NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

USMC INSTALLATIONS COMMAND INFORMATION ENVIRONMENT: OPPORTUNITIES AND ANALYSIS FOR INTEGRATION OF FIRST RESPONDER COMMUNICATIONS

by

Andrew T. Butler
Jason M. Carter

September 2014

Thesis Advisor: Glenn R. Cook
Second Reader: William J. Robinette

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
USMC INSTALLATIONS COMMAND INFORMATION ENVIRONMENT: OPPORTUNITIES AND ANALYSIS FOR INTEGRATION OF FIRST RESPONDER COMMUNICATIONS

5. FUNDING NUMBERS

6. AUTHOR(S) Andrew T. Butler, Jason M. Carter

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release;distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

This thesis analyzes the current, planned, and potential future first responder policies, procedures, networks, and architecture in the Marine Corps. The current technology and information systems are studied to examine the level of interoperability between civilian and military first responders. Camp Pendleton Safety and Emergency Services Battalion is used as a case study in order to assess how these groups can combine their efforts in the case of an emergency or natural disaster. The planned first responder program, Emergency Management Command and Coordination (EMC2), is also assessed to examine the potential capabilities and interoperability that can be garnered through modernization of technology, networks, and information systems. The current and planned systems will be analyzed to determine how the Marine Corps can integrate into the Department of Commerce's first responder network (FirstNet) in the future. This integration planning is vital in order to vet misalignment of civil and Department of Defense information technology security policies, foster ease of implementation of FirstNet for the Marine Corps, and to ensure early planning based on possible implementation models and metrics.

14. SUBJECT TERMS United States Marine Corps Installations Command, Department of Commerce, First Responder Network (FirstNet), Emergency Management Command and Coordination (EMC2), First Responders, Cloud Computing

15. NUMBER OF PAGES 113

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release;distribution is unlimited

USMC INSTALLATIONS COMMAND INFORMATION ENVIRONMENT: OPPORTUNITIES AND ANALYSIS FOR INTEGRATION OF FIRST RESPONDER COMMUNICATIONS

Captain Andrew T. Butler
United States Marine Corps
B.A., North Carolina State University, 2005

Captain Jason M. Carter
United States Marine Corps
B.S., United States Merchant Marine Academy, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2014

Author: Andrew T. Butler
Jason M. Carter

Approved by: Glenn R. Cook
Thesis Advisor

William J. Robinette
Second Reader

Dr. Dan Boger
Chair, Department of Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis analyzes the current, planned, and potential future first responder policies, procedures, networks, and architecture in the Marine Corps. The current technology and information systems are studied to examine the level of interoperability between civilian and military first responders. Camp Pendleton Safety and Emergency Services Battalion is used as a case study in order to assess how these groups can combine their efforts in the case of an emergency or natural disaster. The planned first responder program, Emergency Management Command and Coordination (EMC2), is also assessed to examine the potential capabilities and interoperability that can be garnered through modernization of technology, networks, and information systems. The current and planned systems will be analyzed to determine how the Marine Corps can integrate into the Department of Commerce's first responder network (FirstNet) in the future. This integration planning is vital in order to vet misalignment of civil and Department of Defense information technology security policies, foster ease of implementation of FirstNet for the Marine Corps, and to ensure early planning based on possible implementation models and metrics.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

C2	command and control
CAD	computer aided dispatch
CBRN	chemical, biological, radiological, and nuclear
CERS	consolidated emergency response system
CONUS	continental United States
COTS	commercial off the shelf
DOD	Department of Defense
E-LMR	enterprise land mobile radio
E911	electronic 911
EMC2	emergency management command and coordination
EMT	emergency medical technician
ESI-Net	emergency services IP network
EVA	economic value added
FCC	Federal Communications Commission
FirstNet	first responder network
G-5	plans division
G/S-6	communications department
IA	information assurance
IaaS	infrastructure as a service
IRR	internal rate of return
IT	information technology
LTE	long term evolution
MCICOM	Marine Corps Installations Command
MCIEast	Marine Corps Installations East
MCIWest	Marine Corps Installations West
MCNOSC	Marine Corps Network Operations and Security Center
MHz	megahertz
MOA	memorandum of agreement

MOU	memorandum of understanding
NMCI	Navy Marine Corps intranet
NPV	net present value
NTIA	National Telecommunications and Information Agency
PaaS	platform as a service
PMO	provost marshall's office
PSAP	public safety answering points
RCIP	regional and county interoperability project
SaaS	software as a service
SES	Security and Emergency Services
SLA	service level agreement
USMC	United States Marine Corps
VHF	very high frequency

I. INTRODUCTION

A. PURPOSE OF STUDY

Proliferation of cloud data and infrastructure as a service now offers organizations the ability to streamline processes and share information economically. Utilizing these techniques and services, the Marine Corps has the ability to capitalize on private sector information technologies and ways of doing business. Companies such as Verizon, Amazon, and Google have established cloud data resources accessible by the public with the potential of providing a range of information technology services. Analysis of these models could potentially prove fruitful in creating an organic Marine Corps prototype for providing management and governance over Marine Corps Installations information technology architecture.

Currently, Marine Corps Installations Command is looking at acquiring and combining Verizon's Terremark services with the Department of Commerce's first responder network. Verizon's Terremark provides cloud, data and infrastructure as a service (IAAS) (outsourcing servers, networks, data, and computers to organizations that are paid to support information networking operations) (Terremark.com, 2014). Department of Commerce's First Responder Net provides broadband network architecture, to include Long-Term Evolution (LTE) voice, video and data services (GPO, 2012). Important to Marine Corps decision makers in choosing a cloud computing service is understanding their own needs, choosing or creating a costing model that provides the best fit for performance needs and fiscal restrictions, and understanding issues with pricing transparency in order to develop mitigation techniques.

B. RESEARCH QUESTIONS

1. What business, governance, and architecture models does the USMC use for providing first responder services to its customer base and capital investment over its infrastructure?

2. What business, governance, and architecture models does FirstNet use for providing its services to first responders and capital investment over its infrastructure?
3. How can these models be applicable for Commander Marine Corps Installation Command and its services to their tenant organizational customer base?
4. How can the Marine Corps integrate the cost metric structure in order to create the most cost effective solution options?

C. BENEFITS

The benefits of this research will enable a better understanding of the proposed FirstNet architecture and how Marine Corps Installations Command (MCICOM) integrates in the network. FirstNet may offer a greater degree of interoperability and collaboration between first responders across the nation. The FirstNet system is intended to integrate first responders across federal, state, and local levels in order to respond to daily occurrences and natural disasters in a more cohesive manner. The network could enable first responders to share information, communicate more effectively, and share information and effects as a cohesive force.

The Department of Defense and MCICOM might be able to leverage resources and the network in order to assist federal, state, and local entities in responding to situations within their area or across the nation. Instances occur on DOD installations that require the assistance of outside agencies, such as wild fires on the West Coast, tornadoes in the Mid-West, and hurricanes on the East Coast. These situations cannot always be addressed or resolved by the organic assets and personnel on their associated installations and may require outside assistance from local authorities. Similarly, federal, state, or local agencies may require the assistance of first responders on DOD installations in responding to national, regional, or local disasters. FirstNet could facilitate all agencies, whether federal, state, local, or DOD, to communicate, share information, and streamline their efforts to address and resolve the issue at hand.

D. METHODOLOGY

In order to determine how MCICOM might integrate into FirstNet, the research will be tailored to assess current, planned, and future first responder policies, procedures, and technology. Initially, the research will focus on the current policies, procedures, and technology used by the SES Battalion in Camp Pendleton.

To further the research, the planned first responders programs will be researched in order to assess how planned capabilities can assist in future implementation of FirstNet. The Emergency Management Command and Coordination program is an upgrade from current first responder capabilities and provides first responders with enhanced abilities. This program and research will act as a bridge between current capabilities and future FirstNet implementation and interoperability.

Finally, FirstNet will be assessed in terms of its planned architecture and implementation. Due to the limited information about the implementation and architecture, the research and proposals will be focused on potential models for the implementation of the program. Level of infrastructure management and established policy will be researched to propose potential models for future implementation of FirstNet.

E. LIMITS OF RESEARCH

FirstNet is a program that is currently in development by the Department of Commerce. At the beginning of the research there was minimal information on the program and how it would be implemented. During the research, a great deal of progress was made with the architecture and the future implementation of the project. With FirstNet's planned timeline, a great deal of the research is based on how the program can be implemented in the future and how it might benefit Marine Corps Installations Command.

The timeline for the implementation of FirstNet currently affects the ability to research accurate costing models for employment. However, there are costing

metrics that can be assessed in order build costing models in the future. The costing metrics integrated in the research will be relevant and integral in predicting cost models at FirstNet matures.

Another key limitation to the research is the planned architecture and employment of FirstNet. Without knowing how FirstNet will be employed, at the national, state, or local level, the research is focused on the potential benefits and detriments to each implementation model.

II. LITERATURE REVIEW

A. CLOUD CONCEPTS

The concept of cloud computing has been around for a significant period of time. In 1961, Professor John McCarthy proclaimed that computing would eventually be organized similar to a public utility where a user would purchase services and capabilities based on their capacity as required (Garfinkel, 2011). Fifty years later, the National Institute of Standards and Technology has defined cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources” (Mell & Grance, 2011).”

A cloud computing provider, such as Verizon Terremark, Amazon, or Google, will establish, operate and maintain the physical and logical architecture of a network. The provider will establish the physical backbone for the network in a data center, which will house the servers for storage, applications, and other software. Administrators will operate and maintain a virtual environment that provides virtual machines, with the requisite operating system and applications, required for a user or an organization. The resources can rapidly be made available with minimal interaction or management from the provider (Mell & Grance. 2011).

The cloud computing model offers an organization a potential cost savings in hardware, software and personnel expenses. The organization can rent or purchase services from a provider on a temporary basis or as a permanent solution for its network architecture.

1. Cloud Characteristics

Cloud computing is becoming a more and more prevalent technology in the business world today. According to Syal and Goswami (2012), cloud technology is seen as a “breakthrough in information technology [that] reflects how organizations design and deliver business services” to their users. The

inherent technology in cloud computing is not new, but the current models and methods of its use are innovative and efficient. Cloud computing allows for the effective use of computing resources, applications, and personal files without reliance on a single computer or system (Syal & Goswami, 2012).

By operating in the cloud, an organization has the ability to access its information and applications at any time from any place. A user or consumer can access these capabilities without having to interact or provision them from a certain department or service provider (Becker, 2012). This access is due to cloud services largely being web-based, which can be retrieved through most systems with access to the Internet (Syal & Goswami, 2012). The end user can therefore utilize almost any platform that they choose, to include smart phones, tablets, laptops or standalone systems to acquire their information (Becker, 2012).

Resources can be pooled to effectively utilize server space and dynamically allocate resources (Becker, 2012). This allocation allows for a user to access resources at any time, regardless of location, and reallocates those resources to other users when they no longer are being utilized. These resources are not only physical machines, but also include storage, virtual machines, processing power and bandwidth (Becker, 2012).

Cloud computing offers a great deal of elasticity. Organizations can expand or contract their networks based on demand of their users (Becker, 2012). This flexibility applies to applications and software required by the users and is not limited to hardware or virtual machines. A cloud provider can allow access for a certain user to a specific application based on need. This accessibility can be created for any duration required by the user or provider (Goel & Aggarwal, 2013).

While cloud computing offers accessibility to end users or an organization’s enterprise, it also allows the provider a way for measuring provided services. The amount of service time, storage space, or number of

users is generally established by a service level agreement (SLA). An SLA is a key element in cloud computing and established to identify the needs of the organization and the level of service that is expected from the provider (Syal & Goswami, 2013). Additionally, if a service level agreement is not established, cloud computing offers the provider a level of metering its services, similar to a power company. This metering can be based on the amount of bandwidth, number of users, data storage or processing power utilized, which allows for on-demand use of the resources with an established SLA (Becker, 2012)

2. Types of Cloud Computing

There are three primary types of cloud computing that are prevalent today, infrastructure as a service (Iaas) and software as a service (SaaS). Each type is unique and provides different capabilities based on a company's size, organization, and needs. Platform as a service (PaaS) is an additional form of cloud computing, but is for focused on software and application development.

a. Infrastructure as a Service

Infrastructure as a service is the most robust version of cloud computing, as it provides a large amount of the underlying physical and logical infrastructure. Services are provisioned for the use by the customer, which extends beyond software applications and platforms (Becker, 2012). Network hardware, data storage and processing power are provisioned for use specifically by an organization as its network backbone. The organization then runs its software and operating systems on the underlying network. In the case of IaaS, the system is ultimately maintained and controlled by the service provider with the user having limited access and control over the network architecture (Becker, 2012).

Figure 1 shows the IaaS architecture that has three primary elements: the administrative center, computing resource center, and the cloud storage resource center (Sun, Ji, Yue, & Xiong, 2011). The administrative center is the overall access control and provider of services to the customer. In accordance with an

SLA, the administrative center is typically responsible for monitoring the usage of resources, scheduling of resources, and managing the systems that have been made available. The administrative center is additionally responsible for ensuring that the customer has the available resources that are needed and adding additional resources if required (Sun et al., 2011).

As indicated in Figure 1, the computing resource center is where the virtual machines and networks physically reside and are utilized by the end user (Sun et al., 2011). These resources are allocated dynamically based on the need of the user and their geographic location. This system can be expanded or contracted based on the need of the user and is controlled by the administration center (Sun et al., 2011).

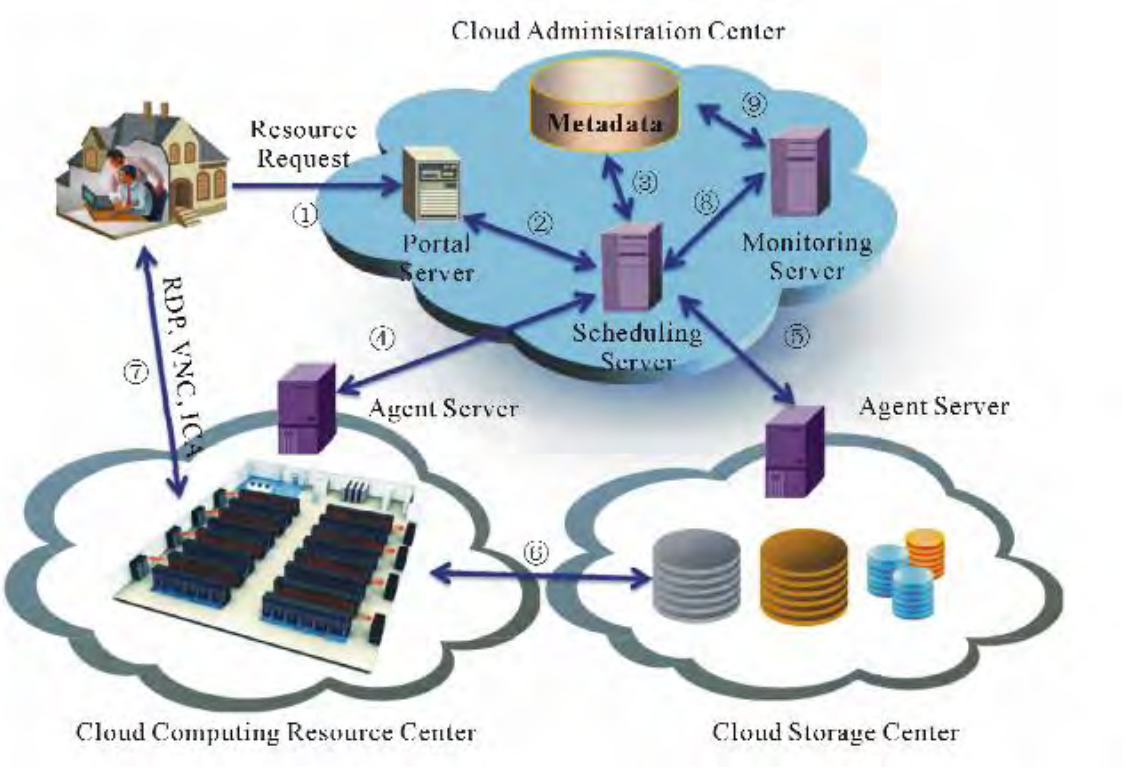

Figure 1. Elements of an IaaS Architecture (from Sun et al., 2011)

The computing storage center is logically where all information for the enterprise's cloud is stored, to include the end user's virtual machines, backups,

and templates to be utilized by future users (Sun et al., 2011). When a customer requires access, their virtual image is transferred and loaded into a physical machine for use by the end user (Sun et al., 2011). This process allows for the dynamic allocation of resources and reduces the requirement for all users to have a dedicated physical machine.

Figure 2 shows how the cloud computing process is accomplished. A user first requests access to a virtual machine from the resource center. If a system is available, that user's virtual image is requested from the storage center and a specific image will be pushed to the assigned virtual machine.

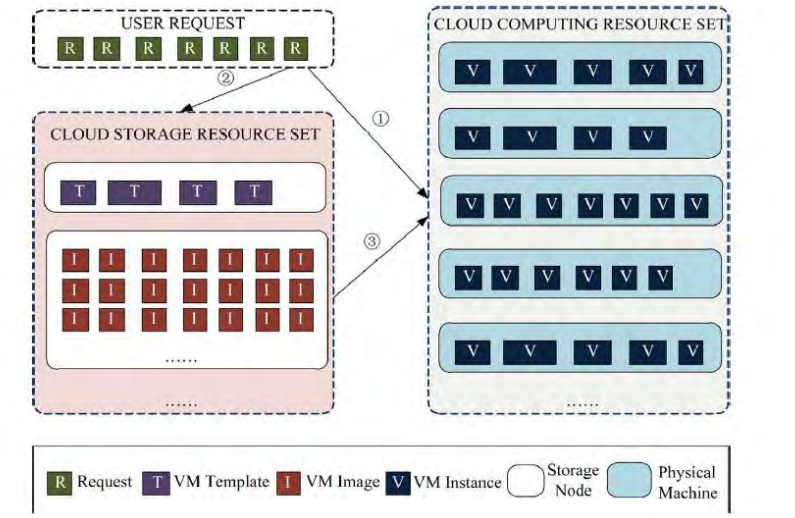

Figure 2. IaaS Session Initialization (from Sun et al., 2011)

Verizon Terremark is an example of an infrastructure as a service provider (Baset, 2012). In addition to providing network services as a backbone for an enterprise, they have the ability integrate and supplement an existing network for additional services. Terremark tailors its service to the established policies and needs of an enterprise, instead of the enterprise adapting to its requirements (Goel & Aggarwal, 2013).

b. Software as a Service

Software as a service is a web-enabled tool that allows access and usage of specific applications that are not resident on a user's system (Becker, 2012). These services are accessible to almost any system that has an Internet connection. They are generally not restricted to a specific platform and can be accessed through a thin client or an established platform (Becker, 2012). Users install or access these applications on their devices and rent services according the duration, number of systems required, and type of application required. Due to the nature of these systems residing in the cloud, they are accessible from anywhere at any time (Syal & Goswami, 2013).

The underlying cloud technology and architecture is maintained by the cloud provider. The user has little control over the applications in which they are accessing and are usually limited to minor configurations that are unique to the customer (Becker, 2012). This architecture limits the need for an organization to invest in additional hardware, software licenses, and bandwidth necessary to run applications, which puts the onus of maintaining and upgrading the system on the provider (Syal & Goswami, 2013). The organization may find such architecture beneficial if they only require specific software for a limited amount of time. Customers do not incur the additional costs of the added infrastructure or maintenance, and may see savings for short projects where services are required for short durations.

c. Platform as a Service

Platform as a service is a mid-level construct in the cloud-computing model that provides an organization with a network environment and a platform for utilizing software. A virtual environment is created for an organization's use with the network administration and access control being managed by the service provider (Dhar, 2012). The provider will establish and manage a virtual operating environment and provide an operating system for consumers to run their own software. The consumer has minimal input into the configuration of the network,

but does have control over the software and the configuration for their software (Becker, 2012). The primary use for PaaS is to provide consumers a platform for use in the development, testing, and deployment of applications (Sun et al., 2011).

3. Cloud Security

In cloud computing, the location of data is hard to know at any given time. Information can be spread across the provider's enterprise and collocated with other organization's data. Also, a service provider can subcontract the storage of an organization's information without the consent of the user (Srinivasan, 2012). By collocating information, this creates an information threat because an attacker could potentially gain access to information while attempting to attack another entity. These kinds of attacks can be mitigated through a SLA and the specification of where and how data can be stored (Srinivasan, 2012). Conversely, this can provide security because an adversary may not know where your data is located.

4. Understanding Needs

First and foremost, an organization must fully develop a desired end state upon completion of cloud computing integration prior to determining which company they want to do business with, whether Terremark, First Responder Net, or otherwise. While Marine Corps Installation Command is choosing between different cloud computing solutions, it must understand what schemes marry up with its intended goals. For instance, Terremark's services do not include specialized storage services, an attribute of Terremark that could be a deal breaker for Marine Corps Installations Command should this attribute have an adverse effect on future storage requirements (Baset, 2012).

Concerning cloud infrastructure itself, Marine Corps installation command must be absolutely sure that it requires IAAS to meet its long-term goals, as opposed to platform as a service (PAAS) where each facet of a service stack can be rented to run existing applications or develop and test future applications

(Search Cloud Computing). IAAS requires elasticity built into its scheme if individual machines are required (Goel & Aggarwal, 2013). In PAAS, however, scalability is effective if the organization is willing to recode applications (and has the manpower and time to take on such a laborious task) to take advantage of big data systems (Goel & Aggarwal, 2013). Therefore, an organizations understanding of what they have, what they need, and what goals they desire to reach is imperative before considering cloud computing resources from providers.

B. FIRST RESPONDER CONCEPTS

According to Merriam-Webster, a first responder is defined as an individual "who is among those responsible for going immediately to the scene of an accident or emergency to provide assistance." Thus, for the purposes of this paper, we will consider a first responder as those individuals limited to fire, police, and emergency medical personnel. Emergencies often require a combination of these three types of personnel to respond in order to effectively combat an emergency situation. Therefore, one can see the importance of providing an interoperable medium for these personnel to connect with one another.

Emergency personnel working closely with one another will soon have the ability to share large amounts of streaming data in a manner that is interoperable for every First Responder agency across the United States, expanding communication, control, and efficiencies. For instance, according to Bogden (1998) Florida wildfires led to the evacuation of 30,000 Central Florida residents. Because of these wildfires, Florida enlisted the help of firefighting crews and equipment from states such as Virginia, who sent 45 firefighters from different Virginia firefighting agencies to assist local crews operating in Central Florida (Hopper, 1998). According to Hopper (1998), Florida paid for both the crews and equipment that were sent to aid in fighting the blazes. However, different fire

crews operate under different practices, procedures, protocols, and even communicate using different radio frequencies (GAO, 2007).

These operating differences greatly reduce the efficacy of command and control, and can stall the overarching goal of emergency requisition. Thus, an overarching system that can facilitate information sharing and command and control is necessary for first responders. One example might include the previously mentioned Florida wildfires. Take an individual at ground level requiring the assistance of ground crews that are having difficulty locating that individual, or who altogether are unaware of that individuals need for assistance. A helicopter acquired from an out of state agency that has located that individual needs an effective way to communicate the location and best corridor of approach for rescue crews to remain safe. While data streaming and broadband information sharing was not available in 1998, crews operating presently with the correct interoperable equipment could presumably stream data, video, and voice communications from the out-of-state rescue bird to local ground crews to facilitate a safe and effective rescue.

Commercial use of widespread Long Term Evolution (LTE) services to bring digital communications and broadband data streaming to mobile devices has until this point, been unavailable as a tool for first responder interoperability. Barnett (2012) pointed out the many potential benefits of streaming data to first responders, including the ability to transform first responders' ability to respond to endangered property and individuals, command and control emergency resources and more efficiently affect disaster stricken areas. One can imagine the potential benefits the Marine Corps may have in tapping into such a resource, as Marine Corps installation first responder entities would have access to the same network as local civilian entities. Some perceivable benefits include more efficient training for situational response with law enforcement and medical personnel local to Continental United States (CONUS) installations focusing on situations requiring joint Marine Corps and local response. Additionally, Marine Corps teams responding to CONUS disaster areas would have the ability to tap

into a pre-established network of first responders on scene to more effectively administer aid. The possibilities for a shared LTE network for first responders are incredible, and have been recently realized by Congressional attention.

In February 2012, President Barack Obama signed into law a bill ordering a reallocation of the 700 MHz D block section of the Radio Frequency (RF) spectrum to first responders (Jackson, 2012). The bill had roots in pieces of legislature initiated by Representative Peter King, Senator John McCain, Senator Jay Rockefeller, and Senator Joseph Lieberman, who all expressed interest in a dedicated RF section for first responders capable of passing large amounts of information (Jackson, 2012).

Getting firm support was an uphill battle, as the Federal Communications Commission recommended against the public safety acquisition of the D band in favor of auctioning it off to the commercial industry (Jackson, 2012). Moreover, the bill promised upwards of seven billion dollars from the federal government in order to support the creation of “a nationwide LTE network for first responders” (Jackson, 2012). Jackson (2012) noted that Senator Rockefeller’s intent behind the legislature and funding was to ensure that once the process to create a first responder network had begun, it would be impossible to stop. By 2011, Jackson (2012) noted that a wide majority of Congressmen were behind the project, although discussions were still ongoing as to its implementation and how to write it into law. Once the language of the bill had been solidified, efforts to attach the bill to other, larger, allegedly more concerning pieces of legislature were not successful until the end of 2012 (Jackson, 2012). Upon the passage of the Middle Class Tax Relief and Job Creation Act of 2012, FirstNet was given life, the D band was allocated to first responders, and seven billion dollars was allocated to FirstNet development (Barnett, 2013). The development of this network will be overseen by the First Responder Network Authority, an independent arm of the National Telecommunications and Information Administration (Ferrus, Pisz, Sallent, & Baldini, 2013).

FirstNet is a program established in the Middle Class Tax Relief and Job Creation Act of 2012 (GPO, 2012). The purpose, in general, is to provide first responders with interoperable communications that offer "an array of broadband services" (Barnett, 2013). This program aims to establish a nationwide broadband network that will be implemented between federal, state and local officials. The infrastructure will allow emergency responders and public officials' transparent communications in times of natural disasters and public safety needs (GPO, 2012). Ultimately, FirstNet aims to "erase the decades-long, life threatening calamity of non-interoperable communications" (Barnett, 2013).

The primary infrastructure that is proposed by FirstNet is a "3-in-1" approach (Reynolds, 2013). This approach uses three different communications systems that are employed in unison to create a homogenous network for transparent communications. As Barnett (2013) noted, FirstNet will be allocated a 24MHz bandwidth piece of the electromagnetic spectrum. According to Barnett (2013), FirstNet is currently touting "billions of dollars in federal funding in order to fully realize and implement the current FirstNet plan." The total dollar amount associated with FirstNet is currently estimated to be between two and seven billion dollars (Barnett, 2013). The compilation of multiple terrestrial systems, mobile satellite systems, and deployable mobile systems allow emergency responders the ability to communicate regardless of the method of transmission. The FIRSTNET system ensures that all personnel that utilize this system continually have redundant and reliable communications (Reynolds, 2013).

C. FIRST RESPONDER ISSUES

As with any large scale Information Technology (IT) network, FirstNet is not without its share of hurdles. Many of the current issues that FirstNet faces stem from a lack of precedence for large scale federal interoperable communications networks for first responders. Barnett (2013) noted, "no recipe or model exists" to form the building blocks for FirstNet. Importantly, Barnett

(2013) warned against trying to fit FirstNet into a model currently in existence or to try and fit FirstNet to preexisting system architectures.

The seven billion dollar federal promise is not expected to fund the FirstNet capability from start to finish, simply act as “a much-needed financial jumpstart to a long-awaited broadband initiative” (Jackson, 2012). Ferrus et al. (2013) noted that the government creation of a completely “stand-alone network” is probably not financially feasible, and even if possible, is not practical.

The infrastructure alone required to create a country-wide architecture would be exceptionally expensive, as Ferrus et al. (2013) pointed out that U.S. mobile technology companies have already cumulatively spent in excess of 350 billion dollars. In order to avoid such lofty expenses, the First Responder Network Authority will be forced to levy existing infrastructures from wireless network providers through partnerships (Ferrus et al., 2013). The creation of these partnerships can potentially provide up to 60% savings over a ten year period by forgoing elements such as “site acquisition costs,” which Ferrus et al. (2013) noted as the predominant cause of a large scale network price tag. Additionally, these savings should appear under an “incentive-based partnership model” where network and commercial operators partner together to create and oversee the network operation (Ferrus et al., 2013).

Thus, FirstNet will require such partnerships. Who, then, should be involved in an economic partnership with First Responders? Jackson (2012) touched on the benefits of such partnerships by noting that partners can provide assets that allow congressional funding to be spent elsewhere——assets like “rights of way, fiber for backhaul and additional funding…that could make the network more reliable, robust, and economical.” Additionally, determinations must be made as to what governmental level funding is expected to be disbursed at for procurement (i.e., local, state, federal), and if numerous vendors are appropriate for an overarching system that is “executed in an efficient and cost effective manner that maximizes LTE coverage and application use throughout the nation” (Jackson, 2012). Barnett (2013) argued that First Responder Network

Authority officials must include the desires of state governance and CIO's in order to avoid possible state estrangement that could result in states opting out of the FirstNet program.

Barnett (2013) also pointed out that an overarching system did not mean an overarching architecture. As previously pointed out, congress does not have the capital to create an overarching architecture. Different networks and contracts can work at different levels in different locations, provided they are interoperable with one another. Barnett (2013) asserted that commercial wireless technology firms are mostly "networks of networks or shared architecture networks." Therefore, as opposed to building or contracting for a single architecture, Barnett (2013) argued that the First Responder Network Authority should focus on creating a system of standards to follow in order to ensure interoperability across state lines and the nation as a whole. Ensuring these standards cater to creating efficient, economically feasible networks at any level is a major challenge the First Responder Network Authority now faces. Thus, Barnett (2013) advocates "national interoperability, but local control" in order to facilitate the maximum amount of symbiotic partnerships as possible.

Another example of issues to be worked out is exactly how interconnectivity is expected to work and who exactly is needed to be interconnected. Jackson (2012) noted the example of a burst gas pipe. Should first responders arrive on scene to find a burst gas pipe, first responders can clear the area and handle injuries, etc., but the only agency that can actually turn off the gas pipe is the gas company itself. The gas company would suffer from an influx of calls due to the loss of gas services for its customers, eliminating the ability for first responders to contact the company to respond to a burst pipe that could explode at any moment. Assuming worst case scenario that the gas company is located across town, the situation fosters wasted time and plausibly exposes individuals to more danger as opposed to the gas company responding simultaneously with first responders should they both be properly interconnected and dispatched (Jackson, 2012).

Considering the unending list of potential scenarios requiring interconnectivity with civilian entities or other government bodies in order to be efficient, the determination as to exactly who communicates across FirstNet and when their participation is appropriate must still be made. Mass disaster situations such as hurricane Katrina requiring many different government, civilian, and even military units operating together is exactly the type of situation where FirstNet could streamline command and control and foster efficiencies in cleanup efforts. However, a plan must be made as to how these organizations are expected to communicate across FirstNet.

According to Jackson (2012), many First Responders are currently using portions of the T-band, set to be reallocated for FCC auction over the next ten years. Upon acquiescence of this band, departments will immediately require a functioning network to transition to. Jackson (2012) pointed out that these departments may not have a system to transition to should FirstNet not be mature or available in their area. Moreover, clarity is required in determining the need to strip departments of the T-band in order to auction it off even if there are no bidding companies (Jackson, 2012).

A costing model for FirstNet does not currently exist, although its creation has been asserted (Barnett, 2013). The lack of a current costing model complicates FirstNet buy-in for potential users, and according to Barnett (2013), this lack "causes mistrust among its customers and confusion among its stakeholders." Barnett (2013) argued that the "costing model and…financial analysis" is incredibly important for explaining to customers the cost of the network, available services, and inner workings of the system itself. Coincidentally, Barnett (2013) noted that he did not believe the burden of creating a costing model should be on the shoulders of the FirstNet Board or the National Telecommunications and Information Agency (NTIA). Barnett (2013) went on to explain that "a major milestone would be to hear that one or more studies has been contracted for to produce a cost model and financial analysis…"

III. FIRST RESPONDER MODEL OVERVIEW

A. CURRENT USMC FIRST RESPONDER OPERATIONS

The following is a case study conducted at security and emergency services battalion aboard Camp Pendleton, California. The case study was conducted from operational, technological, and user standpoints in order to gain a better grasp on the current state of Marine Corps first responders. The study was conducted March of 2014.

1. Security and Emergency Services Current State

Security and Emergency Services (SES) Battalion aboard Camp Pendleton, California, is an organization of both Marine Corps and civil personnel built to "provide law enforcement and security, fire protection, emergency medical response and temporary detention in support to Marine Corps Base Camp Pendleton in order to protect life and property, promote quality of life and preserve good order and discipline" (Pendleton.marines.mil, 2014). SES covers all 911 calls aboard Camp Pendleton and responds to any and all emergency situations, both civil and military aboard the installation, and is organized into a battalion structure. Thus, SES personnel operate with numerous pieces of gear, communications equipment, and information technology (IT) systems that are in some cases interoperable with outside civil entities and in some cases not interoperable with one another. This chapter will assess the current state of SES structure (as indicated in Figure 3), equipment, and IT systems using SES aboard Camp Pendleton as a case study.

Figure 3. SES Battalion Structure (from Pendleton.marines.mil, 2014).

The following information was gained through a site visit with Security and Emergency Services Battalion aboard Camp Pendleton from 24 March 2014–28 March 2014:

a. Local/Organic SES infrastructure

Tying SES operations together on a daily basis is the current 911 system in use by SES personnel. The 911 database system is sustained by the state, to include the components and equipment. Therefore, the state of California pays into public safety answering points (PSAP), which can be defined as "a call

center responsible for answering calls to an emergency telephone number for police, firefighting and ambulance services (techopedia.com, 2014)." Furthermore, "a PSAP facility runs 24 hours a day, dispatching emergency services or passing 911 calls on to public or private safety agencies (techopedia.com)." While the 911 database system is sustained by the state, 911 calls feed into the Camp Pendleton dispatch center when applicable. Camp Pendleton SES does not actively try to acquire money with which to administer maintenance to the 911 PSAP. Rather, SES queries state PSAP administration officials for required maintenance that falls outside of normal upkeep under the PSAP plan.

SES systems that require maintenance include an audio logger, the 911 dispatch system, and a fire station alerting system. Between these three systems, maintenance costs for SES are roughly $17,000 a year. When an individual makes a call via cell phone or one of the Camp Pendleton housing areas, the call is routed to the 911 server which populates in the dispatch office. Because of the current base certification/accreditation concerning base office telephone numbers, telephone numbers that are issued cannot touch (i.e., be updated to) the 911 database system and must be manually updated roughly monthly in the Camp Pendleton 911 dispatch servers via hard disk. In early 2014, one such update took place and required the update of approximately 20,000 phone numbers. This process is in contrast to a concept in place at the Pentagon, where the phone database downloads at 0200 each morning to the 911 database system automatically, keeping all phone numbers up to date for first responders in near real-time.

Various contractors including General Electric for the fire station alerting system, Cassidian Communications for the 911 dispatch system and subcontractors for the audio logging system are used for maintenance issues on the three systems requiring upkeep from SES. Most contractors are bound by contracts requiring four hour response time, but usually they can facilitate support via telephone quicker than the four hour requirement. IT dispatch

personnel spend a large amount of time maintaining the current systems outside of the intended work of required updates and backups on the systems.

Sources of good updates for the current systems are hard to come by, as the systems were purchased before all of the current IT staff began their work at SES. The age of the systems are the key problem, as each system has been individually information assurance (IA) accredited in order to ensure DOD standards of confidentiality, integrity, and availability. These IA standards are not the same standards that civil institutions must adhere to, and may vary by locale. To revert back and accredit these systems to work with one another is expected to be as expensive as replacing them. The systems were individually purchased, not necessarily with interoperability as the primary concern.

2. Comparative Organizations

Installations similar to Camp Pendleton have a high degree of self-sufficiency, although interoperability would potentially increase efficiency resulting from a shared database structure. Small installations such as Barstow, California would particularly benefit from a shared database structure with local California Emergency Responders. Similar sized installations must rely on local Sheriffs and municipalities for ambulance and law enforcement services.

Camp Pendleton SES, particularly fire fighters, routinely helps with California responders using VHF radios. Often upon arrival to unfamiliar areas, the on scene command will necessarily have to provide a way to patch VHF radios. Despite the ability to patch these radios so that every member can be tied into a command and control structure, voice is the only information that can be passed.

In comparing existing equipment aboard Camp Pendleton versus local emergency responders, San Diego police officers have more advanced equipment where the officers themselves can run queries from their vehicles or mobile devices. The provost marshall's office (PMO), or the Marine Corps equivalent to police on Camp Pendleton, is still required to radio information to a

central authority that processes the requests and retrieves the required information.

With regard to the local southern California terrain aboard Camp Pendleton, Marine Corps Installations West Communications Division (G6) is planning additional towers to cover some of the gaps created by local hills and valleys. Currently some areas with ravines require climbing to higher ground in order to communicate. Reporting status of fire generally requires transportation to the nearest scalable hill in order to report it. The operations officer will receive a status, determine where the responders are in relation to the fire and progress, and report it to the G6. While attempting to integrate an archaic computer aided dispatch (CAD) system to create efficiencies in dispatching across the radio network, pushed data packets sat in a queue. The data packets were stalled as voice communications took priority over the system and bandwidth was not large enough to handle the amounts of information required to pass. By the time an official call came in for a fire related emergency after the CAD was able to push the information through, the responders were already on scene, as they are required to respond in seven minutes 90 percent of the time for one engine.

Existing equipment provides required interoperability for Joint operations with civilian responders across San Diego County at a minimal level. Concerning local Marine Corps installations such as Miramar, interoperability is seamless, as Miramar allows the use of the same equipment and radio frequencies that Camp Pendleton responders use. Outside installations in the local area, SES has the ability to program Harris 152 radios in order to respond to fire crises. PMO, however, maintains only VHF radios and has little interoperability with local entities.

Outside the local area, if SES could not program its radios to the in-use frequency, SES operators would be required to use temporary radios borrowed from other responders. Other means of communications for disaster relief include a G6 mobile communications van that can create its own network, and was on scene during hurricane Katrina disaster relief. Additionally, for disaster relief, it

may be the MEF who responds as opposed to SES, as the MEF has more personnel, equipment, and capabilities to bring to a large-scale disaster. In situations where MEF responds as opposed to SES, MEF would likely use its own communications network to operate more singularly as opposed to full integration with responding personnel.

When most mutual aid responders arrive to a scene requiring assistance from local municipalities, Camp Pendleton firefighters switch to their VHF radios, which are common across municipalities. PMO currently cannot talk to its counterparts out in town on existing equipment. There are no MOA's to communicate with other agencies for PMO out in town, the only way to do that is to build a patch through dispatch to communicate to other responders. California Highway Patrol may have an incident that requires joint attention that would require a face to face before communications could take place. On the fire side, personnel can program radios on the fly if necessary within the bounds of their Harris radios. The S6 can help program or acquire a radio from a mutual partner to assist in programming radios for joint firefighting. With regard to the numerous frequency ranges used aboard Camp Pendleton (including radios in vehicles of all types: planes, armor, etc.), bleed over and interference from other radios is not an issue. Lack of bleed over is due to the planned and evolved assignment of equipment and radio frequencies.

3. LTE Considerations

Mobile LTE device use by SES personnel in their vehicles and on their persons has the potential to help establish a massive decrease in dead zones. Dead spots are primarily a symptom of local mountainous terrain, of which mobile networks can provide relief. This decrease is especially true when combined with satellite communications to further eliminate dead spots aboard Pendleton. Moreover, the increased speed and bandwidth would increase capabilities for SES personnel, to include faster response times, mapping, greater on-scene situational awareness, and enhanced command and control.

There are ways that LTE service could inhibit current operations, should it be improperly used or cause information overload. If multiple radios are used, radios that have less priority can be turned down in order to focus on the line that is most important. Should mobile devices not allow for prioritizing bands in some fashion, devices could potentially become overburdened. However, if information could be directionalized to responders over certain allocated bands, this problem could be overcome. The problem would remain for multiple agencies responding that may require a hierarchy of directionalized communications in order to facilitate C2 for a given incident response. Additionally, much of LTE service is carrier dependent, and different carriers provide better or worse service depending on location.

4. SES Civilian Interoperability

Existing database infrastructures for Security and Emergency Services Battalion at Camp Pendleton model a stove piped structure where databases do interoperate, and require manipulation and monthly updating from personnel in the dispatch offices. According to the SES personnel, San Diego County worked to consolidate CAD systems. Under the regional and county interoperability project (RCIP), sections of San Diego County consolidated their CAD systems. Had Camp Pendleton been able to participate, San Diego County dispatch agencies could have been able to dispatch Camp Pendleton units to local calls and vice versa should the situation dictate. Essentially, Camp Pendleton dispatchers could have been able to dispatch Oceanside personnel. The dispatch of Oceanside personnel could have occurred in the joint area if calls were directed to Camp Pendleton dispatch where Oceanside personnel were more appropriate responders. The dispatch of Oceanside personnel would also be appropriate if a situation arose where Camp Pendleton required the support of Oceanside responders. Many of the county systems were already tied in together for mutual support. Camp Pendleton was still trying to gain interoperability among stand-alone systems in early 2014, and due to the fact that the standalone systems could not talk to one another, gaining interoperability with nearby San

Diego county systems was not possible. Moreover, Camp Pendleton SES does not currently have a CAD system, therefore are not able to pay to tie into the system. Resultantly, accreditation for joining the existing system aboard Camp Pendleton to San Diego County systems could not be completed. The current SES dispatch process is indicated in Figure 4.

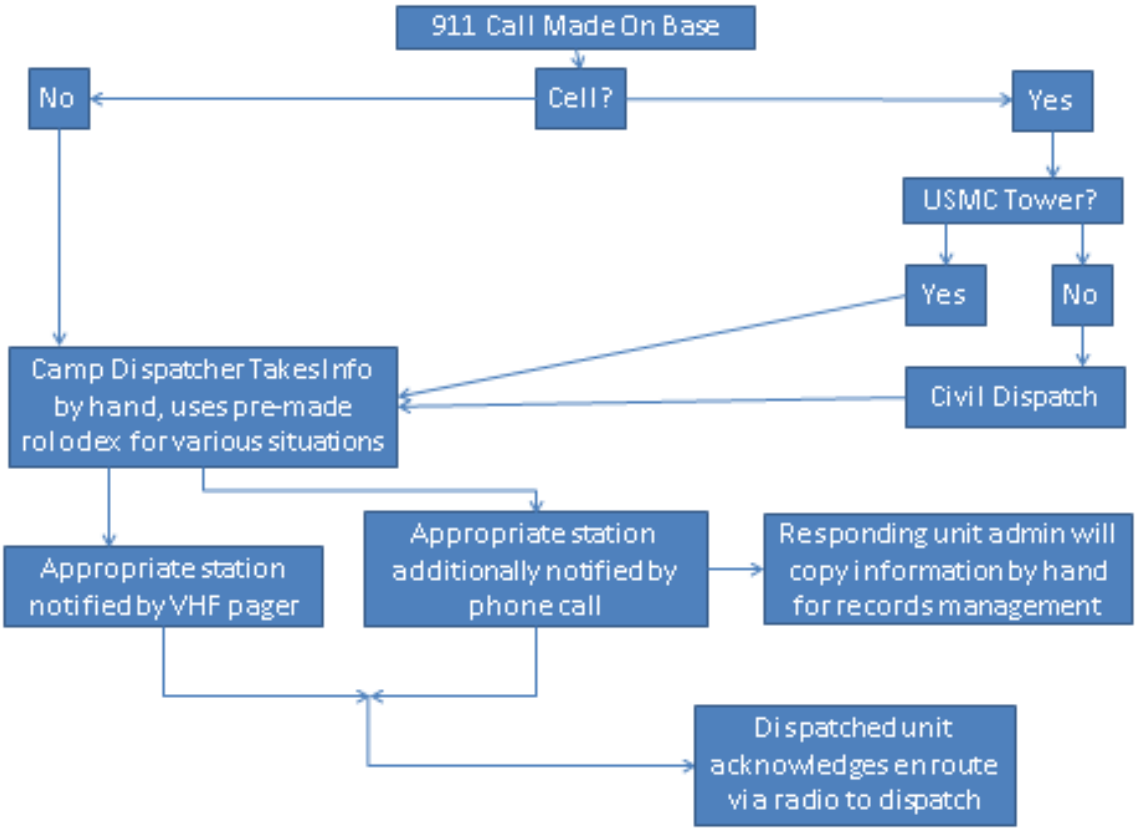

Figure 4. 911 Dispatch Process

Several procedures are in place for interoperability with local and state level emergency services. A fire truck coming on base can communicate with dispatch notifying dispatch that the unit is on base. Dispatch has to communicate which talk group on-scene units are operating on. Dispatch will direct the arriving units to the scene of the applicable incident, since units arriving on base may not be able to communicate with on-scene units prior to a face to face with on-scene

responders. Talk groups are regulated by the state, specifically the California Forest Service, and must be coordinate prior to use by Camp Pendleton responders.

PMO currently has only one MOA with the Oceanside police department, which helps to process turnovers with civilians that need to be removed to an outside agency that PMO does not process. The Fire Department has multiple MOU's and MOA's with mutual aid partners that are handled through the G3/5 to include updates. In June, Camp Pendleton hosts a fire school with the forest service, CalFire. Oceanside and other California fire agencies train aboard Camp Pendleton to train new captains and perform incident type scenarios for running engine companies. On the law enforcement side, because Camp Pendleton PMO interacts in a limited manner with local agencies, a lot of cross training has been eliminated. For instance, PMO previously trained with the local sheriff's department, and it was misconstrued that PMO was actually performing law enforcement in violation of posse comitatus. The Posse Comitatus Act states, "Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both (Brinkerhoff, 2009)." Essentially, while PMO may train with civil organizations, PMO may not carry out law enforcement in civil locales unless authorized by congress. Most training for PMO and fire department are done at the department level. PMO is comprised by roughly 400 people managed by a Lieutenant Colonel. The Camp Pendleton fire department is managed by the fire chief, which is comprised of about 175 people. Communications systems that are more interoperable with local agencies would allow SES personnel to operate more efficiently. When big fires occur, SES requests to other agencies dispatch centers for support.

LTE style service with mobile devices could assist interoperability with civilian counterparts namely by reducing the equipment carried and ensuring a quick network join when arriving on scene. Should SES personnel be able to go

from three radios to one cell phone or a tablet to do law enforcement and firefighting work, that reduction could economize the amount of equipment and add to the advantageous information flow to first responders.

Numerous issues could arise in trying to create joint LTE networks across local or state departments. Sending personally identifiable information (PII) information across CADs to local municipalities regarding Camp Pendleton personnel likely would not be able to occur. A more probable outcome is a generic request for an asset across the base boundary in order to gain the resources responders need from available units outside (e.g., responders need an ambulance for an individual who is experiencing heat related issues). There must be to be memorandums of agreement (MOA's) developed regionally. Instead of local memorandums of understanding (MOU's) and MOA's, regional efforts to bring in all agencies that might be involved in overlapping networks would consolidate efficiency gains. Currently, the Marine Corps Installation West Plans Division (G5) maintains MOU's and MOA's with local agencies. When considering local MOU's and MOA's, Camp Pendleton Fire has far more interoperability and communication than PMO. The increased interoperability for Camp Pendleton Fire is partially due to posse comitatus, as Camp Pendleton Fire does not engage in policing actions.

5. Infrastructure

The Camp Pendleton SES Battalion operates four primary information systems that support the reporting process for incidents received by its call center: a 911 reporting system, an audio logger, the fire alarm reporting system, and fire station alerting system. All of these systems are supposed to work together to assist in identifying an emergency, recording all pertinent information, identifying fires on base and automatically alerting the dispatch center or the fire department in case of an emergency. Each system has a unique function in this process, which assists the dispatcher in ensuring the right personnel are able to respond to an emergency with correct and timely information.

The 911 reporting system is responsible for assisting the dispatcher with precise location and pertinent information, which will be forwarded to either military police, fire fighters or EMTs. If an individual is calling on a cell phone, the 911 system uses cell towers to identify an individual's telephone number and accurately isolate an individual's location on the installation. When an individual is calling from on base housing via a commercial telephone, the system will identify the phone number that is being utilized and provide the dispatcher with the street address of the caller in order to identify the location on the installation. However, if an individual calls 911 from a base telephone, the system will provide the dispatcher with the individual's base telephone number and a building number, which identifies the location of the building on the installation.

The 911 system utilizes three different methods of identifying an individual's location depending on the way that someone could call 911, either a cell phone, commercial land line, or government land line. This provides an added layer of depth and translation for the dispatcher to relay information to one or many first responders. Using a cell phone will provide the dispatcher with a geographic location, which is not directly tied to a street address and may have an error in the precise location, depending upon the number of towers that are used to triangulate an individual's location. When calling from a commercial line, the dispatcher is provided the street address that is registered to that number by the commercial provider.

However, for base phone numbers, the information provided is based on a listing of phone numbers that are associated with certain building numbers. Over time phone numbers and are switched from one building to another, which requires constant updating. The 911 system is not accredited to operate on the Department of Defense network, because of its information assurance accreditation and the fact that it connects to outside networks. This creates an issue when trying to update base phone numbers and their associated building number. With commercial phone lines, the system can update automatically if a phone number changes to a different street address. Since the system is not on

the DOD network, the updates for base phone numbers and their building number must be updated manually. The dispatch office receives these updates on a disc from the base, which are then uploaded into the system to ensure the dispatcher has the appropriate information to forward to first responders.

The Audio Logger works with the 911 system to record all information once a call is received at the dispatch center. The Audio Logger is also connected to and passes information to the central database, which records all information for an individual's call. This system, in conjunction with the official database ensures that an audio recording of the entire call is maintained in permanent records in addition to the ANI/ALI (Automatic Number Identification / Automatic Location Identification) information.

Most buildings on the installation are equipped with a fire and/or security alarm system that can send a signal to the dispatcher in case of an emergency. The Fire Alarm Reporting System is a system that is operated by SES and maintained by General Electric. This system receives an automatic notification when smoke or a fire is detected on the installation, which allows the dispatcher to send first responders immediately to investigate the issue or attend to the situation. Additionally, there are sensitive areas, such as classified spaces or places that house weapons or ammo, that have security alarms in case of a breach of security. If one of these systems is tripped it will also notify the dispatch center in order to allow the military police to respond to the situation.

The Fire Station Alerting system is a system that is operated by SES and maintained by a subcontractor to alert individual fire stations. When a call is received or a fire alarm is tripped this system allows the dispatcher to notify a specific fire station in order to respond appropriately. This system allows the dispatcher to identify the specific area where an incident has occurred and activate only those first responders that are needed to according to its geographic locations.

The SES Battalion operates all of these systems, but contractors maintain most of these systems. Due to these systems being operated by different contractors there is not a great deal of interconnectivity between them. Additionally, each system that is maintained by a contractor has its own maintenance contract and warranty. If there is an error or failure in the system, SES must contact a specific contractor in order to repair that system. The onsite maintenance response time for these systems is four hours, but the contractor can also assist SES personnel via phone in order to assist them in repairing the system.

6. Equipment

As discussed with Marine Corps Installations West G-6 personnel, the primary means of communication for first responders is via three different radio systems. Security and emergency services personnel operate using VHF, four hundred (400) megahertz MHz, and eight hundred (800) megahertz radios. These three radio systems operate in different portions of the electromagnetic spectrum and are used for different purposes within the organization.

The primary system used is the 400 MHz radio network, which applies to military police, fire and EMTs for voice and limited data on the installation. This system is supported by a network of repeater sites that expand coverage throughout a majority of the base. On Camp Pendleton, it is planned to ultimately have six repeating towers located on the installation and three repeating towers located outside the boundary of the base. The system of repeating towers allows for approximately 95 percent coverage for the 400 MHz network throughout the installation.

At each repeating site, there are capabilities that facilitate the continuity of service in the case of equipment failure, power outage or natural disaster. Each site has redundant equipment, which allows for a backup in case of a primary system failure. Also, each site is outfitted with a power fail over capability to a local generator in case of an outage. Each site can operate for approximately

eight hours with its organic fuel supply prior to needing a resupply. These capabilities allow for continuous service while maintenance personnel can service an equipment failure or restore power to the repeater sites.

The 800 MHz and VHF systems utilized by first responders are for backup communications or mutual aid with outside agencies. Police and fire fighters in the local area surrounding Camp Pendleton operate primarily on an 800 MHz system and have no ability to utilize the 400 MHz system used by SES Battalion. Therefore, SES personnel must carry an additional radio when conducting operations off base.

When conducting operations on base with outside agencies supporting, SES personnel are required to utilize a VHF system. The local fire and police 800 MHz system does not have full coverage on base, which forces all first responders to operate on VHF. The VHF system allows for local communication, but has a limited range and not the level of coverage of the 400 MHz network.

7. Information System Interoperability

The information systems that are utilized by SES are largely independent of the DOD network. These information systems were procured and installed in the early 2000's. At the time they were designed and implemented, they were not information assurance accredited. Therefore, these systems could not be integrated into the DOD or Navy Marine Corps intranet (NMCI) network. This caused issues with interoperability because SES has to maintain a commercial network infrastructure in order to system these systems and still operate on the DOD network as well. Any information that must be transferred between these two systems must be done manually or by migrating the information via disc.

Additionally, the information systems utilized by the dispatcher are all maintained and created by different contractors. This creates an issue when trying to collect information or notify a specific agency in response to an emergency. These systems could be made interoperable, but that would require

additional resources and training in order to allow these systems to communicate and pass information to each other.

Differing radio systems that operate on different frequencies complicates the interoperability of SES personnel and local first responders. These differing systems require SES personnel to carry additional equipment, attend additional training, and spend more money on maintenance and procurement of additional equipment. Also, operating on different systems creates confusion in communicating between these agencies. Without common or interoperable communications systems, the flow of information between first responders is greatly reduced. Additionally, while conducting mutual aid operations on base, the incompatibility of these systems requires first responders to utilize VHF systems. With the VHF network there is a reduced capability for communication and is limited to only voice communications.

As discussed with MCI West G-6 personnel, a method being utilized for interoperability between SES personnel and local first responders to initially establish communications is via cellular phone. The dispatcher or military police officer will use a personal cell phone, or government cell phone if available, to contact their civilian counterparts to work through which method of communication will be utilized. The process is necessary, however, it is time consuming and in the case of a natural disaster the cellular network could potentially be saturated.

B. SHORT TERM USMC FIRST RESPONDER ENHANCED CAPABILITIES (EMC2)

Marine Corps Installations Command, in conjunction with Marine Corps Systems Command, is designing and implementing a new family-of-systems, which provides first responders with enhanced and updated systems. The new system, called Emergency Management Command and Coordination (EMC2), will replace a great deal of existing and outdated systems that are currently in use today. “The desired end state for EMC2 is the seamless ability to

expeditiously integrate diverse communications media to effectively handle all emergency management communications functions, such as call for service, dispatching, and response (Headquarters, United States Marine Corps, 2012)." This family of systems will provide a level of integration that will enable first responders to access and share information more rapidly and thus reducing the response time in disaster situations.

EMC2, as displayed in Figure 5, is a capability set that is a holistic system that integrates wired (Base Telephone Infrastructure) and wireless (E-LMR) communications into a central information system known as the Consolidated Emergency Response System (CERS). The system also integrates key public safety programs, such as the Mass Notification System, Fire Station Alerting System, Fire and Security Detection Sensors and the chemical, biological, radiological, and nuclear (CBRN) Sensing Networks (Headquarters, United States Marine Corps, 2012). The integration of all these systems allows the dispatch center to quickly receive and disseminate information to first responders on Marine Corps Camps and Installations.

One of the primary focuses of the EMC2 system is the CERS. The "CERS is required to provide the Marine Corps installation commander the same level of emergency response capability as the civilian populations outside of the military installation (Headquarters, United States Marine Corps, 2012)." The CERS is a highly integrated system, which is scalable to support larger Marine Corps Installations and smaller camps or stations. Additionally, this system will interface with the Mass Notification System and electronic security systems installed in buildings (Headquarters, United States Marine Corps, 2012). These new capabilities will allow first responders to easily view and pass along information that currently requires multiple independent systems to accomplish.

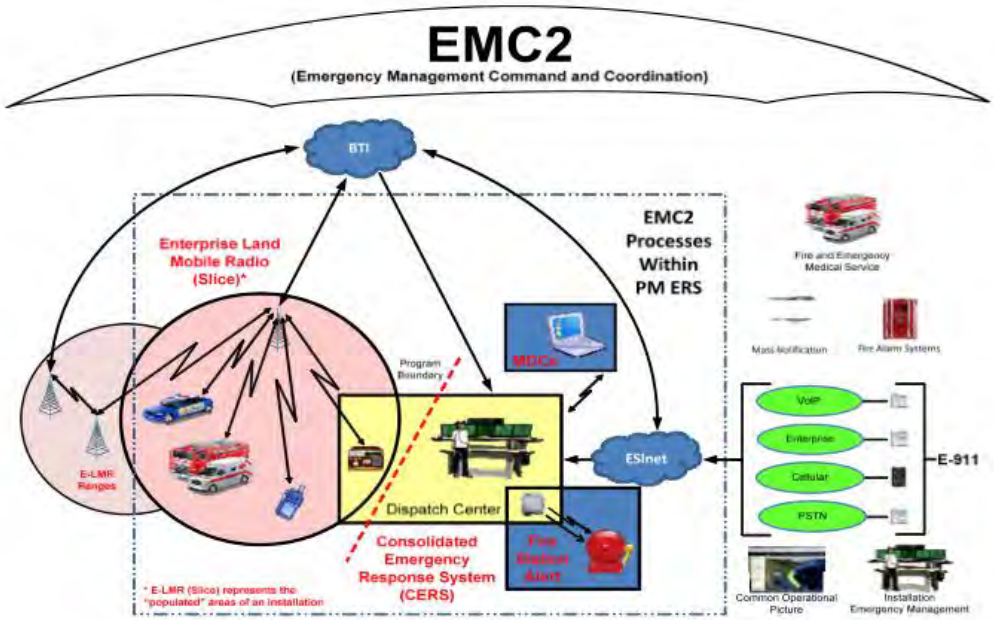

Figure 5. EMC2 Umbrella (from Headquarters, United States Marine Corps, 2012)

1. Equipment

The equipment supporting EMC2 will largely be utilizing a good deal of the existing base telecommunications infrastructure with some additional upgrades to increase throughput and processing speed. EMC2 will utilize the existing base telephone system in addition to commercial telephone services from local providers (Headquarters, United States Marine Corps, 2012). However, additional lines will be added that provide specific E911 trunks that are dedicated to support the E911 system. This additional infrastructure will ensure that all government and commercial landline calls or commercial cellular calls, originating from with the installation, will be able to reach the dispatch center (Headquarters, United States Marine Corps, 2012).

Using the Enterprise Land Mobile Radio (E-LMR) network, which is currently integrated into most major installations, will provide the needed radio services for first responders. E-LMR is a current system in use, which provides

first responders with a voice and data capability utilizing the 380–400 MHz band (MARADMIN 497, 2007). The system is truncated to provide a more reliable means of communications over a longer distance (MARADMIN 497, 2007).

To support the CERS and E-LMR systems, the Emergency Services IP Network (ESINet) will be established to provide the network backbone for packet and circuit switched services (Headquarters, United States Marine Corps, 2012). ESINet is segregated from all other installation networks and traffic. It is designed to be interoperable "with DOD, Joint Services, other federal agencies, and state and local government First Responders (mutual aid) (Headquarters, United States Marine Corps, 2012)." With the system segregated from other networks and interoperable with other first responder entities, it will allow for closer coordination and greater information sharing. Additionally, the system will be backwards compatible with existing command and control systems.

2. Information Systems

The Consolidated Emergency Response System will be the backbone dispatching system, which provides dispatchers with enhanced capabilities over the current systems in use. The system will integrate the E911, Computer-Aided Dispatch System, Records Management System, and Fire Station Alerting System (Headquarters, United States Marine Corps, 2012). Integrating these systems into one homogenous system will allow dispatchers and first responders more rapid access to critical information. Additionally, digitizing the system will provide the dispatcher the ability to more quickly input information, instead of trying to rely on paper and pencil recording of information during 911 calls. This information can then be quickly uploaded to first responders on the ground.

CERS will leverage commercial-off-the-shelf (COTS) technology to integrate the many of the supporting system modules (Headquarters, United States Marine Corps, 2012). By utilizing COTS equipment it reduces the timeline in procurement and certification of the system. This process will reduce the time and potentially the cost to develop the system, because there would be no need

to design or manufacture a propriety system to meet these specifics for the program. Another key gain from using COTS technology is the scalability it would offer for when establishing the system on the many separate installations (Headquarters, United States Marine Corps, 2012). Utilizing COTS allows each commander, at each installation, the ability to customize his or her system according to specific needs.

3. Interoperability

With the implementation of EMC2, interoperability is a key issue that is addressed. Radio systems and spectrum usage are key issues to ensure communications capability between first responders is a fluid process. Additionally, it is important to use commercial-off-the-shelf technology is new information systems to ensure that these systems can be upgraded and improved throughout the lifecycle of the program.

a. Enterprise Land Mobile Radio System

The Marine Corps Network Operations and Security Center (MCNOSC) is the approval authority and spectrum manager for the E-LMR system, which will be utilized with EMC2 (MARADMIN 472, 2007). An issue with the current first responder network is the ability to communicate with local first responders in mutual aid situations. Federal, State, and Local first responders are currently utilizing the 700 MHz band for radio communication, where E-LMR operates in the 380–400 MHz band (MARADMIN 497, 2007). This would present similar issues as previous radio networks, which it would require first responders to carry additional equipment and conduct prior coordination prior to integrating outside entities into mutual aid situations.

However, E-LMR is utilizing the international standard, Association of Public-Safety Communications Officials Standard 25 (APOC-25), trunked system and associated command and control systems, which is the standard that is used at the Federal, State, and Local levels (MARADMIN 497, 2007). By utilizing APOC-25 standards, individual installations may request the integration of other

frequency bands, such as the 700 MHz band, into s system to allow better communication in mutual aid situations.

b. Commercial Off-the-Shelf Technology

The use of commercial off-the-shelf (COTS) technology is beneficial to the acquisition and implementation of the EMC2 system. It reduces time to develop and deploy to new system with proven technology utilized in the commercial sector. With the integration of COTS technology into EMC2, each commander can tailor the system to meet the needs of each particular installation. The final system will be certified and approved to ensure that it is in accordance with EMC2 standards and meets national, regional, and local requirements (Headquarters, United States Marine Corps, 2012).

This provides greater flexibility not only to tailor a system to site-specific needs, but also provides an opportunity to deviate from the system as originally designed. Different commands may update different components at different times, which could lead interoperability issues within the USMC system or with their local civilian counterparts. This is beneficial because the commander can ensure the system is upgraded with the latest technology, but also must be synchronized with partner entities to ensure they maintain interoperability.

c. DOD Accreditation and IA Compliance

An issue with some current first responder systems in use is that they are not accredited and certified for use on DOD networks. This requires them to operate on independent commercial networks and equipment, without logically or physically touching DOD systems. This creates an in issue with trying to transfer or update information from base services in order to integrate that information into dispatching information systems.

EMC2 and the CERS systems will comply with DOD certification and accreditation processes. Additionally, the goal is to certify these systems as fully IA compliant (Headquarters, United States Marine Corps, 2012). This will allow

the CERS system and other information systems the ability to connect to DOD networks and integrate and update essential information on a daily basis. The IA capabilities provided in all EMC2 systems will ensure security and protection of information that is maintained within the system and on the servers (Headquarters, United States Marine Corps, 2012).

Having a DOD accreditation and IA compliance is essential to ensure the integrity and availability of information on DOD networks and providing interoperability between camp services and first responders. However, a system that is operating or connected to a DOD network must have to same IA compliance as established by the DOD. This becomes an issue when trying to integrate information from state and local municipalities. The local municipalities system must have the same level of security as DOD networks in order to integrate systems and information, such as the Computer-aided Dispatch system. Without this security compliance level, either the installations first responder system must be segregated from the DOD network or with not be able to fully integrate with state and local municipalities.

C. LONG TERM PROGRAM ENHANCEMENT OPPORTUNITIES WITH FIRSTNET

The following information was gained through conversations with the DOD Public Safety Communications Working Group, the liaison between the First Responder Network Authority and the DOD:

1. Role of FirstNet in the DOD

The role of the DOD in the U.S. can widely be viewed as fighting and winning our nations wars. Relating to the role of FirstNet in the DOD, FirstNet will play a role in our tertiary responsibilities to include defense support of civil authorities and the protection of troops within the United States. FirstNet will be able to be applied to public safety communication requirements within DOD installations. It will protect troops from outsiders and in some instances protect troops from one another. It will ensure, from the public safety perspective, that

the best capabilities are available aboard DOD installations. The value added by FirstNet to installations includes geolocation, data to the edge for first responders, interoperability, and expanded and ubiquitous coverage.

2. FirstNet Value added

The presumed value added in conjunction with the previously mentioned current state of SES is important to note in several ways. First, geolocation continues to be an issue for first responders at Camp Pendleton; as mobile mapping data is minimal to nonexistent and addressing issues (i.e., building numbers vice typical street addresses) continue to plague responding personnel, especially from outside civil agencies. Allowing the use of mapping data and other information at the edge can not only help to decrease response time, but additionally allow safer, more efficient responses from responders. As an example, PMO aboard Camp Pendleton currently has the use of only VHF radios. Any information passed to responding PMO members must be passed either prior to dispatch or en route via radio communications. With data pushed to mobile devices, there are far fewer limitations to what information can be passed. A responding PMO member would have the ability to arrive on scene with greater situational awareness, including known registered weapons at a domicile, prior calls regarding similar situations with suspected persons (historical data, etc.). This kind of information can additionally help dispatchers determine economy of force when dispatching units, allow civil responders the same or similar information depending on information assurance issues, thus increasing interoperability, developing a common picture, and encouraging synergy of efforts with civil authorities.

3. Coverage

Expanded and ubiquitous coverage is an important addition to U.S. DOD installations. While not every installation has the same First Responder budget, coverage, and personnel at hand, FirstNet can provide a way to help bridge this gap. Small installations that use memorandums of agreement with local law

enforcement to patrol installations will likely benefit first, as civil responders will see the positives of FirstNet prior to DOD responders. As far as expanding coverage, mountainous locations such as installations in Southern California will see added coverage with satellite communications that can cover gaps that do not exist in more open locales such as east coast installations.

4. FirstNet Outlook

While FirstNet is a system that is set to take place long after EMC2, foresight must be used to help bridge the gap between EMC2 and FirstNet. The aforementioned analysis of EMC2 and the current state of Camp Pendleton first responders allows insight into what role FirstNet might play in the Marine Corps and DOD as a whole. Unity of command potentially provided by FirstNet, funding means, and the current goals of FirstNet are all factors important to note when analyzing FirstNet for the future.

a. Current State

Despite the optimistic outlook of FirstNet, the role of FirstNet in the DOD is in the early stages of development, and will evolve over the duration of its development. Importantly, FirstNet and the DOD Public Safety Communications Working Group will have the capability to transform opinions of those outside the DOD in the public safety sector. These civil entities may not view the DOD as an organization that has for years addressed public safety across its installations. The DOD Public Safety Communications Working Group has the opportunity to break down these preconceived notions that may not view the DOD as a relevant player in public safety. In essence, the DOD Public Safety Communications Working Group has the ability to build stronger communications bridges with civil public safety members through the FirstNet project by creating a common understanding of how public safety is viewed by the DOD and civil authorities. This understanding will benefit the DOD as a whole regardless of FirstNet's outcome.

Consider that an installation operates much like a city, where an installation commander and a city manager have similar responsibilities in providing public safety to their members. In this sense, execution in identification and application of requirements is remarkably similar. Certain organization components exist from the installation commander's perspective outside the boundaries of the installation. The installation commander may require the support of outside public safety entities for an event, and would necessarily express that need in a way that resonates with both sides. At a local level, this understanding has been established at locations such as Camp Pendleton. As these understandings exist at the local level, the next logical step is to create and exploit the benefits of such understandings at the defense, federal, and national level.

b. Unity of Command

A major improvement to DOD first responder operations themselves that FirstNet has the potential for improving is that of unity of command. Unity of command is "the principle that no subordinate in an organization should report to more than one boss (Unity of Command, Businessdictionary.com)." An incident team chief may have fire and in some cases force protection issues and safety of life issues. The 9/11 Commission Report identified unity of command problems after initial response at the Pentagon. The side of the building was exposed to open air, federal law enforcement had problems with open air classified material and areas, firefighters had to put out fires and protect lives, and EMS was involved to provide injury support. Considering all of these assets——federal, state, local, and installation——necessity is derived for an agency in charge to show unity of command and focus efforts. This agency must additionally be able to handle potential classification issues, and assign assets accordingly. The DOD TEAM aims to mitigate problems in providing unity of command at least through a concept of operations, if not through a single network. FirstNet could provide this mitigation through a single broadband network that would allow response teams to more easily adhere to a unity of command. Further, attempting to put

everyone on a single network may highlight the necessity for having clear roles, responsibilities, authorities, and relationships in a way that may not have been experienced before. While there are tremendous benefits in terms of application of resources, economy of effort and unity of effort, but there is also necessity to ensure that the conditions are right for facilitating these benefits.

The disparity between communications equipment is an issue today that FirstNet has the potential to improve. Issues occur when organizations arrive at a single crisis and join or turn over with other organizations and are forced to use shared resources in order for communication to take place. Shared resources infer that units that would normally have their own equipment and provide better economy of force must share potentially unfamiliar equipment. These units may be tied more closely to others in order to facilitate communications. This lack of unit flexibility hampers economy of force, where units otherwise might be able to spread the work more efficiently. Moreover, adding a shared resource such as FirstNet could potentially be a huge enabler toward formalizing training and disaster relief command structures.

c. Physical versus Virtual

FirstNet itself can currently be described as in the beginning stages of brainstorming. Importantly, whether FirstNet is going to be a physical asset comprised of data centers, networks, and computers or if it is going to be a virtual asset where the tools to join a network with rules regulations and guidance prescribed by the Department of Commerce is yet to be determined. Local municipalities that own all of the hardware, software, or centralized data servers may deliver information to municipalities at the edges. FirstNet may also become a combination of both physical and virtual possibilities. Questions remain as to how equipment acquisition will be handled by the First Responder Network Authority. FirstNet may identify developers as single source providers for first responder network hardware or determine a list of requirements for hardware to ensure interoperability across the nation and certify potential sellers for states. If

virtual, equipment acquisition may be handled at the state/local level and adhere to a set of requirements outlined by the First Responder Network Authority. Whether or not cloud computing would be compatible with FirstNet will depend on geography, demographics of the environment, the demand signal from the environment, propensity for crisis or emergency conditions, and countless other factors. Simply put, it will likely depend on different customer requirements. Currently, whether the DOD will allow services to use commercial database and cloud computing providers such as Verizon's Terremark and still be interoperable with other FirstNet users cannot be determined.

As of April 2014, out of 100 employees that FirstNet plans to hire, they are currently less than 50 percent manned. Recently, they hired their Chief Technology Officer. The direction FirstNet is currently taking is applying the network state level, and will require buy in in some form from state officials. There will be a core network at the federal level in some form, and states will be allowed to opt in or opt out. Again, what that federal core is comprised of is yet to be determined.

d. Current Phase

The current phase of FirstNet could be described as a consultation phase. One of the things that the First Responder Network Authority is determining at the state level is what capabilities exist that can be leveraged to save money and equipment. Companies such as Verizon and AT&T spend billions yearly to simply maintain their networks. Thus, building a new network across the United States to facilitate FirstNet is a far too expensive endeavor to begin. This allocation is especially small considering how little the seven billion dollar appropriation would pay for in a nationwide network. Historically, nationwide networks have spent hundreds of billions to ensure nation-wide coverage. Partnerships at the state level must therefore be made with federal and commercial entities within the states in order to be successful with the current and future dollar amounts allotted to FirstNet.

The DOD TEAM specifically has a current vision to use an enterprise approach that is mindful of the needs at the edges in order to facilitate FirstNet in the DOD. This vision entails a balancing act on the part of the DOD TEAM to ensure that interoperability is enterprise wide but information and creativity can be pushed to the edges. The previous information concerning the vagueness of what exactly FirstNet will be comprised of means that the DOD may not need to apply overarching new hardware to the different branches. Rather, the DOD can facilitate acquisitions of minimal equipment in certain locales or provide policies to allow the different branches to adapt their own. This facilitation would still maintain interoperability consistent with the vision of FirstNet. As mobile devices and other technologies become more and more part of normal operations in the DOD, such assets may be able to be leveraged and used in different ways to reduce acquisition costs. The DOD has the added benefit of acquiring FirstNet after the state and federal rollout, allowing the DOD to see good and bad ways in which the state and federal entities develop FirstNet that the DOD can use to its advantage.

e. Allocated Funds

Notably, all of the 7 billion dollars is allocated to the civil environment. Several business models have been proposed but are still under scrutiny, including spectrum arbitrage. Under spectrum arbitrage, unused portions of the 700 MHz band would be leased back to the public. These considerations are all being researched for the civil sector. Adding to the capabilities that also need to be taken into consideration are the possibilities for hastily formed networks that could operate over the respective spectrum where remote areas may necessitate supplemental network coverage to the proposed satellite portion of FirstNet.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. POTENTIAL MARINE CORPS BENEFITS (IF/THEN, CAUSE/EFFECT)

A. CLOUD COMPUTING

In relation to the models in this chapter, cloud computer could have potential benefits and uses. Different models may be able to leverage cloud computing in different ways. In an IaaS model, cloud providers would be able to provide the user or users the entire infrastructure needed to establish, operate, and maintain the FirstNet system. In this model, a cloud provider would administer the infrastructure and information system with the user accessing the system for any location. This would alleviate the cost of a municipality from establishing, administering, and maintaining a network and/or data center, but would require an investment cost with a cloud provider.

In a PaaS model, cloud providers would provide a platform for users or a network to use their own services. The provider would provide the backbone services and infrastructure for a municipality to administer its own information systems and manage its network. This would alleviate some cost from an infrastructural standpoint, but would still require an administration staff to service and maintain its FirstNet systems.

A SaaS model established by a cloud provider would establish a specific set of software, unique programs, which a user could access from any location around the nation or world. This would benefit a municipality that is small in size, which would only have and require a limited set of resources. This could also benefit first responders in a mutual aid situation to increase their level of integration and collaboration. For example, SaaS could be used for specific natural disasters, which would bring together a large number of organizations and allow them to share and corroborate information on a single platform for a limited amount of time.

1. Costing Approaches

The following information is split into two categories. The first category is *costing methods*, which provides several ways that may be helpful in approaching the overall problem of creating costing models. The second category is *costing metrics,* which are the essential elements that go into costing methods. The primary focus of this chapter will center on costing metrics, as they are likely to remain more focused and relevant during the duration of FirstNet development and can be applied to numerous different costing models. The purpose of describing several costing methods is to provide examples of what might be used in conjunction with the potential metrics provided.

a. Methods

Different methods of creating cost modeling schemes are important to research before beginning the FirstNet acquisition process for the DOD. Full cost transparency that can be provided by costing methods can potentially allow cost savings for the Marine Corps. Additionally, these methods can provide insight into what kinds of resources (both physical and capital) need to be allocated toward acquisition of FirstNet.

(1) Hedonic and PriCo

After fully understanding the needs of the organization, costing models can be explored to provide buyers with the most efficient use of their capital. Two models for creating costing transparency include the hedonic pricing method and PriCo, a pricing plan comparison method proposed by Kihal, Schleret, & Skiera (2011). The hedonic pricing method involves taking each required service, applying its market price, and adding it to the end cost (Kihal et al., 2011). This pricing method is predicated on three assumptions: objective utility characteristics, objective market cost, and equal utility demand across a company's services for prospective customers (Kihal et al., 2011). Utility in this case refers to the "total satisfaction received from consuming a good or service" (Utility, Investopedia.com). Therefore, the assumptions refer to satisfaction

received or usefulness of a comparative entity to the buyer, market value of an entity as valued by a collection of buyers, rather than valued by a single buyer, and the requirement that all marketed entities carry the same level of satisfaction or usefulness from customers. PriCo identifies favorable profiles to alleviate market competition that is lacking in the hedonic model by maximizing monetary advantage and controls for bundling and unbundling (Kihal et al., 2011).

Hedonic pricing is “a method of pricing based on the principle that the price of a marketed good is affected by certain external environmental or perceptual factors that can raise or lower the *base* price of that good” (Hedonic Pricing (n.d.a.), Businessdictionary.com). Further, the method is used as estimation into what individuals in a market are disposed to pay for said goods (Hedonic Pricing (n.d.a), Businessdictionary.com). In other words, this model identifies “price factors according to the premise that price is determined both by internal characteristics of the good being sold and external factors affecting it” (Hedonic Pricing (n.d.b), Investopedia.com). One major example is the U.S. Housing Market, where factors such as location, views, schools, and environmental quality affect the price of a home (Hedonic Pricing (n.d.b.), Investopedia.com). This example can transfer to IT in a number of ways, including items like bandwidth where location may play a role in how much bandwidth may be available in areas outside of urban centers where DOD locations exist but low populations may have prevented higher bandwidth providers from marketing. This example could have an impact on both price and availability in general.

The relative values that the models create provide solid figures for organizations considering cloud computing, and help achieve cost efficiency for interested parties. These methods are an outstanding starting point for matching organizations needs to streamlined services on the market. Due to numerous companies providing cloud and infrastructure as a service, a model based on simply two major company’s information services using the hedonic pricing method would allow the Marine Corps a basis for comparison, primarily due to

the hedonic pricing method's compensation for the absence of market competition (Kihal et al., 2011).

Using the hedonic pricing model, both Terremark and First Responder Net would allow Marine Corps Installations Command to establish a cost and pricing archetype for providing services in the absence of market competition (Kihal et al., 2011), should the Marine Corps plan to simply look at these two services and desire room for negotiating cost. In the case of a lack of market parameters, models can be developed through hedonic pricing using pre-determined characteristics. Similar to the housing example where models can be determined based on size, number of rooms, etc., internal to the house itself (Hedonic Pricing (n.d.b.), Investopedia.com), items such as average latency required can be assigned value estimates in the absence of specific data due to internal characteristics. Not all services would necessarily be required to be tested from each company, just those that are critical.

After settling on a costing model and using it to derive the most appropriate system for their needs, organizations must be wary of costing transparency. Costing model transparency is tremendous for putting together a prototype to assess any system, including both Terremark and First Responder Net. IT cost transparency "measures multiple factors, such as software utilization, cost upon purchase and return on investment (ROI)," and by measuring these factors, managers can analyze IT investments to help ensure maximum productivity for each IT dollar spent (Techopedia.com, IT Cost Transparency, 2014). Kihal, et al. (2011) noted that different pricing plans can make comparing IAAS providers difficult. Moreover, poor standardization in cloud-based services causes a corresponding lack of clarity in the service level agreements offered by different providers (Baset, 2012).

Two pricing plans commonly seen in today's market are price bundling and unbundling (Kihal et al., 2011). Bundling can be seen in many environments today: from fast food to cable television, Internet, and telephone services. Product bundling is "act of placing several products or services together in a

single package and selling for a lower price than would be charged if the items were sold separately" (Bundled Pricing, Businessdictionary.com). At a fast food restaurant for example, many patrons order off of a value menu that combines fries, a hamburger, and a drink—or less than the price of all three purchased separately.

Performance versus fit additionally complicates pricing models, as organizations may pay a higher cost for each unbundled service (similar to a la carte restaurants) and get exactly what they need, or pay a lower overall cost and sacrifice capabilities or performance or even overbuy. Kihal, et al. (2011) pointed out that bundled services can often veil prices of the characteristics of the bundle, in an effort to provide either higher prices for services that are not necessarily useful, or to ensure that organizations have to pay higher overall prices to get a single service that is offered only in a bundle.

Testing performance can also be difficult, as proper measures for latency can be subjective depending on the needs of the customer. Goel and Aggarwal (2013) used four tests across five cloud computing services (Amazon, Google, Terremark, Rackspace, and Salesforce) to measure latency, as displayed in Figure 6. They found that none of the five providers was fastest at every test, and each provider was good at different tasks. (Goel & Aggarwal, 2013).

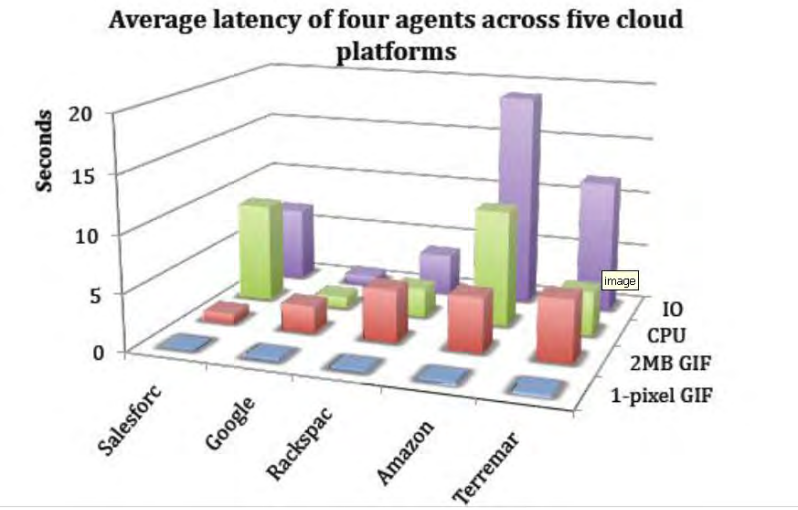

Figure 6. Average Latency for Cloud Providers (from Goel & Aggarwal, 2013)

Therefore, it is not only necessary to create a cloud computing costing model that primarily considers costing, but additionally provides information regarding best fit for customers.

While latency is definitely a characteristic Marine Corps decision makers must consider, there are numerous other characteristics, some plausibly more critical than latency. Delving farther into characteristics of different corporations' offerings, Rufer (2012) examined system characteristics and transparency with Amazon, Terremark, Rackspace, Windows Azure, and IBM cloud computing systems, as indicated by Figures 7, 8, and 9 (Rufer, 2012). Rufer (2012) found that pricing transparency was an issue with Amazon and Rackspace, and especially drew attention to Rackspace's hidden fees. Baset (2012) pointed out that Window's Azure put the onus of reporting an already complicated service level agreement (SLA) violation and providing evidence…on the customer. Additionally, the complexity of Windows Azure itself complicates the ability to price its system and assure buyers that they are getting what they need at a competitive price (Rufer, 2012).

Price per GB / Month			
Bandwidth	**Amazon**	**Terremark**	**IBM**
1 GB	$0.00	$0.17	N/A
10 TB	$0.12	$0.17	$0.15
50 TB	$0.09	$0.17	$0.11
150 TB	$0.07	$0.17	$0.08
500 TB	$0.05	$0.17	$0.09

Figure 7. Amazon, Terremark, and IBM Bandwidth Pricing Scheme (from Rufer, 2012)

Server Sizes:	Linux®*** Hourly (Estimated Monthly)	Windows® Hourly (Estimated Monthly)
256MB RAM **10**GB Disk	**$0.015/hr.** ($10.95/mo.)*	—
512MB RAM **20**GB Disk	**$0.03/hr.** ($21.90/mo.)*	—
1,024MB RAM **40**GB Disk	**$0.06/hr.** ($43.80/mo.)*	**$0.08/hr.** ($58.40/mo.)*
2,048MB RAM **80**GB Disk	**$0.12/hr.** ($87.60/mo.)*	**$0.16/hr.** ($116.80/mo.)*
4,096MB RAM **160**GB Disk	**$0.24/hr.** ($175.20/mo.)*	**$0.32/hr.** ($233.60/mo.)*
8,192MB RAM **320**GB Disk	**$0.48/hr.** ($350.40/mo.)*	**$0.58/hr.** ($423.40/mo.)*
15,872MB RAM **620**GB Disk	**$0.96/hr.** ($700.80/mo.)*	**$1.08/hr.** ($788.40/mo.)*
Bandwidth Out	18¢ / GB	
Bandwidth In	No Charge	

Figure 8. Rackspace Pricing Scheme (from Rufer, 2012)

Virtual Machine Size	CPU Cores	Memory	Disk Space for Local Storage Resources in Web and Worker Roles	Disk Space for Local Storage Resources in a VM Role	Allocated Bandwidth (Mbps)	Cost Per Hour
Extra Small	Shared	768 MB	19,480 MB (6,144 MB is reserved for system files)	20 GB	5	$0.04
Small	1	1.75 GB	229,400 MB (6,144 MB is reserved for system files)	165 GB	100	$0.12
Medium	2	3.5 GB	500,760 MB (6,144 MB is reserved for system files	340 GB	200	$0.24
Large	4	7 GB	1,023,000 MB (6,144 MB is reserved for system files)	850 GB	400	$0.48
Extra Large	8	14 GB	2,087,960 MB (6,144 MB is reserved for system files)	1890 GB	800	$0.96

Figure 9. Windows Azure Pricing Scheme (from Rufer, 2012)

Not all of the findings made were adverse. Further complicating product selection, many of the systems seemed to balance complex pricing with positive attributes. Windows Azure naturally integrated into the Windows environment, while Amazon offered wide configurability and Rackspace offered simple server pricing (Rufer, 2012). Baset (2012) noted that Amazon provided a distinct SLA. Contrarily, Terremark and IBM, who offered good Transparency in their prices, limited their services with no reserved resources and platform dependence respectively (Rufer, 2012).

Ultimately, the only realistic deterrence to hidden prices is decision makers having a robust awareness of what potential hidden fees exist. Decision makers must ensure to the best of their ability that the only thing they are paying for is exactly what they need. While having this knowledge will not remove the issue of hidden fees, it will give decision makers room for negotiations when considering multiple competitors.

Marine Corps Installations Command should take several steps before choosing whether to use a vendor's cloud computing model to create an organic asset or to spend in conjunction with vendor cloud services. First, Marine Corps Installations Command must fully understand the systems already in place, the systems offered, and the desired goals that the organization wishes to achieve. Next, the organization should use a costing model that best emphasizes the attributes that the organization needs and additionally vets the best possible cost from potential vendors. Using a costing model that forces transparency, or at least identifies areas where transparency does not exist, allows Marine Corps Installations Command room for negotiations against competing companies. The key to making a good cloud computing decision is a robust understanding of all attributes in both the purchasing company's organization and potential providers' organizations.

(2) Net Present Value, Initial Rate of Return and Economic Value Added

Economic Value Added (EVA) is the net profit of an investment less the capital itself, cost of capital (interest for debt holders), and shareholder return. In other words, "EVA equals the net operating return minus any applicable capital charges" (Berry, 2003). In contrast to net return, EVA considers the cost of capital itself, as net return after taxes fails to consider interest rates (Berry, 2003). Berry (2003) claims that CIO's and Information Technology (IT) executives who use EVA as a primary metric "will experience a whole new level of technology investment assessment." EVA, while effective in the commercial world, can also be applied effectively across the DOD as a primary metric for evaluating IT investments.

By transposing familiar parts of the EVA equation, one can apply similar or equal factors in determining the EVA for a DOD project. The EVA equation is as follows: EVA = NOPAT–WACC, where NOPAT is the Net Operating Profit After Taxes, and WACC is the Weighted Average Cost of Capital (Capital * Weighted Cost of Capital) (Economic Value Added, Investopedia.com). Berry (2003) noted

that “the challenge…is pinning down those hard-to-measure benefits so that they are intellectually honest.” Nothing could be truer for measuring DOD investment successes. As the DOD technically does not have a true to form “profit,” applying honest, measurable factors is the key to successfully using EVA in the DOD.

First, taking the Net Operating Profit After Taxes in a DOD EVA assessment involves staunchly vetting what the return actually is. In a DOD IT investment, return can take many tangible, measurable forms. Profit and net savings on IT systems are two examples. If a new IT investment cuts the workforce in half and still costs less than the individuals that originally performed the same task, those savings can be considered returns for the DOD. Capital can be considered anything that the DOD either has in its budget to spend or is allotted toward a project by Congress. The weighted cost of capital is equally transposable; especially considering the current national debt, therefore money borrowed by Congress in order to facilitate DOD spending would carry interests rates levied upon DOD capital.

For DOD decision makers, it is imperative to get the best “bang for the buck” in order to mass capital together to further other projects. Essentially, using a business metric such as EVA in IT “makes people accountable for the capital invested and the risks in doing so” (Berry, 2003). In order to ensure that EVA works as a metric, Berry (2003) stated that “effective EVA implementations also require a formal compensation plan that puts bonus money at risk.” This bonus money is essentially what DOD decision makers are left with to improve other areas of their respective branches. DOD leaders are incentivized to save money whenever possible in order to ensure the success of the DOD in other areas. While traditional corporate bonuses to employees are not seen in the DOD, consideration should be given to outsourcing IT where EVA estimates success and bonuses can be leveraged on civilian employees that “behave as if the company money they spend is their own” (Berry, 2003). Capitalism, rather than virtue towards an organization, can arguably be a greater money saver.

Net present value (NPV) is used to measure project return by comparing "the present value of cash inflows with the present value of cash outflows" (Net Present Value, Investopedia.com). The important factor levied through NPV calculations is the "time value of money," that is—"a dollar earned in the future won't be worth as much as one earned today" (Net Present Value, Investopedia.com). Organizations identify this "discount rate" usually by using expected returns on projects of similar risk (Net Present Value, Investopedia.com). For example, if an organization desired to buy an IT system that advertised the ability to streamline a given process and generate return, the organization could choose to use a NPV analysis to decide whether or not to buy. In this example, assume the system cost was $100,000 after running the NPV analysis to determine future cash flows and applying them in today's dollars. Should the system cost more than $100,000, the organization would end up losing money in the long term and thus should not buy. Contrarily, if the system cost less than $100,000 it could be considered a sound investment in this example.

Internal Rate of Return (IRR), another sound metric to determine project worth, is "the interest rate at which the net present value of all the cash flows (both positive and negative) from a project or investment equal zero" (Internal Rate of Return, Investinganswers.com). IRR is a metric that is effective in determining the appeal of a given investment, and identifies a worthy investment when the IRR is greater than "[an organization's] required rate of return" (Investinganswers.com, 2014). The primary difference between IRR and NPV is that IRR calculates yield, and allows executives to "rank projects by their overall return rather than their net present values" (Investinganswers.com, 2014).

EVA, when integrated with methods such as IRR and NPV, presents a complimentary method of measurement. IRR is not as useful in comparing investments of different durations and shows favoritism toward shorter projects, and eventually reaches a plateau where IRR is no longer effective (Internal Rate of Return, Investinganswers.com). NPV is factored into EVA, and while one

project may have a higher IRR, the EVA on a competing project could prove to be higher in the end, resulting in a more sound investment and proving the IRR an ineffective measurement. Moreover, an investment could harbor a short term negative IRR, but a long term positive EVA, thus saving DOD money in the long run. This money savings is especially apparent in big IT expenditures, which usually entail an initial loss in productivity and money before savings begin to be realized. In other words, EVA is a good tool for sanity checking investments to ensure that all factors are taken into consideration and that the end result is what the buyer is looking for. For DOD decision makers, EVA is an excellent metric for effectively managing the business due to EVA being an ultimate, robust metric that gives executives a "realistic focus on maximizing true shareholder value" (Berry, 2003).

b. Metrics

In order to assess the viability of each model, they should be analyzed using metrics that are relevant to each model. The following metrics will address the major factors that should be considered when studying how FirstNet should be implemented in the USMC.

(1) Bandwidth

The metric for bandwidth refers to the necessary throughput of information across the network to ensure that information arrives to the needed user in a sufficient response time as established by policy. The bandwidth requirement will depend on the numbers of users that are using the system and the amount of information that is traversing the network.

(2) Equipment

The equipment that is used to establish the physical and logical structure for the FirstNet network architecture will be a varying costing metric, dependent upon the model used. The policy established will determine the level of standardization and requirements for the needed equipment. Additionally, the model used and standardization requirements will determine whether the network

can be established using COTS technology or will require proprietary hardware and software purchased from specific vendors.

(a) *Scalability* The scalability of the system will be determined by policy and standardization requirements. If the government procures the equipment as a holistic system by a single source provider or vendor, then there is little ability to scale the system appropriate to the needs of a specific state or municipality. However, if policy allows for more open standards to be used then the federal, state, or local levels could scale the equipment requirements according to the need of their specific requirements.

(b) *Maintenance* Maintenance costs are going to be determined by the complexity of the hardware and software systems and the level of expertise of organic personnel operating and maintaining the system. Due to the model used, organic personnel may not have the ability to maintain all of the equipment and software, which would require outside contractors to fill that role. This would require additional cost compared to a system where the resident personnel have an in depth knowledge on the operation and maintenance of the equipment and software.

(c) *Spectrum Usage* Spectrum availability and usage is based on the population density of the area and the saturation of the network by first responders. These metrics will determine the amount of spectrum that a state or municipality will need to purchase. For example, New York City or Los Angeles will need to purchase more spectrum in order to conduct their operations compared to a small or medium sized town. The saturation of the network can be determined by the population size and number of first responders in the area or a high occurrence or need for first responders. An example would be a city with a high crime rate where first responders are constantly responding to a high number of calls and need to pass a large amount of information. This would require additional spectrum to ensure that the sheer volume of information being passed does not saturate the system.

(d) *Security* The level of security that is required by the system will be a major cost metric. The security requirement for the system will be determined by policy of the federal, state, and/or local governments. The policy standards for security will determine the complexity of the hardware and software required to establish an operating environment that will ensure personally identifiable information is secure. Additionally, if levels of security differ between federal agencies, states, or local municipalities, this will cause an interoperability issue and additional cost. The additional cost would be necessary to allow information to be shared across the FirstNet system or when mutual aid situations occur.

(e) *Risk* The level of risk associated with the implementation of a new information system is based on two primary factors, probability of failure or delay and the monetary or time impact that it will have on the implementation of the system. The metric is significant because there is a great deal of money and time involved with resolving these issues.

B. FIRST NET ARCHITECTURE

To assess the implementation of FirstNet, three models will be used, physical, hybrid, and virtual, as shown in Figure 10. The models differ by the level of government that will establish overarching or amplifying policy regarding the implementation of the system. Also, these models will assess how different levels of government would potentially establish, operate, and maintain the network infrastructure needed to support the FirstNet system. These three models can determine the manner and at which governmental level that the DOD integrates into the overall system.

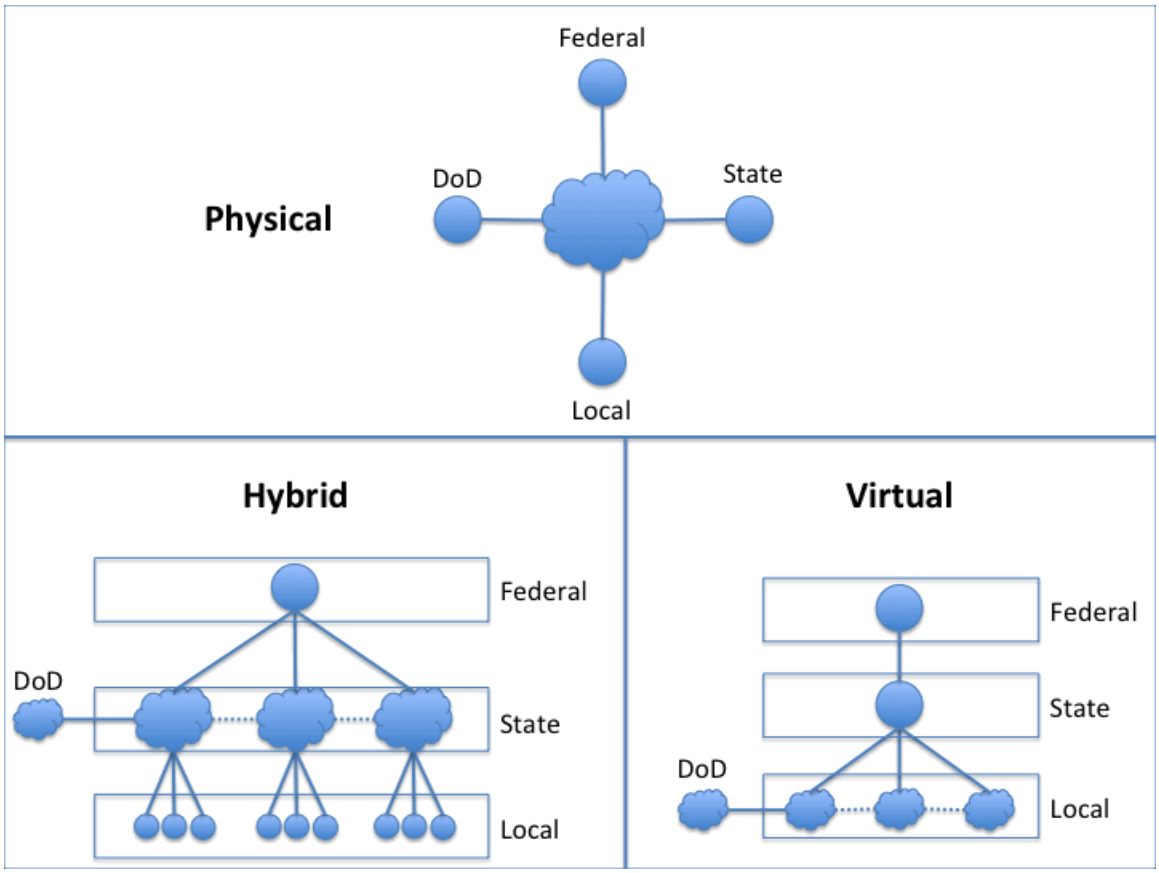

Figure 10. Implementation methods of FirstNet architecture.

The physical model represents a centralized system in which the federal government establishes all policy governing the implementation and operation of FirstNet. The federal government would be responsible for the establishing, administering, and maintaining the physical network infrastructure. This would allow the federal government to provide a standardized service to all state and local municipalities.

The hybrid model is more decentralized than the physical model. In the hybrid model, the federal government establishes overarching policy to standardize the implementation and operation of FirstNet to State governments. The State government is then responsible for creating and maintaining the physical network within its State, in accordance with federal policy. The State government would provide services to the local municipalities within its State.

The virtual model is the most decentralized system of the three. The federal government established the overarching policy regarding the implementation, operation, and interoperability of the FirstNet system. The State government then establishes amplifying guidance to the local municipalities, which is accordance with federal government policy. The local municipalities and counties are responsible for the establishment and maintenance of the physical network within districts and cities.

C. PHYSICAL

In a physical system, as displayed in Figure 11, policy, management, administration, and control for the FirstNet enterprise network would be centrally controlled at the federal level. The physical model would create a homogenous network across the nation, which federal, state, local and DOD entities would use. The responsibility for establishing a broadband network, information systems, equipment requirements, equipment procurement, and spectrum management would reside at the federal level.

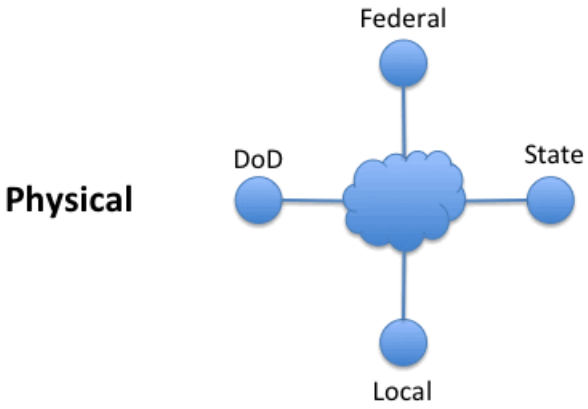

Figure 11. Physical Model

This would be a massive undertaking at the federal level in terms of cost and scale. The total cost of establishing the infrastructure would require a large initial investment on behalf of the federal government, but could be offset later on through state and federal agencies opting in to the program. This funding after

establishment of the FirstNet system would be used to maintain and fund the necessary services required to keep the system operational, without the government having to front the entire bill.

Additionally, the FCC has already leased the necessary spectrum for the system to states and local entities as a fundraising mechanism for the initial startup of FirstNet. In order to continually fund the program, this spectrum would likely be renewed on a time-share basis, which would provide future funding for the FirstNet system to offset some of the federal government budgetary requirements.

In terms of the DOD accessing FirstNet in the physical model, the system employed would be largely standardized across each service and the DOD as a whole. The DOD and MCICOM would adopt and adhere to the equipment and system requirements universally across all installations. Therefore, the system adopted in MCIWest would mirror the system installed in MCIEast, which would provide a standardized system across the Marine Corps.

1. Leveraging Current Equipment

Leveraging and using current DOD equipment within the physical model would be based on the requirements established by the Department of Commerce. The minimum standards would be established and if current equipment meets or exceeds those standards, then current equipment could be reformatted and utilized in the FirstNet system. However, if standards are established and current equipment does not meet the criteria then the DOD would be required to procure all new equipment to support integration into the FirstNet system. With equipment requirements being established at the federal level this would potentially require state, local, and DOD systems to be largely upgraded to maintain the minimum equipment standards.

2. New Equipment Acquisition and Standardization

In the physical model, standardization of equipment and standards would be established at the federal level. Additionally, the acquisition of new equipment and contracts with providers would be centrally administered at the federal level. The standardization and acquisition of equipment at the federal level, does have some positive and negative aspects that should be considered.

The standardization of equipment and information systems at the federal level provides a streamlined system that is common among all federal, state, local and DOD entities. This level of standardization would ensure that all first responders would be using the same equipment with the same systems, which would ensure that any first responder could access needed information regardless of their location or whose equipment they are using. This level of standardization could incorporate all information needed to respond to any natural disaster, including wild fires, hurricanes, earthquakes, tornados. Conversely, there would be a great deal of information and resources allocated, which would not pertain to regional trends for first responders. Thus, there would be an added overhead of information systems and resources required for all municipalities, which would not relate to their common requirements.

The acquisition of equipment, within the physical model, would benefit the commonality and interoperability of a national system. Having equipment standardized and negotiated with specific vendors would ensure that local municipalities, states, and federal entities would have similar, if not identical equipment. Additionally, with acquisition and procurement of equipment being retained at the federal level, there would be potential cost savings for bulk equipment orders. However, procurement of equipment on this scale would require a large initial investment on part of the federal government or could potentially pass off the procurement of the equipment to the state level.

3. How to Transition

For the DOD, transitioning in the physical model would pose limited risk. Due to the DOD transitioning to FirstNet, potentially years after the civilian sector, a national network would already be online and a great deal of the technology, systems, and procedures would have matured. The DOD would be able to utilize lessons learned from the civilian sector to avoid previously identified pitfalls during implementation. The DOD would also be able to model its transition after larger organizations and municipalities to leverage their transition models.

4. System Maintenance

System maintenance in a physical model would be difficult in terms of funding and common level of service across the nation. The federal government would have to use multiple contractors and vendors to establish SLAs and maintenance requirements to ensure proper functionality and service of the network. However, when service or maintenance is required in small or remote municipalities a national vendor may not be able to provide the level or service required. This could be detrimental to first responder reaction time and degrade the level of service provided at the lower levels.

A large issue with system maintenance at the federal level is the funding requirement. It would be unlikely that the federal government would have resources to sufficiently fund the establishment, administration, and maintenance of a system on the scale of FirstNet. There would likely be a funding requirement from all entities that opt into FirstNet in order to offset the cost of establishing and maintaining the network and would share the cost burden.

5. Cloud Computing

Cloud computing in a physical model could be leveraged to reduce the cost of procuring the equipment needed to operate a nationwide network. The system could be virtualized, regionalized, and managed without having to procure physical equipment for all state and local municipalities. Creating

regional cloud networks for different regions of the country would allow state and local first responders to tie into the network with minimal equipment. In a cloud environment, the system could also use resource balancing to shift resources from an underutilized node to an over stressed node in case of a natural disaster or emergency situation.

Virtualizing the network and leveraging cloud technology would allow the federal government to maintain backups and fail over systems in case a primary node failed or a natural disaster. Through a cloud provider, the federal government would be able to backup and duplicate all system data to ensure that a network failure would not be catastrophic to the system.

6. Costing Metrics

In a physical model, there are several important things to consider when addressing costing metrics. With all resources and standards being established and contracted at the federal level, this has great implications on bandwidth, spectrum usage, equipment procurement and maintenance, implementation risk, and security requirements.

In a physical system, bandwidth requirements and contracts would be established at the federal level, which potential cost savings could be realized based on the scale and negotiating power between the federal government and national ISPs. The federal government would have the bargaining power based on the size of the contract to negotiate a reasonable cost to ensure proper service and response time across the nation. Conversely, a national contract for bandwidth with national ISPs would meet the needs of the standards established by the approval authority. However, with the bandwidth requirements differing between large and small municipalities a general contract may not meet the individual needs of a specific locality at the lower levels. A small municipality would potentially not need as much of a robust system and bandwidth allocation as opposed to city the size of Los Angeles or New York. With a common contract across the nation, small municipalities may have excess bandwidth and excess

cost and larger municipalities many have insufficient bandwidth and degraded performance.

A physical system would require spectrum management to be administered at the national level, likely by the FCC. Spectrum management is essential in a national broadband network to ensure that a federal, state, or local entity has the necessary spectrum and broadband bandwidth to ensure proper communication within its municipality or region. The administrative overhead for allocation, deconfliction, and management for a nationwide system would increase the cost compared to allocating blocks of spectrum at a lower level, i.e., the state level.

Equipment requirements and procurement at a national level have the ability for cost savings of the overall network. Establishing one set of standards for all federal, state, and local entities would ensure a uniformed set of equipment for use within the network. The federal government could establish relationships and contracts with specific vendors and negotiate cost for procurement of equipment on a national scale. The cost of the government procuring this amount of equipment would be enormous and would like be offset by states opting in and assuming a large deal of the cost burden for usage of the system. However, this could potentially affect system maintenance if the federal government contracts vendors that use proprietary equipment. Then federal, state, and local entities would be required to purchase equipment and services from specific vendors, in order to keep their system operational. This increased cost for proprietary equipment and service could be offset or negated by the federal government negotiating contracts that utilized COTS technology and prohibit or limit the use of proprietary hardware or software.

The implementation risk for a physical model would be dependent upon the process for integration and the level and depth of testing prior to bringing the system online. Due to the scale of the system, the impact risk would be high, however could be mitigated through thorough testing of the system prior to transition to a fully operational status. Additionally, the risk to the DOD would be

reduced further because a national FirstNet system would be similar if not identical in the implementation process.

From a security standpoint, the cost for the DOD would likely be reduced compared to a virtual or hybrid system. With FirstNet being managed and administered at a national level the security requirements for the system would also be administered at a national level. The requirements would be more in line with DOD IA and OPSEC requirements and thus would not be a great need for additional equipment or procedures to ensure the sharing of information across the spectrum.

D. HYBRID

In the hybrid method, as shown in Figure 12, the federal government establishes policy guidance for the implementation of the FirstNet system. At the federal level, policy is established for operating procedures and standardization of equipment across the network. The state level is then responsible for acquisition of the needed equipment, establishment of the system at the state level, and maintenance of the network. The policy established by the federal level would ensure that the individual state's system would be interoperable with all other states. Marine Corps installations would then tie into the network at the state level, which would allow a more regional control and administration of the system.

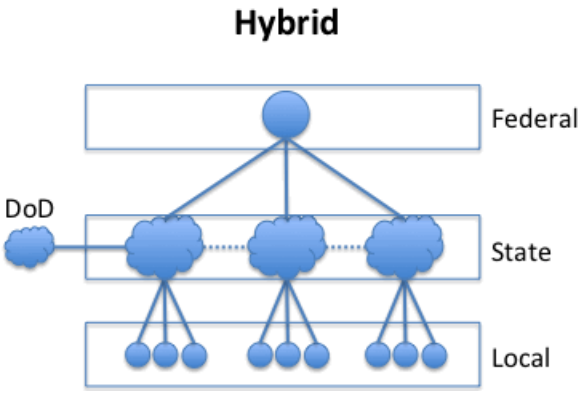

Figure 12. Hybrid Model

Marine Corps installations would benefit from this model because installations are generally regionalized in specific states with a few outliers, such as Yuma, AZ, Albany, NY, and Parris Island, SC. This model would allow MCICOM to standardize its equipment with California and Arizona, in the west, and North Carolina and Virginia, in the east. Due to the DOD delaying the implementation of FirstNet following the states, contractors and vendors would already be established by the states. This would benefit the acquisition timeline and cost for MCICOM because vendors would have established systems operating within the state and the technology would have matured from the initial implementation of the system.

The hybrid model would also allow states and therefore regional commands to customize their network based on the common disasters that their state or region encounters. For example, California's system would be tailored to responding to wild fires and earthquakes more effectively than hurricanes. Conversely, North Carolina's system would be tailored towards responding to hurricane response. This would allow the MCICOM to similarly tie into these systems with similar capabilities without having to purchase unnecessary equipment or software, which would be required for a national universal system.

1. Leveraging Current Equipment

With the primary infrastructure piece being levied at the state level, current equipment will be hit-and-miss as to its utility. While the virtual structure offered the most flexibility for leveraging current equipment, and the physical structure offered the least flexibility for leveraging current equipment, the hybrid level will offer something in between. A potential course of action at the state level is to create an infrastructure that is able to incorporate as many existing systems and equipment as possible. Seemingly, again smaller municipalities will likely have the most ground to catch up on for such a structure. The benefit of the hybrid system is that it provides a good combination of both flexibility and interoperability, as each local agency must tie into a statewide system.

Therefore, at least in the state, interoperability should be more efficient than in a virtual system. The downside, however, is that equipment must be applied at a greater level than the virtual model; therefore equipment may not necessarily fit all the needs of municipalities.

2. New Equipment Acquisition and Standardization

Equipment acquisition and standardization at the hybrid level works well for ensuring interoperability across the state. Since acquisition will be handled at the state level, subsidies and equipment can be monitored more easily, as the state is responsible for each and every county and city to be capable of tying into the statewide system. Equipment purchased by the state and pushed to the edges will have a few layers of hierarchy, compared to the virtual model. Therefore, autonomy in equipment purchasing is replaced by a system that the state would enact of requesting new replacement equipment. Finally, standardization would be easier for the state to enact and effectuate across its realm of responsibility, rather than relying on local entities to abide by rules using their own funding.

3. How to Transition

Importantly, states and DOD installations should potentially begin to transition, if able, during the FirstNet development process. As previously discussed, each state will have to buy in to the overarching FirstNet. While the definition of buy in has not been solidified, states will likely have to provide funding for some portion of infrastructure. Therefore, if requirements are identified early in the FirstNet development process, states may begin transitioning cities that require more time for transition at an earlier date. Additionally, states may identify early on municipalities that will already meet their states particular requirements for FirstNet compliance, therefore will be able to begin to allocate money toward noncompliant municipalities.

DOD installations should follow the lead of the states they are in, as the ability to create an overarching DOD system that has the capability to tie into

every state system will be difficult. Therefore, installations may group together in a region of a state or an entire state DOD network to meet state interoperability requirements while still buying in bulk for DOD installations in a respective state.

4. System Maintenance

System maintenance will be the responsibility of the state in a hybrid system. In this system, local agencies do not have to worry about the costs of maintenance for the system. They do, however, lose autonomy in requiring maintenance response times through SLA's or maintainer ownership. Importantly, the state must ensure proper response time through SLA's or maintainer ownership state-wide, which is far greater a task than at a local level. Thus, maintenance processes will become more complicated in this model, and robust requirements must be made and adhered to, ensuring that every agency state-wide will receive proper and timely attention when required.

A primary advantage of system maintenance in the hybrid system for local municipalities is that the cost would largely be carried by the state. This would allow municipalities the same level of maintenance and across the state. For municipalities that do not have the budgetary freedom of other localities, this would ensure that maintenance of the system is similar across the board. The DOD would be able to establish the same SLAs and use the same maintainers, which could potentially reduce the overall cost for the state.

5. Cloud Computing

Cloud computing in a hybrid model could be used to alleviate some cost and infrastructure requirements for the state. Leveraging cloud technology could reduce the requirement for the state to maintain a large data center to house and store all of the FirstNet infrastructure and data. Cloud providers can be used to store the data for the state's FirstNet system, which would reduce the personnel cost associated with maintaining a large data center or many data centers across the state. Additionally, using a cloud provider would allow the state and the installation to backup and store data offsite, in a secure location, in case of a

natural disaster. This would ensure that data and system infrastructure is not lost if there were a massive earthquake in Los Angeles. The cloud providers could store and backup data in a location that is not susceptible to natural disasters.

6. Costing Metrics

In a hybrid model, there are several important things to note regarding the costing metrics. Bandwidth requirements, while established at the federal level, could be negotiated at the state level with the major providers in the state. Spectrum management would be monitored and implemented at the state level to ensure no overlap or interference at the local level. Equipment would be standardized across the state to ensure interoperability with all first responders. Security requirements and implementation would be enforced by the state, which could provide a greater degree of security than individual municipalities.

In a hybrid system, the state will be able to negotiate bandwidth and latency requirements with providers in the state. This would allow the state to negotiate the on a larger scale compared, compared to the virtual model, and therefore could see potential cost savings. The state would also have the power to negotiate requirements for municipalities based on their size and bandwidth requirements. The requirements for latency and bandwidth would be established by the state, in accordance with federal policy, to ensure that the state's acceptable response time is met. The DOD would be able to leverage the SLAs and contracts with the state government and Internet providers to ensure they maintain the same standards established within the specific state.

Spectrum usage within the state would be monitored and allocated by the state. This would ensure that municipalities have the requisite frequencies available and sufficient bandwidth based on their population size and need. The state would also be able to provision and allocate spectrum in the case of natural disasters or during times that required mutual aid from other entities in the state. Managing spectrum at the state level would provide better control and usage of the spectrum within the state. Additionally, the state would have the ability to

allocate spectrum to the DOD for use within a specific municipality for mutual aid situations and spectrum that is specific to a particular installation.

In a hybrid system, equipment requirements would be standardized across the state and could be tailored to the needs of municipalities, based on size. The standardization of equipment across the state would ensure a greater degree of interoperability between different agencies and localities. Procuring equipment at the state level would allow for greater bargaining power with contractors and providers, which could reduce the overall cost. Also, the state would monitor, administer, and maintain the equipment, which would provide for a greater level of security due to a larger amount of resources compared to a small municipality.

Risk during implementation would be reduced compared to a virtual system, because there would be one system centrally controlled and administered by the state. With a large number of municipalities administering individual systems, this could pose a significant risk to interoperability and maintenance of FirstNet. For the DOD it would reduce the risk and cost of having to tailor each installation's system to be interoperable with the local municipality, while still maintaining interoperability at the state and federal level.

E. VIRTUAL

In a virtual system, as displayed in Figure (13), overarching rules and guidance are defined at the federal level and passed down to be further amplified if necessary at the state level. Ultimately, equipment and infrastructure is left to be purchased and implemented at the local level. Several implications are made by this model. Investment will not be equal across DOD installations, local relationships can be exploited, and the DOD will be freer to apply individual infrastructure where it is both cheapest and necessary.

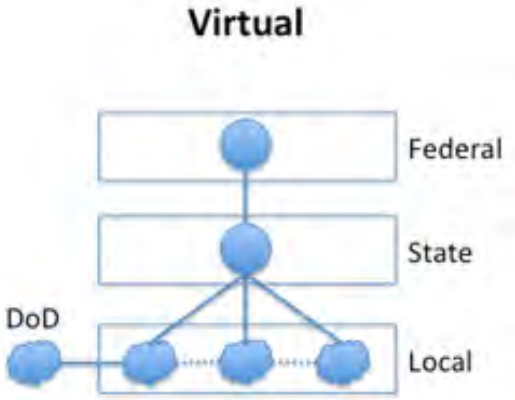

Figure 13. Virtual Model

DOD organizations with strong relationships with local municipalities will be able to invest at the local level to meet the gap in interoperability on an as needed basis. That is, from a DOD perspective, a given installation may be more capable of interfacing with local responders based on FirstNet rules and regulations than another. The DOD is therefore able to spend more money on one installation while they can garner cost savings through minimal implementation on another. Camp Pendleton, through the acquisition of the EMC2 system may prove to be far more capable of upgrading to FirstNet accreditation than an installation such as Barstow. Conversely, Barstow may prove to require less investment as rewritten MOU's and MOA's with local authorities could potentially suffice.

Many installations can benefit from a virtual structure, as installations are already prone to be more interoperable with municipalities in their immediate vicinity. That is, Camp Lejeune responders work frequently with Jacksonville, NC responders and Camp Pendleton responders work frequently with San Diego County responders, but not vice versa. From the standpoint of a virtual structure, implementation of FirstNet is targeted at the location in the structure where relationships are already the strongest. Due to these close, premade relationships, infrastructure that supports local needs rather than mass needs will better suit the initial stages of FirstNet.

Since the federal government will prescribe rules and regulations, the DOD will be free to invest in different infrastructure providers at different rates across the United States. An overarching provider that can adhere to FirstNet regulations in every location across the U.S. may not exist at the time of deployment. Therefore, the DOD will be able to barter contracts with different providers at different locations based on the needs of those individual locations. The benefit of these contracts is that differences in requirements at the local level can be invested in on an individual basis rather than applying an overarching contract to the DOD that may have provisions some installations may not require.

1. Leveraging Current Equipment

While equipment on hand at the time of DOD implementation is unknown, several assumptions can be made. Since all local entities are responsible for their own equipment, existing equipment can be more easily leveraged in the virtual model. Moreover, large municipalities can capitalize on large budgets and upgradable technologies.

Provided existing equipment is already in line with regulations that are passed at the federal and state level, some municipalities may be able to transition to FirstNet with minimal expense. As FirstNet will likely telegraph its rules and policies long before implementation takes place, municipalities may have the ability to upgrade to systems that are likely to be compatible or be able to be transitioned to FirstNet long before rollout begins. Larger municipalities with large budgets and systems on the forefront of first responder technology would have the easy transition in this case. Smaller municipalities making due with minimal technology would probably have a more relatively higher expense. Much up front expense would be spared should FirstNet allow insight to its operating rules to allow municipalities to purchase equipment in stages before rollout or within a long period of phasing after rollout.

2. New Equipment Acquisition and Standardization

Should new equipment acquisition and standardization be needed at the local level, there are several important positive and negative factors to consider. Procurement would be done at the local level and standardization may or may not suffer. Standardization success will be based on restrictions at the state and federal level in the virtual model.

Procurement must and gets to be done at the local level, which has several implications. Cost and responsibility for procurement of equipment, systems, and technologies is placed on the local municipality, likely with subsidies in some circumstances. This responsibility is both good and bad, as responsibility requires action and expense from the municipalities, but additionally allows for bartering their own contracts, buying more of what they need than what they do not need, and appropriately administering scalable equipment to fit the size of the municipality. Because these local entities will have this autonomy, appropriate decisions can be made on equipment rather than the overarching decisions of the other models that may apply to different sized municipalities and not quite fit any.

Standardization may or may not suffer, dependent upon restrictions and policies set forth by the state and federal levels. While flexible standardization policies are good for keeping costs down at the local level and ensuring that local municipalities pay only for what they need, loose standardization rules are bad for catastrophic events such as wildfires and earthquakes. With tight standardization rules, equipment and systems purchased at the local level will likely cost municipalities more, as there is a greater chance that existing equipment may not meet requirements. Relatively smaller municipalities again suffer mass expense under tight standardization.

3. How to Transition

Transition to FirstNet at the local level poses the benefit of hindsight for DOD installations. Since FirstNet for the DOD will be implemented possibly years

after the civil sector, the installations will be able to capitalize on local decisions. Mapping local municipal decisions with a given installation is imperative as the installations will ultimately want to be highly interoperable with local authorities first and foremost. Therefore, installations should use local municipalities as a case study, learning from mistakes and successes and investing in systems that tie in well with existing local systems.

The benefit of knowing the mistakes and successes made by local agencies in their own respective implementation of FirstNet could provide cost savings in a virtual structure. Installations benefit from this hindsight in a number of ways. Because of the close interoperability need, installations may have similar requirements to those municipalities they are working closely with, and would thus be looking for similar capabilities. Installation decision makers would have excellent perspective on what worked versus what did not work outside their local gates, and could thus adjust.

Having the ability to invest in systems that had already been sorted out by providers would give the added benefit of a smoother transition. This ability should be used in two ways: to barter lower costs and vet requirements. Knowing the capabilities of a vendor to meet installation requirements not only allows the selection of the best vendor for their offered price, but additionally allows for negotiation for lower prices on services that either are not a priority or have not been proven to work well. Installations would therefore be able to buy a pre-made and proven system from a vendor, rather than suffer through the implementation stages of a new system.

4. System Maintenance

System Maintenance in a virtual model will incur several defining factors. The costs of infrastructure are placed on the local user, thus placing maintenance costs on the local user. As such, maintenance and maintenance personnel expenses would be levied on local owners.

Due to local ownership of infrastructure, maintenance must be done at the local level through SLA's or through the hiring of permanent maintenance personnel. Obviously, larger municipalities with larger budgets have the ability to sustain their own maintainers and infrastructure if required, although SLA's may still prove to be more economically feasible depending on location and needs. Smaller municipalities would have to determine whether a small infrastructure with minimal maintenance staff was feasible or whether SLA's were more appropriate for budget constraints and on-hand equipment.

Importantly, first responder systems have factors that other systems do not have. Literally, quick maintenance could mean the difference between life and death with first responder systems. Should a system go down, owners must have either robust backup systems, which would likely be more feasible through IaaS, strict SLA's to minimize maintenance response time, or incredibly reliable on-hand maintenance personnel.

5. Cloud Computing

Cloud computing in a virtual model has the potential ability to drive cost savings among users. Of particular benefit are those users who lack the resources to invest in heavy infrastructure and can only afford to pay providers for use of their systems rather than creating their own. Larger municipalities can also gain cost savings through cloud computing, especially considering maintenance costs. This savings for larger communities, however, would only be beneficial if the net present value of cloud computing is greater than the cost of the life of a purchased system.

Cloud computing would also be beneficial to smaller municipalities due to the operating, maintenance and personnel costs. Small municipalities may not have to the capital to invest in a robust or specialized staff that could maintain all the systems required for FirstNet. This would require them to invest heavily in contractors or to outsource the daily maintenance and operation of the system. Cloud computing would allow a small municipality to operate the system, but

have it maintained and administered by a cloud provider. For installations in remote locations, such as Barstow, this would allow them to integrate into the FirstNet system without the requirement of a large staff. There would however be additional requirements in terms of security and information assurance, which would add an additional cost.

6. Costing Metrics

Particular to the virtual model, there are several important things to note regarding the aforementioned metrics. Bandwidth, to include latency and capacity, while dictated by federal and state entities, must adhere to local standards as well. Additionally, spectrum usage must be handled at the state level at a minimum. Equipment requirements must be scalable and available to every municipality across the U.S., and risk and security requirements must allow for interoperability.

In a virtual system, municipalities will be able to buy into the level of bandwidth and latency that they require. One of the major benefits of the virtual system is the autonomy of local agencies to purchase infrastructure directly related to their needs. Bandwidth and latency are important due to the response requirement timelines set by each municipality. Too much latency and too little bandwidth could lead to responders not reaching their response time requirements when the process of dispatching occurs. For the DOD, response time may be different inside an installation compared to the civil institutions in the immediate surroundings.

A virtual system allows for individual station/municipality bandwidth requirements regardless of adjacent unit requirements. On the downside, bandwidth requirements that are not comparable to one another in adjacent units could cause friction when operating jointly over two interoperable systems. That is, if an agency calls on the help of an adjacent agency, but the adjacent agency cannot meet the response time of the requesting agency because of bandwidth restrictions, problems may arise considering joint agreements, expectations, and

response efficiency. Moreover, spectrum usage among adjacent agencies must be vetted at the state level to ensure that each agency has the proper bandwidth to meet their requirements.

Equipment requirements must be feasible for agencies both large and small to meet across the U.S. for use, security, and risk. Provided requirements are realistic for all agencies to meet, the virtual system works well for smaller agencies to spend less on only the equipment they need to meet their own local standards. These standards are very likely to be different between DOD installations and local agencies regardless of understandings reached at the state and federal levels. These differences, as previously stated, have much to do with confidential information about on-base buildings and personnel. Thus, security and risk will be heightened for DOD installations compared with local agencies. This heightened security and risk due to both the complications of extra security in a system in relation to cost and the importance of what the extra security is guarding should be taken into account when contrasting local agencies expenses on considered systems. Additionally, DOD installations must first consider security requirements that can be both feasibly reached and also tied into local civilian systems securely. Thus, the DOD will likely have a much harder time creating one overarching system in a virtual model due to differences in every single local municipality across the country.

F. SUMMARY

Physical, hybrid, and virtual models all have their own characteristics that provide both advantages and disadvantages. Provided cloud computing is compatible with the eventual model that FirstNet employs, cloud computing may be capable of providing increased efficiencies and cost savings to FirstNet compatible DOD systems. Pairing FirstNet with the best DOD cloud computing schemes via IaaS, PaaS, or SaaS to create a synergistic will depend on which model for FirstNet is chosen and how that model relates to DOD installations. That is to say, depending on the model and individual installation, numerous

schemes may be necessary across the DOD to ensure flexibility and cost savings.

These cost savings must be vetted by comparing multiple cost models and metrics. Through the use of multiple models and metrics, different approaches can be measured and compared to ensure that the DOD gets the most effective system for the best cost. It is important to use numerous checks and balances through multiple models as each model has different strengths and weaknesses. The key to any model, however, is to first understand exactly what the DOD finds most valuable in order to place a larger weight on what the DOD needs vice what the DOD can do without or at least values less.

V. CONCLUSION

A. INTRODUCTION

The predictive physical, virtual, and hybrid models all offer their own respective benefits and downsides to both the Marine Corps and the civil sector. Combining the input variables in the form of potential costing models, costing metrics, and lessons learned from using Camp Pendleton SES as a case study, an overall analysis can be completed to analyze the generic potential impacts of each model for the Marine Corps and civil sector alongside one another, albeit with no real costing data to speak of, as FirstNet is currently still in the beginning stages of development. This chapter seeks to compare the analyzed predictive models gain an understanding of future Marine Corps impacts, and provide MCICOM G-6 with a sound way forward in FirstNet development for the Marine Corps.

B. BENEFITS/DRAWBACKS OF IMPLEMENTATION (PHYSICAL, VIRTUAL, HYBRID)

Each potential predicted model has many different beneficial factors useful for comparison, as displayed in Figure 14. It is especially important to note how these factors will influence the DOD implementation of FirstNet and which factors are in line with both the most effective way for DOD first responders to operate with one another and with civil entities. Therefore, an analysis of the predictive models against one another is appropriate.

	Physical	Hybrid	Virtual
Overall Benefits	• Homogenous network • High interoperability • High standardization • Low DOD risk	• States already lease spectrum • Local level gets state assistance • Can incorporate some existing systems • Maintenance assistance from state for local agencies Balance of flexibility vs. scalability	• High flexibility/ scalability • DOD can apply by case • Local agencies can purchase only what they need/ barter for lower costs • Strong DOD/ local networks • Possible minimal expense for large/ cutting edge agencies • Local control of maintenance
Overall Pitfalls	• Decreased flexibility/ scalability • High cost • Difficult maintenance • Complications from massive enterprise undertaking • High potential overhead at edges • Lack of local control	• DOD that operates regionally must adjust to meet state needs • States must ensure compliance even with poor agencies with poor equipment (potential high state costs)	• Decreased interoperability • Loose standardization possible • Higher cost at local level • DOD must purchase multitude of systems • Difficult for small agencies • Maintenance costs for small agencies high
Benefits vs. Physical	NA	• Happy medium of flexibility/ scalability • State control can cater large network to state problems (i.e., wildfires, hurricanes) • Small local agencies backed by larger state funding • Local agencies have state controlled maintenance	• More flexible/ scalable • DOD can save money by applying upgrades only where needed/ easier to barter lower costs depending on region • Strong local DOD/ civilian ties • More autonomy to cater system to local problems

	Physical	Hybrid	Virtual
Benefits vs. Virtual	• Standardization across the DOD regardless of location • Few seams/ gaps • Nationwide ubiquitous interoperability/ standardization	• State funding backs local agencies • Overall state integration creates less seams/ gaps • State more capable of incurring initial investment than some small agencies	NA
Benefits vs. Hybrid	• No DOD regional or state problems with hierarchy or equipment (DOD standardization) • Standardization/ interoperability improved for mass disaster issues	NA	• Local municipalities can cater directly to its own needs • Increased flexibility • More scalable • DOD can apply costs to each installation based on local needs

Figure 14. Physical/Virtual/Hybrid Comparison

1. Physical System Benefits/Drawbacks versus Virtual and Hybrid Systems

Overall, the physical system is the most homogenous network, providing high interoperability and standardization through nationwide coverage. Additionally, the Physical system poses a low risk for the DOD, as the entire country will be forced to standardize and vet the system prior to the DOD applying itself to FirstNet. Lessons learned from coast to coast would be beneficial from the physical system model, as there would be more data on what worked versus what did not work for the single system as opposed to the virtual or hybrid systems where many different systems might be created.

Compared to the virtual model, there are several important items of note where the physical model excels. First, standardization across the DOD regardless of location means that the same equipment, maintenance standards, training courses,, enables the DOD to be completely interoperable across

services. Additionally, each installation would be interoperable with both local civil entities and civil entities in other states, making the physical model excellent in response to national disasters which may require out of state resources. This interoperability and nationwide ubiquitous coverage means that there are few seams and gaps across municipal boundaries.

The physical model would be ideal if money were no object and could result in allowing for a robust and flexible network. Realistically, however, a large scale enterprise across the nation would require a hefty infrastructure and robust organizational and maintenance planning. Unfortunately, the large, overarching infrastructure and high cost that would be associated with such an enterprise could lead to decreased flexibility and scalability and complications from the massive enterprise undertaking.

A physical model would likely not be able to provide unique support to the edges, creating a flexibility/scalability problem. Unique support is required, as every area in the United States suffers from its own natural and societal issues, whether a problem with natural disasters such as earthquakes or an urban center with high crime. FirstNet must be able to meet the unique demands of every municipality across the United States, due to the lack of local control of the system in a physical model. Ultimately, the more overarching the system, the more difficult it will be to solve maintenance problems at low levels, ensure proper response time of responders, and keep local municipalities from having a high initial overhead, especially in poorer agencies with older equipment.

2. Virtual System Benefits/Drawbacks versus Physical and Hybrid Systems

The virtual system has several overall benefits that distinguish it from the physical and hybrid models. First and foremost, the virtual system has high flexibility and scalability. Since the virtual model is applied at the local level, local agencies would be able to purchase only what they need and additionally barter for lower costs through providers in the local area. Areas that are prone to unique

natural disasters will be able to tailor their systems to include provisions for such emergencies.

Concerning the DOD, the virtual model would provide the strongest ties between installations and the surrounding civil municipalities. Agencies that already have newer equipment would plausibly have smaller initial costs, provided the capabilities of their existing equipment were in line with federally mandated requirements. The DOD would be able to apply funding and network upgrades by each unique case pertaining to installations. Additionally, the local control of networks would allow municipalities to adjust for local maintenance problems as soon as they see fit.

Compared to the physical and hybrid models, state and nationwide interoperability would potentially be diminished. As each and every local municipality would be responsible for their own networks, reasonably these networks may vary. The variance would be dependent upon the federal rules and regulations that prescribed requirements for local municipalities. The decreased interoperability would be most apparent during mass emergency situations such as natural disasters.

Local municipalities would be required to fit the bill for costs of networks and equipment. Moreover, DOD installations would be hamstrung by networks that local municipalities were operating on, and required to use equipment that could tie into local municipalities but would not necessarily be interoperable across the DOD. Therefore, the DOD would likely have to purchase a multitude of systems to apply to each and every unique installation's needs, based on acquisitions of agencies local to each installation. Because of the high costs of maintenance for each agency, many smaller agencies may have a difficult time fitting the bill to become compliant with federal standards.

3. Hybrid System Benefits versus Physical and Virtual Systems

Overall, the hybrid model is currently the most logical model for FirstNet to follow. The hybrid model provides the most reasonable compromise of flexibility

and scalability. While not necessarily the ideal model for the DOD from a cost and standardization standpoint, the DOD has much to gain from the effective regional layout of the hybrid model. As previously stated, states have already leased and are using the D-band spectrum, and will continue to acquire equipment and procedures to fully utilize the D-band.

At the local level, agencies would gain assistance from an overarching state layout that tied all agencies in the state together, allowing for flexibility toward the unique problems that each state has. This assistance and state architecture could potentially alleviate financial problems across a given state, especially considering smaller agencies with little capital. Each state would be able to incorporate some existing systems in the form of agencies that are on the edge of first responder technology, and have already started acquiring equipment that would eventually be compliant with federal regulations. The same is true for DOD installations, which could develop and acquire systems and networks in preparation for FirstNet rollout.

Overall state integration would create fewer seams and gaps compared to the virtual model. The fewer seams and gaps allow for increased interoperability, at least among states. However, these seams and gaps can be eliminated through regional cross-state partnerships. Instances where the DOD operates in regional networks across state lines (e.g. MCIWEST operating over installations such as Camp Pendleton in California and Marine Corps Air Station Yuma, Arizona) have much to gain by encouraging such partnerships. Moreover, states are more capable of incurring the initial investment and maintenance costs than many small agencies.

Similar to the virtual model, the hybrid model would require a multitude of different systems, networks, standards and equipment across the DOD. Organizations such as MCIWEST must adjust to meet state needs across plausibly several states. Additionally, states must ensure compliance with poor agencies that could incur high initial state costs to help upgrade each municipality. Contrarily, if a given state decides to place the burden of initial

upgrades on local agencies, those local agencies must find a way to meet costs and comply. While requirements for DOD installations would not be as diverse as the virtual model, requirements would still be unique to each state, or at the very least each regional partnership of states.

4. Security and Policy Issues

As previously mentioned in Chapter III, there are numerous concerns regarding security and policy issues at each individual installation. Should the local municipalities not have the same level of security as a given DOD network, the DOD network must be able to prevent disclosure of sensitive security information, block hazardous incoming information, and still meet security requirements of the local municipality. These requirements are in addition to the overall interoperability goal of a union between installation and local responders. Should security requirements be too incompatible with interoperability, both the installation and local authorities will suffer from the lack of mutual support capabilities. At the crux of security requirements is the interoperability of CAD systems across installation/local agency boundaries. While EMC2 may alleviate some of these issues, it is imperative that MCICOM continue to analyze and consider solutions to any EMC2 interoperability gaps that may arise due to security, and strive to solve these either before or through FirstNet implementation. The overall goal should be full interoperability with civil responders while maintaining the security integrity of installation information and systems.

Policy must be developed through both MCICOM and the DOD Chief Information Officer (CIO) to allow for FirstNet to fulfill its interoperability intent. As discussed, current security requirements, funding issues, and network and equipment interoperability issues prevent such interoperability. While FirstNet may address much of the technical issues, security policy will continue to be a disparate quality between both the DOD and civil sector.

Recently, the Department of Defense partnered with the National Institute of Standards and Technology (NIST) to build a "unified information security network for the entire federal government" (Brown, 2014). The new requirements, which currently will be integrated over the course of three years, have the ultimate goal of "the defense, intelligence and civil communities using a common strategy to protect critical federal information systems and associated infrastructure" (Brown, 2014). The integration of NIST standards will have an impact on installation and local security interoperability, but due to the developing nature of NIST implementation, the DOD currently has the ability to integrate NIST standards with existing and upcoming equipment such as CADs, EMC2, and FirstNet equipment through bridging the gap in policy to allow integration of these systems.

C. SUGGESTIONS FOR FURTHER RESEARCH

First and foremost, it should be repeated that the models outlined in this paper are predictive models, and in no way absolutes for what the future of FirstNet will look like. Because the development of FirstNet is in the beginning stages, further research should track changes in the development of FirstNet and identify areas where attention is needed to strengthen an inevitable Marine Corps rollout of the program. Moreover, policy must be developed for the Marine Corps and the DOD in general to address FirstNet; therefore further research is necessary to determine how the Marine Corps and DOD can best partner with developing local, state, and federal entities to ensure Marine Corps interests are protected and that joint policies are concurrently developed.

Analysis must be made regarding whether security requirement disparity between the civil and military sector are truly necessary at the level they currently reside. That is, should the current differences in system security between Marine Corps installation first responders and local agencies be held to the same standards as other networks on the same installation? Easing or

compartmentalization of security requirements for Marine First Responders may allow for increased interoperability and decreased security costs at local levels.

As FirstNet further develops, it is additionally important to try to integrate upcoming and current DOD projects with FirstNet if possible. A current project such as Web Emergency Operations Center (WebEOC) is just one of the many plausible upcoming projects that would benefit from research concerning the compatibility with FirstNet (lee.army.mil, 2014). WebEOC is a "common operational picture platform used…to maintain situational awareness and facilitate faster decision making during emergency situations" (lee.army.mil, 2014). The only requirement that WebEOC has for users is a web connection, and is a good tool for "sharing and disseminating information" (lee.army.mil). This kind of technology could provide enhanced usage out of FirstNet should research provide compatible points of the two systems. Overall, the most important facet of continuing research is for MCICOM to continue to monitor the development of FirstNet, ensure MCICOM stake at the appropriate levels, and use research to facilitate policy making, acquisition decisions, and relationship development.

D. CONCLUSION

In conclusion, MCICOM G-6 should keep close ties with the DOD Public Safety Communications Working Group. As the premier DOD liaison to the First Responder Network Authority, the working group enables MCICOM G-6 to both present Marine Corps requirements through the working group and stay ahead of upcoming FirstNet developments.

These ties are vitally important for the future of Marine Corps first responders for several reasons. First, MCICOM must stay abreast of upcoming FirstNet requirements. These upcoming requirements have impacts on equipment and network acquisition for Marine Corps installations. Should FirstNet present future requirements long in advance, it is in MCICOM's best interest to work with state and local administrations in order to steer installation acquisitions toward compliance with upcoming requirements long before rollout in

order to both save money and ensure flawless integration with FirstNet. Moreover, MCICOM can present current equipment and determine whether new acquisition is required, or whether MCICOM has the ability to influence overall FirstNet regulations for the best interests of the Marine Corps and possibly the DOD overall.

In regard to relationships, ensuring that Marine Corps installations are aware and working toward developing new and maintaining current relationships would allow Marine Corps installations to be embedded in state development in order to ensure that installation requirements are considered at the state level long before rollout begins and state buy-in occurs. The Marine Corps must embed itself early in the FirstNet development process at the DOD level and state level in order to ensure that each Marine Corps installation is acquiring equipment that will be both compliant with state and local standards and capable of saving the Marine Corps from wasting time and money on systems that will need to be replaced upon the rollout of FirstNet. Additionally, MCICOM should ensure that when state and local security and policy development begins installation interests are represented in order to ensure system flexibility, regional, state, and local administrative seamlessness, and overall interoperability. This early and continuous application of attention and negotiation in all levels of local, state, and federal FirstNet development would pay dividends in the form of time and capital for MCICOM.

LIST OF REFERENCES

Barnett, J. (2012). *What should FirstNet do first? State integration into the National Public Safety Broadband Network*. Washington, DC: Potomac Institute Press.

Baset, S. (2012). *Cloud SLAs: Present and future*. IBM Research. Retrieved from http://www.cs.columbia.edu/~salman/publications/baset-sla-osr.pdf.

Becker, M. (2012). *Interoperability case study: Cloud computing*. Cambridge. Berkman Center for Internet and Society, Harvard University.

Berry, J. (2003). How to apply EVA to IT. *CIO.com*. Retrieved from http://www.cio.com.au/article/180157/how_apply_eva_it/

Bogden, G. (1998). Florida's historic 1998 wildfires: 1998 wildfires scorch central Florida. *The Orlando Sentinel*. Retrieved from http://www.orlandosentinel.com/multimedia/orl-1998wildfires-pg,0,6789435.photogallery?index=orl-1998wildfire2pic20070308134926

Brinkerhoff, J. (2009). Domestic operational law: The posse comitatus act and homeland security. *Center For Army Lessons Learned Newsletter*, 10–16. Retrieved from http://usacac.army.mil/cac2/call/docs/10–16/ch_12.asp

Brown, E. (2014). NIST, DOD, intelligence agencies join forces to secure U.S. cyber infrastructure. *NIST Public and Business Affairs*. Retrieved from http://www.nist.gov/public_affairs/releases/cyber_infra_061009.cfm

Bundled pricing (n.d.). In *Businessdictionary.com.* Retrieved from http://www.businessdictionary.com/definition/bundled-pricing.html

Dhar, S. (2012). From outsourcing to cloud computing: evolution of IT services. *Management Research Review*, 35(8), 664–675.

Dowd, C. (2013). FirstNet story. *APCO Public Safety Broadband Summit*. Retrieved from http://www.ntia.doc.gov/files/ntia/publications/apco-may_14–2013chuck_dowd_final.pdf

Economic value added (EVA) (n.d.). In *Investopedia.com*. Retrieved from http://www.investopedia.com/terms/e/eva.asp

First responder (n.d.). In *Merriam-Webster.com*. Retrieved from http://www.merriam-webster.com/dictionary/first%20responder

Ferrus, R., Pisz, R., Sallent, O., & Baldini, G. (2013). Public safety mobile broadband: A techno-economic perspective. *IEEE Vehicular Technology Magazine*, 8(2), 28–36.

GAO (2007). First responders: much work remains to improve communications interoperability. *GAO Report to Congressional Requestors*.

Garfinkel, S. L. (2011, Nov). The cloud imperative. *Technology Review*, 114, 74–75.

Goel, N., & Aggarwal, A. (2013). Cloud computing platform: A Perspective Overview. *International Journal of Scientific and Research Publications,* 3(6), 1–4.

GPO. (2012). *Middle class tax relief and job creation act of 2012*. 112th Session of U.S. House of Representatives (2012). Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf.

Headquarters, United States Marine Corps (2012). *Consolidated emergency response system (CERS) capability production document (CPD)* [Memorandum]. Washington, DC: Author.

Hearing on oversight of FirstNet and emergency communications: Testimony before the Subcommittee on Communications and Technology Committee on Energy and Commerce, 113th Session of U.S. House of Representatives (2013) (testimony of James A. Barnett. U.S. Congress).

Hedonic pricing (n.d.a.).In *Businessdictionary.com*. Retrieved from http://www.businessdictionary.com/definition/hedonic-pricing.html

Hedonic pricing (n.d.b.).In *Investopedia.com.* Retrieved from http://www.investopedia.com/terms/h/hedonicpricing.asp

Hopper, D. (1998, July 7). Virginia firefighters to lend a helping hand in Florida. *The Free Lance-Star*.

Internal rate of return (IRR). (n.d.). In *Investinganswers.com*. Retrieved from http://www.investinganswers.com/financial-dictionary/investing/internal-rate-return-irr-2130

Jackson, D. (March 1, 2012). The big bang. *Urgent Communications*. Retrieved from Urgentcomm.com

Kihal, S. E., Schlereth, & C., Skiera, B. (2011). *Price comparison for infrastructure as a service*. Frankfurt, Germany: Goethe University.

Lee.army.mil. (2014). Fort Lee webEOC. *Lee.army.mil*. Retrieved from http://www.lee.army.mil/dptms/ioc/installation.operations.center.aspx

MARADMIN 497 (2007). MCNOSC mission statement tasking addition–enterprise land mobile radio (E-LMR) system management. *Marines.mil*. Retrieved from http://www.marines.mil/News/Messages/MessagesDisplay/tabid/13286/Article/113457/mcnosc-mission-statement-tasking-addition-enterprise-land-mobile-radio-e-lmr-sy.aspx

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *NIST Special Publication*, 800(145), 7.

Net present value (NPV) (n.d.). In *Investopedia.com.* Retrieved from http://www.investopedia.com/terms/n/npv.asp.

Pendleton.marines.mil. (2014). Marine Corps Base Camp Pendleton security & emergency services. *Pendleton.marines.mil*. Retrieved from: http://www.pendleton.marines.mil/StaffAgencies/SecurityEmergencyServices.aspx

Platform as a service (n.d.). In *searchcloudcomputing.techtarget.com*. Retrieved from: http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS

Reynolds, E. (2013). *FirstNet: Vision for the future.* [PowerPoint slides]. Retrieved from http://www.ntia.doc.gov/files/ntia/publications/georgia_technology_association_ed_reynolds_052113_final.pdf.

Rufer, S. (2012). *The hidden extras: The pricing scheme of cloud computing* [PDF document]. Retrieved from http://www.csg.uzh.ch/teaching/hs11/inteco/extern/talk5.pdf

Sekiya, Y. (2012). Software technologies of composing IaaS clouds: WIDE cloud as a case study. *Computer Software*, 29(2), 2–15.

Srinivasan, M. (2012). Building secure enterprise model for cloud computing environment. *Academy of Information and Management Sciences Journal*, 15(1), 127–133.

Sun, A., Ji, T., Yue, Q., & Xiong, F. (2011). IaaS public cloud computing platform scheduling model and optimization analysis. *International Journal of Communications, Network and System Sciences*, 4(12), 803–811.

Syal, S., & Goswami, M. (2012). Effective cloud computing: Innovations and challenges. *International Journal of Management Research and Review*, 2(10), 1800–1809.

Techopedia.com. (2014). IT cost transparency. *Techopedia.com*. Retrieved from http://www.techopedia.com/definition/27221/it-cost-transparency

Techopedia.com. (2014). Public safety answering point (PSAP). *Techopedia.com.* Retrieved from http://www.techopedia.com/definition/2969/public-safety-answering-point

Terremark.com. Enterprise cloud services. *Terremark.com.* Retrieved from http://www.terremark.com/services/infrastructure-cloud-services/enterprise-cloud.aspx

United States Department of Commerce. (2013). National Telecommunications and Information Administration website. http://www.ntia.doc.gov/

Unity of command (n.d.). In *Businessdictionary.com*. Retrieved from http://www.businessdictionary.com/definition/unity-of-command.html

Utility (n.d.). In *Investopedia.com.* Retrieved from http://www.investopedia.com/terms/u/utility.asp.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California