval Station Great Lakes is the home of the USN's only boot camp, located near North Chicago, in Lake County, Illinois. According to their website,¹¹ in the event of an emergency, Naval Station Great Lakes provides real-time alerts to the Navy community throughout the lifecycle of the incident or crisis through: Giant Voice, a voice announcing system using exterior speakers; Computer Desktop Network System (CDNS), an administrative broadcast across Navy computer networks that overrides current applications, thereby reaching all Navy users almost instantly; and Mass Warning and Notification, which is provided by AtHoc, and disseminates information via text message and email.

At the current time, Naval Station Great Lakes does not participate in the Lake County FATPOT architecture. However, a connection with the USN PSNet ROC has been established (see the USN Regional Dispatch Centers and the Public Safety Network case study on p. 2-2). As was mentioned in that case study, interoperability with adjacent civilian CAD systems appears not to have been established. Given the maturity of this

¹¹ https://www.cnmc.navy.mil/regions/cnrma/installations/ns_great_lakes.html

architecture, and using the example of Charleston County/Joint Base Charleston, incorporating emergency response should not be difficult, if required. Figure 2-9 shows the Lake County, Illinois, architecture.

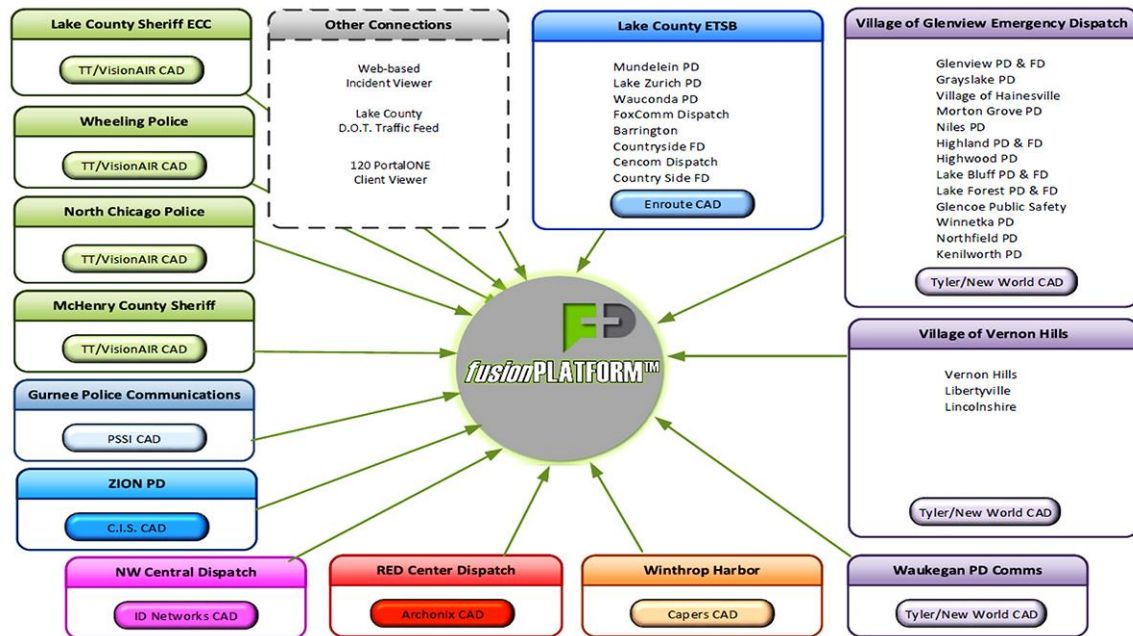


Figure 2-9. Lake County, Illinois, FATPOT Architecture Diagram

Another specific FATPOT architecture instance is the Boston Region, consisting of nine cities and towns: Boston, Brookline, Cambridge, Somerville, Quincy, Chelsea, Winthrop, Revere, and Everett. In addition, two universities (a third is planned), the Fallon Ambulance Company, and the Boston Region Intelligence Center are interoperable, using a total of seven different CAD systems.

The first phase of what is now known as the Public Safety net (PSnet) began in 2004 with a four-city (Brookline, Cambridge, Chelsea, and Boston) proof of concept using microwave and fiber optic links to provide a one-way view, via existing cameras, of regional incidents, thereby providing situational awareness. Funding for this proof of concept was provided by the Department of Homeland Security's Urban Area Security Initiative (UASI). This funding source also allowed the other five cities to join PSnet by 2012, and in 2015, email, text, and a mass warning and notification application were added to the CAD interoperability. Region-wide (excluding the city of Boston's 1,000-plus cameras), approximately 100 pan, tilt, and zoom (PTZ)-capable cameras were installed on the network. In the near future, the cameras will respond to appropriate CAD call codes to move the cameras to image any scene in question. The city of Boston is not in the current effort simply because of the large number of PTZ cameras involved.

Two universities currently use data exchange to assist in their compliance with Clery Act reporting.¹² A third university is studying joining PSnet. Since the implementation of the FATPOT software solutions, data can be automatically fed to the Boston Region Intelligence Center to support criminal activity analyses. Data is also supplied to the state fusion center. A short description of the response to the Boston Marathon bombing is given below.

The Boston Marathon is always held on the third Monday in April. The event attracts approximately 500,000 spectators and over 20,000 participants. On April 15, 2013, 26,839 people were entered in the event. At 2:50 PM, EDT, nearly three hours after the winners crossed the finish line, two explosions occurred about 200 yards apart, in approximately the last 225 yards of the course. Three spectators were killed and 264 people were injured. The Brookline Command Post was located in the Massachusetts Emergency Management Agency trailer in Brookline, approximately 2.5 miles from the finish line. The staff monitored 16 camera feeds in Brookline and Boston, the Brookline CAD showing all Brookline calls and CAD feeds from eight other cities. The locations of all responding Boston EMS and Fire units were visible on this distributed network. According to the Brookline Director of Technology and Communications, Officer Scott Wilder, this gave the Command Post staff situational awareness nearly five minutes before confirmation by phone or radio.¹³ Figure 2-10 shows the FATPOT architecture diagram for Boston.

¹² The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act, or Clery Act, signed in 1990, is a federal statute codified at 20 U.S.C. § 1092(f), with implementing regulations in the U.S. Code of Federal Regulations at 34 C.F.R. 668.46. The Clery Act requires all colleges and universities that participate in federal financial aid programs to keep and disclose information about crime on and near their respective campuses.

¹³ FATPOT White Paper, FATPOT Data Sharing During the Boston Marathon Bombing, FATPOT Technologies, December 10, 2013.

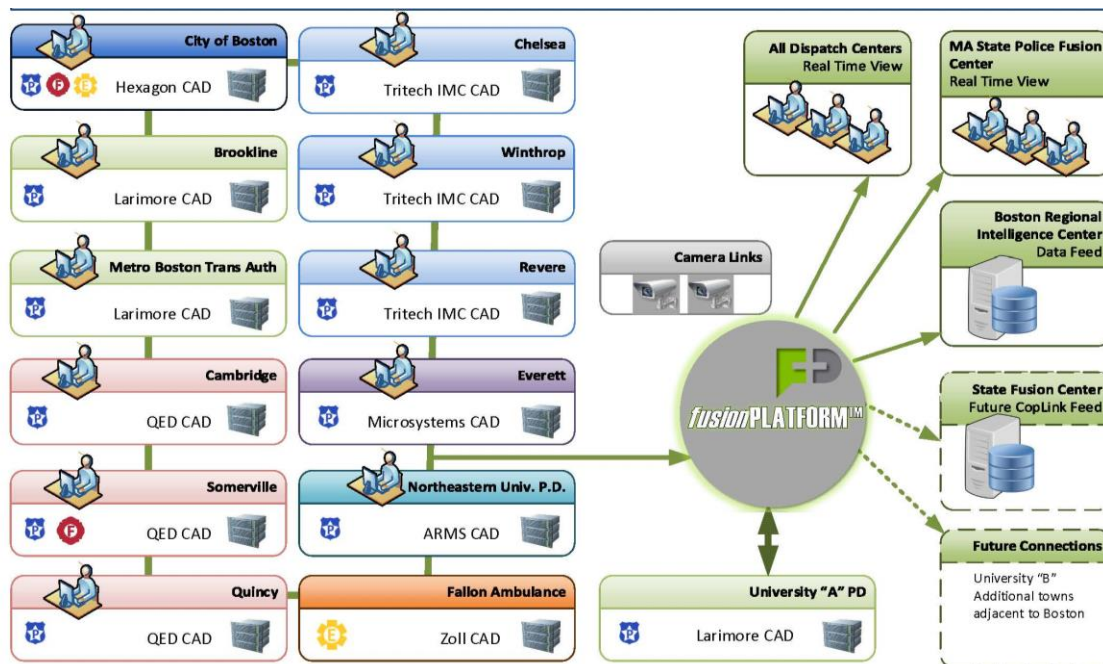


Figure 2-10. FATPOT Implementation Architecture for Boston Region

The Boston project involves 13 agencies, and is growing, with various CAD systems. The first phase involved a one-way view of regional incidents providing situational awareness (fusionAWARE). Some agencies migrated to fusionNOTIFY and fusionUNIFY when the hub was upgraded to fusionPLATFORM in 2017. Harvard University uses fusionUNIFY (bi-directional data exchange) to assist in its compliance with Clery Act reporting.

3. Discussion

The expansion of CAD systems paralleled the development of affordable computing, and the U.S. marketplace for CAD systems is now in its fourth decade. For example, Tiburon was established in 1980, and Tyler, which was originally established in 1966 as an industrial, retail, and distribution holding company, began a multi-phase plan in 1997 that changed the company's focus to serving the unique information management software needs of local governments, including CAD. As the availability and affordability of computers increased, many other CAD vendors appeared in the marketplace (see Appendix A for a CAD Vendor List).

As with many fractionated market places, companies seeking greater scale and profits begin to acquire other existing vendors. For the last several years, there has been a general CAD vendor consolidation; this consolidation has accelerated within the last three years with several primary and secondary vendors being acquired by larger competitors. For example, Tiburon was acquired by TriTech in February 2015 along with other TriTech acquisitions of Global, VisionAir, Information Management Corporation, and Zuercher. A short list of acquisitions by larger companies (TriTech Software Systems, Caliber Public Safety, Motorola, SunGard, Tyler Technologies, and Hexagon) appears in Appendix A.

The fiscal scale of the surviving companies is impressive. For example, based on the United States Securities and Exchange Commission (SEC) Form 8K, October 25, 2017, Tyler Technologies estimated that 2017 revenues would range from \$840 million to \$848 million. Of course, not all of that revenue comes from CAD sales and licensing fees, but it is indicative of the financial size and strength of this company.

The Charleston County, South Carolina, and Joint Base Charleston integration project selected TriTech as their CAD provider. TriTech is not a public company, so no SEC information is available; however, it has been aggressive in making the kind of acquisitions described above. Like Tiburon, FATPOT Technologies LLC, described in the Lake County, Illinois, and Boston, Massachusetts, Case Study D, was acquired by Communications International Inc. (CII), in January 2011. The acquiring company, CII is not a public company, so, again no SEC information was available.

Although the CAD market is increasing (from \$1.12 billion in 2017 to \$1.95 billion by 2022)¹⁴ and the number of unique vendors selling new CAD systems has gone down, many jurisdictions and agencies still use legacy CAD products. Anecdotally, major vendors are reluctant to describe their end-of-life plans for these legacy products. However, the

¹⁴ finance.yahoo.com/news/global-computer-aided-dispatch-markets-111400147

existence of multiple generations of products and vendors clearly does complicate the path toward interoperability and potentially increases the implementation cost. An additional concern in this evolving market is the eventual end of software support. The Lake County interoperability example in Case Study D, incorporates eight distinct CAD systems, several of which have been taken over by larger vendors. Overall, despite the consolidations the CAD marketplace can still be considered fractionated. This leads to the following observations listed in the next section.

A. General Observations

Observation 1.

The CAD market is very fractionated. There are at least 21 primary CAD vendors and over 100 secondary vendors. This complicates the process of implementing even a small-scale interoperable, multi-jurisdiction/multi-agency CAD system. An annotated list of CAD vendors is provided at Appendix A.

Underlying the majority of the case study interoperability implementation paths was an already existing Internet-capable bearer network. The existence of such networks facilitated the technical implementation of interoperable CAD systems and significantly reduced the costs attributable to those implementations. For the USN Regional Dispatch Centers, (see Case Study A), the underlying bearer network was the Public Safety Network. As described in the case study, the network evolution began in 2005 and currently spans CONUS and extends to OCONUS locations. For Charleston County and Joint Base Charleston, (see Case Study B), AT&T was already a primary provider of network services in the area and was selected to expand service to provide an interagency network specifically to support the desired CAD interoperability.

In 1992, when MCI took over the Internet backbone from the National Science Foundation, access was limited to only four network access points. Two of the access points were within the NCR: Metropolitan Area Ethernet-East (MAE-East) in Tysons Corner, Virginia, and Federal Internet Exchange-East (FIX-East) in College Park, Maryland. The other two were in San Jose and Mountain View, California.¹⁵ In addition to its historical benefit of being integral to development in the early days of the Internet, the NCR had already undergone a large fiber optic build-out prior to September 11, 2001. In fact, a considerable amount of this was “dark” fiber, and this excess capacity for existing needs formed the physical basis for the NCRIP and the resulting NCRnet (see Case

¹⁵ Internet Alley: High Technology in Tysons Corner 1945-2005, Paul E. Ceruzzi, The MIT Press, 2008, page 154.

Study C). In addition, several of the municipalities had already existing I-Nets, which greatly simplified cross-jurisdictional and cross-agency CAD interoperability.

The Boston Regional Architecture includes nine cities and towns (see Case Study D) and used seven unique CAD vendors. Data interoperability was a problem, and in 2004 construction of the Public Safety Net began, using the Department of Homeland Security's Urban Area Security Initiative funding. The existing network of microwave and fiber optic links was used in a four-city proof-of-concept network, mainly to transmit camera images. Later, five other cities joined PSNet and services expanded using FATPOT software to include CAD and mass warning and notification applications.

Lake County was an exception, since each of the disparate CAD systems operated on its own servers in different locations, with most on separate networks (again, see Case Study D). The CAD implementation used some existing interconnected network links, but the majority were interfaced using encrypted protocols generated by FATPOT software via the Internet.¹⁶ Even with this exception, existing Internet backbones seem more typical than not. This leads to the second observation.

Observation 2.

In the majority of the case studies, an Internet-capable bearer network spanning the area already was in existence. This not only facilitated the technical implementation of interoperable CAD but significantly reduced the costs attributable to that implementation. Bearer networks ranged from national in scope to single counties.

During the development of this paper, IDA met with CAD vendors to discuss their products and the state of the market in general. A consistent theme was the market-driven competitive requirement to closely hold the details of the product. While perfectly understandable, it is no surprise that implementing a multi-vendor CAD system is difficult. As outlined above, in Case Studies B and D, one potential solution is to select a single vendor (using the approach of consolidation onto a common CAD platform), thus eliminating sharing of proprietary information. Alternatively, multiple APIs can be written without proprietary information sharing, and a hub-and-spoke architecture can be implemented. These vendor interactions form the basis for the third observation.

Observation 3.

Anecdotal evidence indicates that cooperation between multiple vendors of CAD systems is often needed but difficult to achieve (requiring proprietary software). This has

¹⁶ Steven J. Winnecke, ENP, RPL, Director of IT, Lake County, Illinois, personal communications, November 3, 2017.

been overcome by the selection of a single vendor or use of multiple APIs to implement a hub-and-spoke architecture.

Observation 4.

Decisions to implement interoperable CAD systems are typically local ones. Each locality will have unique aspects: the CAD systems already in use, the local communities to be included, jurisdictional boundaries, the total population involved, the types of first response organizations selected to participate (one case study included fire and EMS but not police), and finally one Service elected to implement a regional dispatch system connecting bases and letting the base interface with civilian organizations.

Observation 5.

When mobile devices are used on a base to make 9-1-1 calls, the call does not necessarily go to base operators but is routed to a civilian 9-1-1 call center. Eliminating the “call forwarding” delay was a motivating factor in multiple case studies.

Observation 5 was based on discussions with CAD vendors, and discussions with IDA Research Staff Members expert in cellular network characteristics.

Appendix A

CAD Vendor List

The following list was pared down from an initial list of over 150 companies that develop and/or market software for law enforcement, fire, and emergency management services:

- ADSi – Southaven, MS (<https://www.e9.com>);
- Caliber Public Safety & Caliber Justice – Niagara Falls, NY;
(<https://caliberpublicsafety.com>) [web page has copyright “Harris Systems USA, Inc.”];
- Airbus-DS Communications (formerly Cassidian Communications, an EADS North America Co.) – Temecula, CA (<http://www.airbus-dscomm.com/index.php>);
- Crimestar Corp. – San Jose, CA (<http://www.crimestar.com>);
- Emergency CallWorks – Birmingham, AL
(<https://www.emergencycallworks.com>);
- Informant Technologies Inc. – Lansdale, PA (<http://www.informant-tech.com> non-responsive URL);
- Intergraph – Owned by Hexagon, a Swedish company;
- Hexagon Safety & Infrastructure
(<http://www.hexagonsafetyinfrastructure.com/>);
- Intrado, Inc. – Longmount, CO (<https://www.west.com/safety-services/>);
- Mark43 – New York, NY (<https://www.mark43.com>);
- Motorola Solutions – Chicago, IL
(https://www.motorolasolutions.com/en_us.html);
- New World Systems – Troy, MI (<https://www.tylertech.com/solutions-products/new-world-public-safety-product-suite/computer-aided-dispatch>);
- Sungard Public Sector – Lake Mary, FL (<http://www.sungardps.com>);
- PTS Solutions – Harrisonburg, LA (<https://ptssolutions.com>);
- Spillman Technologies, Inc. – Salt Lake City, UT (<https://www.spillman.com>);

- Sun Ridge Systems Inc. – El Dorado Hills, CA (<http://www.sunridgesystems.com/index.php>);
- TriTech Software Systems – San Diego, CA (<http://www.tritech.com>);
- Tyler Technology – Plano, TX (<https://www.tylertech.com/solutions-products/public-safety-solutions/911-dispatch>);
- Zoll Data Systems – Broomfield, CO (<https://www.zolldata.com/>).

The following information is from the document *CAD Service Providers: Research and Initial Observations* by Becky Ward, FATPOT Technologies, Inc., 1 April 2017.

Major Acquisition Summary:

1. TriTech (Inform CAD):
 - Global (Source code for RMS), VisionAir, IMC, Zuercher;
 - Tiburon (five flavors of Tiburon CAD: Command CAD, Stratus CAD, Total Computer CAD, IQ CAD, DispatchNOW CAD (bought from Positron);
2. Caliber Public Safety (owned by Harris Computers):
 - Global, Sleuth, InterAct and SmartCOP (CTS America);
3. Motorola:
 - Spillman;
4. SunGard (recently acquired by FIS):
 - OSSI, HTE;
5. Tyler Tech:
 - New World;
6. Hexagon:
 - Intergraph,
 - Intergraph bought Denali (for RMS).

The following is an accumulated list of CAD providers with CAD as the lead product and either with at least 100 clients/customers or that does business in several states. Companies listed below may also appear in the previous lists.

- Application Data Systems Inc. (ADSI) – Columbus, OH (<http://www.e9.com/>). 100 clients in 17 states.
- Archonix – Marlton, NJ (<http://www.archonixsystems.com/>). 100 agencies in 16 states.

- Bell Canada – Ontario, Canada (www.bell.ca/publicsafety).
- Cardinal Tracking – Lewisville, TX (<http://www.cardinaltracking.com/cad/>). Over 400 municipal clients in US and Canada.
- Cody – Pottstown, PA (<http://www.codycomputer.com/>).
- CISCO (Creative Information Systems Company) – New Port Richey, FL (<http://www.cisco-ps.com/>). Over 300 clients.
- Competitive Edge Software Inc. – Franklin, WI (<http://www.report-software.com>). Over 1200 agencies across USA. Also targeting Corporate, Casinos, Hospitals, Colleges and Security companies.
- Computer information Systems (CIS) – Skokie, IL (http://www.cisusa.org/about_us.php). Over 500 agencies in USA.
- CSI Technology Group – Keasbey, NJ (<http://www.csitech.com/>). Focus in NJ, NC, NM, OK, HI.
- Cyrun – Santa Cruz, CA (<http://www.cyrun.com/>). 100 agencies. Focus is western USA.
- DaPro Systems – Roanoke, VA (<http://www.daprosystems.com/>). 170 agencies.
- End2End Inc. (ARMS) – Rohnert, CA (<http://www.arms.com/>). 700 customers.
- Enforsys – Parsippany, NJ (<http://www.enforsys.com/>). 160 police installations (largest has 1,400 officers). “700 customers in 10 states,” “Over 400 installations of Police and Fire technologies in eighteen states across the U.S. and Jamaica...”
- EZ911 – Valdosta, GA (<http://www.ez911inc.com/>). Clients in GA, LA, AL, WV, TN.
- FDM Software – North Vancouver, BC Canada (<http://www.fdmsoft.com/>). 120 installations “serving hundreds of jurisdictions.”
- Global Software Corporation – Oklahoma City, OK (<http://www.globalsoftwarecorp.com/>). A division of Harris Computer Systems (2009) of Ottawa, Ontario, Canada (see www.harriscomputer.com). Note that Global sold its RMS source code to TriTech; then TriTech bought VisionAIR. 500 customers in 32 states.
- Hexagon (formerly Intergraph) – Huntsville, AL (<http://www.hexagonsafetyinfrastructure.com/public-safety-and-security>).
- Information Management Corp (IMC) (Acquired by TriTech. See TriTech). Over 600 IMC clients (LE, SO, Universities); this may be an old list.

- Information Technologies Inc. (ITI) – St. Louis, MO (<http://www.itiusa.com/>). 600 agencies.
- LawSoft Inc. – NJ (<http://www.lawsoft-inc.com/>). 100 agencies in NJ.
- Law Enforcement Technology Group (LETG) – Woodbury, MN (<http://www.letg.com>). 175 law enforcement, fire and EMS agencies. 15 agencies in Hennepin County use LETG.
- Motorola – Chicago, IL (https://www.motorolasolutions.com/en_us/products/smart-public-safety-solutions/integrated-command-control/premierone-cad.html#tabproductinfo).
- New World Systems (Acquired by Tyler Tech) – Troy, MI (<http://www.newworldsystems.com/>) – Claims over 600 clients in 50 states.
- Nexgen Public Safety Solutions – East Haven, CT (<http://www.nexgenpss.com>). 114 agencies in CT and CT State Police and several CT universities as clients.
- Ortivus North America (<http://www.tritechems.com/>). Bought by TriTech.
- Pamet Systems Inc. (aka Pamet Software LLC) – Hudson, MA (<http://www.pamet.net/>). 170 Agencies, ranging from 10 officers to 2,000.
- Public Safety Systems Inc. (PSSI) – Lanham, MD (<http://www.pssi.com/>). Over 150 agencies of LE, Fire, and EMS.
- Southern Software – Southern Pines, NC (<http://www.southernsoftware.com/>). Claims 1,000 municipal and public safety agencies.
- Spillman Technologies (Acquired by Motorola) – Salt Lake City, UT (<http://www.spillman.com/>). 1,000 agencies in 36 states.
- Sun Ridge Systems – El Dorado Hills, CA (<http://www.sunridgesystems.com/index.php>). 100 customers in California alone.
(http://www.sunridgesystems.com/index.php/company/business_in_california)
- Tiburon (acquired by TriTech). Had a number of different CAD's due to acquisitions and platforms.
- Tyler Technologies – Dallas, TX (<http://www.tylertech.com/>). Tyler Technologies is the largest company in the country solely dedicated to providing software and services to the public sector, including solutions for state, county and local governments and schools.
- USA Software Inc. – Cooper City, FL (<http://www.usa-software.com/>). 150 installations in FL and GA.

- Valor Systems Inc. – Oak Brook, IL (<http://www.valorsystems.com/>). Statewide CAD in NH and RI. Clients in AL, CA, FL, IL, IN, MO, NH, NY, NC, RI, WI.
- Zuercher Technologies LLC – Sioux Falls, SD (<http://www.zuerchertech.com/company/about-us/>). Acquired by TriTech. See also <http://www.zuerchertech.com/why-us/>.

Acronyms and Abbreviations

AES	Advanced Encryption Standard
AFB	Air Force Base
AFIS	Automated Fingerprint Identification System
AFR	Automatic Field Reporting
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
API	Applications Programming Interface
ASE	AT&T Switched Ethernet Service
AT&T	originally American Telephone & Telegraph
ATO	Authority to Operate
AVG	Automated Vehicle Gates
BRAC	Base Relocation and Closure
C2	Command and Control
C3P	Certified Call Center Professional
C4	Command, Control, Communications and Computers
C4I	Command, Control, Communications, Computers, and Information
CAD	Computer Aided Dispatch
CAD2CAD	CAD to CAD
CAD2GIS	CAD to GIS
CCTV	Closed Circuit Television
CDC	Consolidated Dispatch Center
CDNS	Computer Desktop Network System
CFS	Call for Service
CHS	Charleston
CIO	Chief Information Officer

CNIC	Commander, Navy Installations Command
CONUS	Continental United States
COVITS	Commonwealth of Virginia's Information Technology Symposium
DC	District of Columbia
DCIO	Deputy Chief Information Officer
DCIO C4&IIC	Deputy Chief Information Officer C4 and IIC
DCNET	DC's fiber optic network
DEH	Data Exchange Hub
DHEC	Health and Environment Control
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
ECC	Emergency Communications Center
ECMS	Enhanced Crisis Management System
EFD	Emergency Fire Dispatch
ELMR	Enterprise Land Mobile Radio
EMD	Emergency Medical Dispatch
EMS	Emergency Management System
EMWM	Enterprise Mass Warning and Notification
EOC	Emergency Operations Center
ESF	Emergency Support Function(s)
FATPOT	originally, For All The People Of The (World)
FD	Fire Department
FEMA	Federal Emergency Management Agency
FRD	Fire Response Disaster
GB	Gigabytes (2 ³⁰ , or somewhat more than one-billion bytes)
GDX	Government Data Exchange
GIS	Geographic Information System

GPS	Global Positioning System
IAED	International Academy of Emergency Dispatch
IAMS	Identity and Access Management Service
ICI	Interoperability Communications Infrastructure
ICS	Industrial Control Systems
IDA	Institute for Defense Analyses
IIC	Information Infrastructure Capabilities
IMC	Information Management Corporation
I-Net	Intergovernmental Network
IOC	Initial Operating Capability
IoT	Internet of Things
IPSec	Internet Protocol Security
ISSI	Inter RF Subsystem Interface
IT	Information Technology
JB	Joint Base
JB CHS	Joint Base Charleston (SC)
JMS	Jail Management System
LAMAS	Location and Movement Analysis System
LDC	Local Dispatch Center
LMR	Land Mobile Radio
LPR	License Plate Reader
MA	Massachusetts
Mbps	Megabits per second
MD	Maryland
MEMA	Maryland Emergency Management Agency
MOA	Memorandum of Agreement
MWAA	Metropolitan Washington Airports Authority
MWCOG	Metropolitan Washington Council of Governments
MWNS	Mass Warning and Notification System

N6	Office of the Command Information Officer
NACMS	Navy Access Control Management System
NCIC	National Crime Information Center
NCR	National Capital Region
NCRnet	NCR [emergency management] Network
NCRIP	NCR Interoperability Program
NENA	National Emergency Number Association
NERMS	Navy Emergency Response Management System
NFPA	National Fire Protection Act
NGA	National Geospatial-Intelligence Agency
NIBRS	National Incident-Based Reporting System
NIEF	National Identify Exchange Federation
NIEM	National Information Exchange Model
NIPRNET	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NOVARIS	Northern Virginia Regional Identification System
NVERS	Northern Virginia Emergency Response System
NVHA	Northern Virginia Hospital Alliance
OMB	Office of Management and Budget
PD	Police Department
PFOR	Principal Federal Official's Representative
PGC	Prince George's County
POMS	Port Operations Management System
POP	Point of Presence
PSAP	Public Safety Answering Point
PSNet	Public Safety Network
QRT	Quick Reaction Team or Quick Response Team
RAFIS	Regional Automated Fingerprint Identification System
RAMAS	Risk Assessment, Management and Audit System

RDC	Regional Dispatch Centers
RFI	Request for Information
ROC	Regional Operations Centers
RMS	Records Management System
SC	South Carolina
SDK	Software Development Kit
TT	TriTech
USASI	United States of America Standards Institute
UCR	Uniform Crime Reporting
US	United States
USAF	United States Air Force
USN	United States Navy
VA	Virginia
VDEM	Virginia Department of Emergency Management
VDOT	Virginia Department of Transportation
VTC	Video Teleconferencing System
WMATA	Washington Metropolitan Area Transit Authority
WSSC	Washington Suburban Sanitary Commission
XML	Extensible Markup Language

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) 15-12-17		2. REPORT TYPE Final		3. DATES COVERED (From – To)	
4. TITLE AND SUBTITLE Computer Aided Dispatch Interoperability Case Studies				5a. CONTRACT NUMBER HQ0034-14-D-0001	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBERS	
6. AUTHOR(S) Serena Chan, John W. Bailey, Ronald A. Enlow, Clyde G. Roby				5d. PROJECT NUMBER BC-5-4012	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882				8. PERFORMING ORGANIZATION REPORT NUMBER D-8778	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Joseph M. Wassel DoD CIO 6000 Defense Pentagon, Washington, DC 20301				10. SPONSOR'S / MONITOR'S ACRONYM DoD CIO	
				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 This document addresses the interoperability of Computer Aided Dispatch (CAD) systems. CAD systems are used by Public Safety Answering Points (PSAPs) to dispatch first responders to answer Calls For Service (CFS) (9-1-1 calls or alarms). The premise of this document is that neighboring jurisdictions, whether military or civilian, or mixed, can benefit from interoperable CAD systems. This document examined case studies of several implementations of interoperable CAD systems and describes their path toward interoperability with surrounding jurisdictions. These illustrative case studies serve to initiate discussions about whether a DoD-wide policy standard for implementation of interoperable military-civilian CAD systems is viable.					
15. SUBJECT TERMS Public safety and emergency management communications, computer aided dispatch, military-civilian interoperability					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Unlimited	18. NUMBER OF PAGES 58	19a. NAME OF RESPONSIBLE PERSON Joseph M. Wassel
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (Include Area Code) 703-901-7360

