2019

Knowledge Sharing and Customer Relations in Mobility

Katie Dyretha Moore
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Katie Moore

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Lydia Forsythe, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Steven Matarelli, Committee Member,
Public Policy and Administration Faculty

Dr. Mark Devirgilio, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2019

Abstract

Knowledge Sharing and Customer Relations in Mobility

by

Katie Moore

M.S., Indiana Wesleyan University, 1996

B.A., Mississippi Valley State University, 1985

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

June 2019

Abstract

After the events of September 11, 2001, inadequacies in how government organizations and agencies shared knowledge and communication with defense mission partners became readily apparent. A reasonable U.S. government information technology expectation is the integrated use of mobile phones across organizations and agencies. Yet, it is difficult to meet this expectation, as the provisioning process for mobile devices can be different for each government organization or agency. The Department of Commerce National Institute of Standards and Technology does not set provisioning standards, and organizations and agencies determine policies tailored to their particular needs. Using Schein's theory on organizational culture, the focus of this phenomenological study was to explore the Mobility provisioning process from the experiences of government customer support personnel. Eleven personnel responded to 10 semistructured interview questions derived from the research question. The data were manually transcribed and then coded, arranged, and analyzed using a software tool. Three major themes emerged from the analyzed data: (a) expand communication with customers and leaders, (b) identify policy guidelines, and (c) streamline and centralize the process. Using these themes, recommendations include enhancing communication among stakeholders, provisioners, and Warfighters, soldiers in the field; implementing standardized user policies; and improving cross-organization and cross-agency provisioning processes. Social change actions include increasing mobility provisioning efficiencies among provisioners, which not only saves time and money, but also provides Warfighters with affordable, dependable, and reliable mobile communications systems.

Knowledge Sharing and Customer Relations in Mobility

by

Katie Moore

M.S., Indiana Wesleyan University 1996

B.A., Mississippi Valley State University 1985

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

June 2019

Dedication

This paper is dedicated to John Perry Moore and Elmenthel Smith Moore for their sacrifice and struggles to guide and support their family. I am simply one of the benefactors of their hard work and determination to live a peaceful, dutiful, courageous, and blessed life. I humbly, and with the greatest respect, thank you.

Acknowledgments

I want to thank Dr. Lydia Forsythe, my faculty chairperson, for your incredible words of motivation. Also, special thanks to Dr. Steven A. Matarelli for your attention to detail and unbelievable patience. I also would like to thank Dr. Mark DeVirgilio for his guidance and encouragement to move forward. I am overwhelmed by your support but grateful for your knowledge and expertise.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

The challenge for many information technology (IT) analysts is to pull together relevant information for analysis at the right time. According to Geller (2012), IT analysts must have the ability to get the correct information to the right person in the shortest time possible. However, the question is how relevant are current IT policies to secure information for government organizations or agencies? Based on the current government IT culture and new communication techniques that utilize mobile devices, the current policy as it pertains to information security (IS) is broad but does not set standards or boundaries specific to each government organization. Department of Defense (DoD) organizations and support agencies must develop their own policies or regulations that are unique to their risk assessments and needs. Since the events of September 11, 2001 (9/11), the awareness of how government supports national security has escalated on all fronts domestic and foreign (Randol, 2010). My focus in this study was to explore the culture and perspectives of government IT analysts and engineers in a Mobility Directorate, post 9/11, in their support of mobile devices throughout the provisioning process.

I designed this study to identify, describe, and analyze the provisioning practice of a Defense Mobility Unclassified (DMUC) Implementation and Sustainment Process. Specifically, I investigated the users and stakeholders' experiences and perspectives in sharing information with the Mobility customer support team and the factors that affect the provisioning process. To support social change, I examined the experiences of stakeholders who contribute to Mobility's provisioning process.

Social change is not something that just happens in life; it must be cultivated from the experiences of others to support the greater good. There are risk factors and levels of danger associated with the political interpretation of market economies that eventually leads to new systems or social change (Bush, 2016). I based my research on the perspectives of stakeholders who support and utilize mobile products and services to include those who provide the first-hand experience. Stakeholder perspectives added value for new actions, public laws, and policy changes that support social change in the future. Chapter 1 includes the: (a) background of the problem; (b) statement of the problem; (c) purpose of the study; (d) nature of the study; (e) research question; (f) conceptual framework; (g) definition of terms; (h) significance of the study; (i) implications for social change; and (j) assumptions and limitations.

Background of the Problem

Since the terrorist attacks of 9/11, the American government and governments around the world have grappled with how to collect, analyze, and distribute intelligence to protect their homeland against terrorists' attacks (Randol, 2010). The events of 9/11 affected government agencies worldwide, which included a four-letter combat support agency for the DoD. The agency supports IT enterprise systems for the Warfighter, the soldier in the field. In conducting my research, my main priority was to analyze the IT culture of analysts who previously operated in non-sharing environments that now support Mobility's provisioning process through knowledge sharing in the mobile implementation and sustainment process. From the stakeholders' perspectives, I investigated factors that affect Mobility's organizational culture, security policy, and the

provisioning process. After 9/11, there has been a culture change in the United States and an increased awareness worldwide of terrorist threats specifically for defense agencies.

After 9/11, the government security environment adopted a culture of information sharing, which was considered a necessity given the fact that intelligence agencies failed to share information across the board before 9/11; reforms were needed in the current security environment (Jones, 2007). That culture had to change to combat terrorism for future generations. The government needed to transition from restricting information in a Cold War fight to establishing procedures to share information in the new technology age of instant messages and transnational terrorism (Jones, 2007). The Intelligence Reform and Terrorism Prevention Act of 2004 charged the President to develop the Information Sharing Environment (ISE), which provided guidelines to support new policies, procedures, and technology. The guidelines provided a framework to combat terrorism by sharing information to all relevant parties, for example, federal, state, local, tribal bodies, and the private sector (Jones, 2007). According to Jones, the objective was to transition the current security environment from a restrictive "stovepipe" environment to a culture of information sharing.

In the aftermath of 9/11, the U.S. Department of Homeland Security (DHS) was established, in 2002, expanding information-sharing and cybersecurity guidelines for government and industry. For example, federal guidelines and security requirements increased for computer controls systems to operate chemical, electric, and water plants. According to Manalo, Noble, Miller, and Ferro (2015), the National Institute of Science and Technology (NIST) EO 13636 framework "identifies a set of industry standards and

best practices to help organizations manage cybersecurity risks" (p. 62). After 9/11, there were several questions concerning the previous security issues, cybersecurity, and other security problems that may have developed but remain unresolved. To help guard against attacks, including cyber attacks, system acquisitions, development, and maintenance of phones, tablets, removable media, and communication of any kind must be securely supported.

Cybersecurity is directly improved when security requirements are created to improve existing systems, outdated software and hardware are upgraded, and mobile devices and removable media encryption methods are securely backed up (Manalo et al., 2015). Improvements in IS continue to expand and grow, which build a stronger posture in the IT culture and environment. With each new advance brings new challenges because security is never outright, complete, or absolute. Security, whether cybersecurity or otherwise, is never completely secure but rather efforts to protect and secure continue to move forward.

Although some intelligence agencies believe that government information and intelligence should remain restricted due to sensitive information and the potential for a security risk (Hughes & Stoddart, 2012), the restrictive practice of working in a "silo" may have offered a higher level of security. The events of 9/11 changed the perception of working in "silos" to a more collaborative working environment for government officials in the United States and overseas. Thanks to the advances in global communications, including mobility and social media, intelligence agencies can inform the public at large of any potential threats (Hughes & Stoddart, 2012). Intelligence agencies must find new

ways to provide information to those in the field (command combatant posts, agencies, and services) through an effective procurement process that is also secure. Even though defense funds have been reduced and sharing information is still a work in progress, cyber attacks are on the rise and so is the need for safer communication tools.

Defense officials must find the right balance of security and interoperability to support mobility devices across information network systems. Presently, each service or agency has a program or strategy of Bring Your Own Device (BYOD) for implementation, but the provisioning process may be somewhat challenging. The most significant challenges for DoD and the Navy are managing policy and ensuring security (Jontz, 2015). Although government services want to mirror industry by having the latest mobile devices, securing mobile devices has been a slow process due to the previous culture, policies, and cautious process review. According to Jontz, Halvorsen, DoD's chief information officer (CIO), frequently promoted or inserted the words "secure enough" to support mobile policies and practices (para. 7). According to Randol (2010), Congress and the intelligence community made a connection between domestic and foreign terrorist threats. Based on new security intelligence, threats to the homeland are considered national threats, whether the threats come from inside or outside the United States. In this new era of communication, with the advances of the Internet and social media, information is abundant; however, the question of security and consistent regulation across agencies remain. The technical and resource capacities of the United States were insufficient to prevent citizens and their infrastructures from becoming the targets of terrorist attacks (Unlu, Matusitz, Breen, & Martin, 2012). Now the goals are to

synchronize federal and state efforts to share information and to unite efforts and ideas to combat terrorism at all levels. Securely sharing information is essential to government agencies, specifically agencies that provide information to DoD.

In this study, I interviewed government IT team members: IT analysts and leaders, engineers, account managers, and mission partners (MPs), collectively known as stakeholders, from a combat support government agency that supports IT and the Warfighter. I interviewed customer account managers (CAMs) and IT officials to describe their experiences with provisioning mobile devices to detail their thoughts as to how to overcome the challenges of a new culture and policy limitations to explain and improve the overall process. I explored the lived experiences of the stakeholders who support the mobile provisioning process.

For this study, I selected a phenomenological approach using interviews due to the richness of information provided through the lived experiences and personal stories of each interviewee. These interviewees provided an authentic and realistic account of events regarding the process. I obtained firsthand information and insight from the interviewee's perspective as it relates to their concerns regarding public policy, culture, and process challenges.

Statement of the Problem

Computer viruses, security threats, and terrorists continue to threaten homeland security and communities around the world (Randol, 2010). The actions involved in homeland security intelligence (HSINT) are not new concepts. After the events of 9/11, HSINT's level of importance became more relevant regarding local security for

municipalities, state facilities, and private sector stakeholders (Randol, 2010). Therefore, the awareness of how local law enforcement information supports national security and the importance of HSINT have increased substantially since the events of 9/11. The problems of gaps in supporting customers with no designated support team, provisioning devices from manual inputs to match website orders, and working within security guidelines and policies that vary across agencies are challenges. These items are Defense Federal Acquisition Regulation Supplements (DFARS) and DOD Instruction (DODI) policies and regulations, which are listed on a performance work statement (PWS) and are critical elements to homeland security.

The PWS is awarded as a contract, for services and products, which is subject to DFARS and DODI policies and regulations: DFARS 252.239-7017, DFARS 252.239-7018, and Supply Chain Risk, DODI 5200.44 Protection of Mission Critical Functions. Contractors are required to submit a plan to mitigate risk. Per MITRE (2013), "Supply Chain Risk Management (SCRM) is a discipline that addresses the threats and vulnerabilities of commercially acquired information and communications technologies within and used by government information and weapon systems" (para. 1). The expectation is to minimize the risks and identify systems, components, parts, and materials that could be from non-trusted sources or foreign adversaries. Defense agencies attempt to address SCRM guidelines in several ways. Specifically, risks associated with products and services that provide contract support in a PWS. The PWS between the government and vendor must include an SCRM plan with the submission of the vendor's technical proposal. In addition, within 30 days of the contract award, the

vendor/contractor must submit a mitigation plan for products and services that will support the contract. Government officials, specifically the customer support team, IT analysts, engineers, and CAMs, consider these challenges or barriers a security and communication risk to the overall process. At an information combat support agency, the Mobility program offers many collaborative tools, which are utilized by internal and external stakeholders. Because some of the tools are mobile devices that are commercial off-the-shelf (COTS) smartphones or tablets, the inability to secure critical information on a device or to secure the user's location is challenging.

The IT Analyst's objective is to track and identify product and manufacturer ownership, suppliers, and subcontractor changes, to avoid future problems. However, the lack of a cohesive support team to communicate with potential users and customers to guide them through the provisioning process is the main problem. To support the current IT environment, the customer support team must understand and adhere to IT security standards, public laws, and policies. The current environment is transitioning from an IT culture to a cybersecurity culture. The entire process is an enormous challenge. According to Halvorsen,

> The biggest difference with cyber that mobility has to react to is it moves faster than any other warfare. That is a challenge. The things we do today in cyber probably will not be the same things we do tomorrow. (C-SPAN, 2015)

Mobility tools and products that support communication and sharing information in real time for military services worldwide must continue to expand.

The purpose of my research was to understand the impact to the Mobility provisioning process as it related to policy, culture, and process. When mobile devices are not operational, timelines for delivery have expanded, and users cannot access help from customer service. I wanted to help leadership establish better guidelines and policies to support the Mobility effort.

Propose of the Study

The purpose of this qualitative phenomenological study was first to describe and analyze the government IT culture and the attitude regarding provisioning Mobility devices. Second, I asked government IT analysts, engineers, end users, leadership, and CAMs for feedback on the overall provisioning process, configuration schedule, knowledge sharing, and communication with customers. Third, I asked stakeholders for their opinions on IT security policy adjustments and guidelines for Mobility devices for field users. Through this study, I described the impact to security and communication related to the mobile device provisioning process that supports DoD policy and federal code. U.S. Code, Title 44 Public Printing and Documents, Chapter 35 Coordination of Federal Information Policy, Subchapter II Information Security (44 U.S.C. § 3551, 2014) provides an outline to support and ensure effective security controls and oversight for information systems and resources that support federal operations, products and resources (para. 1–6). Per the U.S. Government Publishing Office (n.d.), Title 44 U.S.C. § 3551 supports prior provisions; for example, the e-Government Act of 2002, Public Law (P.L.) 107-347, title IV, sec. 402(b), Dec. 17, 2002, 116 Stat. 2962. PL 107-347, to establish and promote measures on a broad range of government information services (para. 10).

Public Law 107–347 required each federal agency to develop an agency-wide program to provide IS, support operations, policies, and procedures for DoD agencies. The Defense Information Systems Agency (DISA), a DoD combat support agency, manages the mobile device provisioning process in support of the MP's needs. In this study, I explored the lived experiences of government IT analysts, engineers, end users, leadership, CAM, and stakeholders. The stakeholders include all those who utilize the service and support the mission, for example, CAMs, IT analysts, engineers, MP, Mobility's end users, and leadership. I explored how and what they felt about the Mobility process for provisioning mobile devices. The Mobility provisioning component is part of a more extensive operation that falls under the DoD Unclassified Mobility Service (DMUS). Device provisioning supports the onboarding process, registration timelines for approvals, device configurations, and support to end users. The basic concept is to provide safe connection and communication for the end user through mobile devices (Emad-ul-Haq et al., 2015). The provisioning component supports Mobility's overall infrastructure service. This study provided more detail and meaning to the body of knowledge that will contribute to the overall understanding of the obstacles to provisioning a mobile device to stakeholders.

Nature of the Study

To address the problem, I conducted a qualitative phenomenological study to explore the lived experiences and perspectives of the IT stakeholders based on an organizational culture theoretical lens, which supports broader communication and collaboration across directorates. This study entailed obtaining information from in-depth

interviews of 11 research participants. A sample size of 10 is the norm for qualitative phenomenological studies because the saturation of the collected data is typically reached with this number of participants (Creswell, 2013). Chapter 3 contains a detailed explanation of the sample size.

I identified problems in communication to design a research plan that describes the IT culture that supports the mobile device provisioning process. Qualitative research provided an approach to help understand the lived experiences of IT customer support and stakeholders. This research also helped to identify policies, governance, and related knowledge sharing internal information to support a DoD combat support agency. I described and explored the impact of Mobility's provisioning process on IT customer support and stakeholder's culture in strategic planning for cyber development directorates.

The provisioning process supports knowledge sharing, which provided an environment to consolidate information and reduce cultures that support "silos." As noted by Creswell (2009), a good qualitative purpose statement supports the rationale for the study, the potential research participants, and the area of focus. Because the utilization of mobile technology is relatively new for government MP and field users, the groundwork is needed to support and expand policies in the future. To influence tomorrow's policies, the National Security Agency (NSA) Central Security Service's (2009) Mobility Security Guide provides the enterprise Mobility architecture and guidelines that helped build new policies. Currently, the focus is on how to utilize commercial devices to securely connect users to government networks around the world.

The participants that I chose for this study were IT customer support personnel and stakeholders who utilize or support Mobility services. The main research question served as the basis for the study and for devising interview questions (see Appendix A for interview questions). I provide a comprehensive discussion of this study's methodology in Chapter 3.

Research Question

One main research question guided this research: What are the lived experiences for end-users in the government IT culture using the Mobility provisioning process for the sharing of information?

Conceptual Framework

The conceptual framework for my study was organizational culture theory, which I used as the foundation to analyze the lived experiences of stakeholders who utilize, sustain, and support a DMUC Implementation and Sustainment Process, supported by two contrasting theories. Organizational culture theory provided the central theoretical perspective for this study. Communication risk philosophy offered another theoretical perspective used to measure, examine, and explore threat factors with specific communication phases.

Organizational culture theory is used to explain lived experiences from the stakeholders' perspectives. Specifically, the stakeholders provide support to the Mobility provisioning process, which in turn supports organizational beliefs, rules, and procedures. Schein's (2010) organizational culture theory offers a cultural approach based on three levels: artifacts, which includes culture and symbols; beliefs, which includes policy and

rules; and assumptions, which are made up of processes and behaviors. Organizational culture theory provided the theoretical perspective for this study. Schein provided new concepts to observe phenomena, to define a structure, and to predict how it may look in the future. The culture of organization theory offers the ability to examine the behavior of stakeholders and explore the protocols of the provisioning process of one agency. Schein identified three levels of culture: artifacts, belief and values, and basic underlying assumptions. According to Schein, the visible and known aspects of an organizational structure are the outer layers, but what is unknown are the inner layers, or perspectives, of those who have experienced a culture change. I examined those stakeholders from the inner layer of culture change for Mobility's provisioning process.

I used organizational culture theory to describe a government defense agency's environment, ability to communicate and share information, and provision mobile devices to stakeholders. Before 9/11, open communication was considered a security risk. After 9/11, communication and security for government IT stakeholder support took on a new role in cybersecurity. However, there are ranges of distinctions as to how they relate to past and present efforts. According to Sheppard, Jansoke, and Liu, (2012), the National Consortium for the Study of Terrorism and Responses to Terrorism (START) identified a risk communication philosophy indicative of three phases: preparedness, response, and recovery, which are summarized as follows.

- Preparedness: preventative measures of risk communication which include education on different threat factors;

- Response: communication carried out immediately prior to an attack and the warnings or alerts during the event;
- Recovery: communication methods used in the time following an event. (p. 2)

Organizational culture theory identifies organizational environments, rules, and behaviors (Schein, 2010). Sheppard et al. (2012) described risk communication as a philosophy of event phases that identifies threats, rules, responses, methods, processes, and assumptions used to support and recover communication among interested parties. However, Schein focused on organizational culture while Sheppard et al. managed organizational risk. Risk communication philosophy allows stakeholders the ability to measure threat factors, examine IT responses, and explore methods of the provisioning processes now and in the future. Although federal, state, and local communities need a well thought-out and effective way to communicate during times of crisis, emergencies, and threatening events, my study mainly focused on Mobility's organizational culture from the stakeholders' perspectives.

Principally, my research not only described Mobility's organizational culture but also identified policies and defined processes that directly impact the experiences of government IT stakeholders. This my research included policies developed to support knowledge sharing, communication, and collaboration among government IT analysts and stakeholders. Policies are and not created by chance; they are determined and known to be structured and deliberate. Coombs (2015) stated, "A crisis is unpredictable but not unexpected" (p. 3). When a crisis event takes place, I must make sure that I use the best

method of communication that is determined, appropriate, and secure. My research questions addressed culture, policies, and processes for mobile communication.

Definition of Terms

The following terms add clarification to the following chapters. The purpose was to explore gaps in communication with regards to government IT analysts, CAMs, and stakeholders who collaborate in the mobile device provisioning process.

Artifacts: based on organizational structures and processes, which support organizational culture theory (Schein, 2010).

Beliefs and values: based on cultural aspirations, policy, and goals in support of organizational culture theory (Schein, 2010).

Biometrics: a method of authentication by identifying biological or behavioral characteristics of an individual, for example, fingerprints, voice, signature, and other unique features (Jain, Bolle, & Pankanti, 2006).

Common access cards (CAC): used to access, sign, and authenticate DoD unclassified emails, network systems, and other documents (Miller, 2016).

Crisis and risk: provide adverse outcomes, actions, and events that impact an organization's performance that affects stakeholders in significant ways (Coombs & Holladay, 2012).

Culture: supports a level of structural stability in an organization or group. Cultures are the customs and rights, norms, values, behavior patterns, rituals, and traditions accumulated through shared learning and shared history (Schein, 2010).

Cyber: involves computer networks and is related to the ability to keep network data secure or not compromised. Cyber is also linked to computer hacking and cyber warfare/cybersecurity, cyber attacks, and cyber realm from unauthorized network users, which could be related to terrorism (Randol, 2010).

Cyber operating principles: supports authenticated user access and freedom of maneuver to cloud, collaboration, command, and control capabilities; without impact from rogue entities, hacktivists, nation states, or insider threats (DISA: Strategic plan, 2015–2020, n.d.).

e-Government initiatives: increase outcomes for policymakers, public managers, and public organizations and governments to effectively utilize technologies that will increase citizen participation (Welch & Feeney, 2014).

End users: remain DoD customers and stakeholders who subscribe through the DMUC Enterprise Mobile Management Center (EMMC) for a mobile service provider. End users seek access to DoD unclassified networks through a Virtual Private Network (VPN) authentication to ensure that their Mobility devices are protected against data compromise across DoD environments. (Brown, 2015).

Homeland security intelligence: includes various intelligence collection or gathering that is national technical and nontechnical (not specific source; Randol, 2010).

Information sharing: supports improved communication and collaboration across federal agencies, networks, and Mobility devices in support of the Joint Information Environment (JIE; DISA: Strategic plan, 2013–2018, n.d.).

Insider and outsider: supports an agency internal "on-site" or from the field as an external or "off-site" MP; supports and guards against cyber threats globally. (InfoSec, 2015).

Interoperable communication: supports identifying problems and establishing standards for communication across systems and government entities in support of the Warfighter and MP (DISA, 2015).

Leadership: a distributed function that continually evolves, and anyone who works toward an anticipated outcome displays leadership (Schein, 2010).

Mission partners: DoD customers who utilize Mobility services and support the agency's mission. Considered key representatives who request services, advocate specific issues, and provide support and information (DISA, 2015).

Mobility: a DoD mobile device program and an essential component to enabling MP and stakeholder's connection to the JIE using an authorized mobile device, anytime, anywhere in the world (DISA, 2016).

Policy: entails a plan of action or guidance from a government agency, which includes national security directives, executive orders, public laws, acts, and other rules and regulations (Information Assurance Support Environment [IASE], 2016).

Provisioning process: a small component of the overall onboarding and registration process, whereby enterprise services for unclassified mobile devices are configured, validated, and distributed to users or stakeholders (DISA, 2016).

Stakeholders: are internal and external customers (working groups) who are required to identify or utilize resources (equipment and services) for critical tasks in support of the Warfighter and DoD leadership (MacGowan, Lofgren, & Vachal, 2009).

Stove pipes or Silos: based on a similarity of a shared task, background knowledge, organizational subcultures, and shared assumptions (Schein, 2010).

Underlying Assumptions: based on cultural perceptions and feelings in support of organizational culture theory (Schein, 2010).

List of Acronyms

APPS	Android Applications
ARO	Authorized Request Official
BPA	Blanket Purchase Agreement
BYOD	Bring Your Own Device
CAC	Common Access Card
CAM	Customer Account Manager
CEP	Competitive Education Program
CIO	Chief Information Officer
CLO	Chief Learning Officer
CMD	Commercial Mobile Device
COTS	Commercial Off the Shelf
CR	Continuing Resolution
CUI	Controlled Unclassified Information
DEPS	Defense Enterprise Portal Service

DEPS	Defense Enterprise Portal Service
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DMUC	DoD Unclassified Mobility Service
DoD	Department of Defense
DODI	Department of Defense Instruction
DREMS	Distributed Real-time Managed Systems
DTIC	Defense Technical Information Center
EMMC	Enterprise Mobile Management Center
FISA	Federal Information Security Management Act
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
GFE	Government Furnished Equipment
GSA	General Services Administration
HSINT	Homeland Security Intelligence
IP	Internet Protocol
IRB	Institutional Review Board
IS	Information Security
ISE	Information Sharing Environment
ISS	Information System Security
IT	Information Technology

JIE	Joint Information Environment
MAS	Mobile Application Store
MDM	Mobile Device Management
MLS	Multilevel Security
MORFEUS	Mobility Onboarding Request Fulfillment Enterprise User System
MP	Mission Partners
NIAP	National Information Assurance Partnership
NIPRNET	Non-classified Internet Protocol Router Network
NIST	National Institute of Science and Technology
NSA	National Security Agency
PEO-MA	Program Executive Office – Mission Assurance
PKI	Public Key Infrastructure
PL	Public Law
PMO	Program Management Office
PWS	Performance Work Statement
SCI	Social and community Intelligence
SCRM	Supply Chain Risk Management
SP	Special Publication
START	National Consortium for the Study of Terrorism and Responses to Terrorism
STIG	Security Technical Implementation Guides
STP	Simplify the Process
TASS	Trusted Association Sponsorship System

USDHS United States Department of Homeland Security

VPN Virtual Private Network

Significance of the Study

Sharing information with mobility is an essential public policy topic to research and explore, especially after 9/11, from the stakeholders' perspective. My study examined government IT culture's ability to provision mobile devices, share knowledge with stakeholders, and support organizational processes and strategic policies. After the events of 9/11, given the current threats of terrorism in the United States and around the world, more and more smartphones are being used to share critical information that is unclassified and classified. According to DISA Director Lt. Gen. Lynn (n.d.), DISA received top-secret mobile devices, which are undergoing testing. Per FCW Staff (2015), in the future, the plan is to test and deploy up to 3,000 secret-level smartphones in 2016 (para. 17). The process of provisioning and deploying smartphones does not resolve current or future terrorist threats; instead, the process is an attempt to address concerns in providing timely information to specific points of contact (POC).

First, I examined the organizational process and rules for governance that may distract from current IT security policies. According to Geller (2012), an IT security analyst's primary concern is getting the right information to the right person at the right time. Second, I describe and focused on the experiences and perspectives of the government IT analysts and engineers' culture in support of the Mobility provisioning process. Lastly, the results provided insight regarding how government organizations can better collaborate and communicate across the board and how policies are reviewed for

relevance to current security issues. By focusing on problem elements, policy gaps, and the provisioning process, as they relate to customers, support is derived for new directions in strategic planning and knowledge sharing. How the government interprets basic communication, policies, and laws are the cornerstone for social change.

In the 2010 National Security Strategy, to promote democracy and human rights, President Barak Obama supported the emergence of new technologies and open communication, for example, Internet, wireless networks, and mobile smartphones as expressions of freedom of speech. Moreover, the study analyzed a DOD Mobility Directorate IT culture's provisioning process as well as how the process and policies affected the users. Therefore, this study helped to inform and support Mobility and IS leadership's strategic goals for global communication and social change that also supported the Warfighter, IT analysts, the public, and global citizens.

Implications for Social Change

After 9/11, sharing information across government agencies was central to addressing the possibility of another terrorist event. Working in "silos" did not support a more collaborative, sharing environment. According to Roesener, Bottolfson, and Fernandez (2014), cybersecurity policies that explain roles and responsibilities do not adequately address future threats (p. 50). In the age of social media with the ability to contact anyone, anyplace, any time, the current federal policies support open communication with secure mobile devices for field users. Additionally, improving Mobility's provisioning process offers an open connection with secure mobile devices,

supports additional standards and policies to combat cyber threats, and cultivates social change by expanding knowledge sharing across federal agencies.

Assumptions and Limitations

I assumed that current guidelines, provided by NIST, are suitable for managing the security of provisioning mobile devices. However, NIST allows each federal agency to determine the appropriate policies and procedures specific to their needs based on risk assessments. Therefore, each agency creates policies suitable to their needs. There are no principal standards across agencies. Policy standards vary from one agency to the next. That variance limits the level of reliability and consistency, which allows for various assumptions and interpretations.

The device provisioning process encompasses many components, for example, the mobile device, carrier service plan, and infrastructure service. For new capabilities and all components to work together seamlessly, information must be provided and shared with all stakeholders. For the DMUC Implementation and Sustainment Process to work efficiently, communication is essential. DMUC systems support the provisioning infrastructure process that provides registration guidelines for end users, which will eventually influence new policies. The assumption was that NIST needed to develop additional policies that focus on updating security standards for products and services, for example, mobile devices, while also limiting communication risks.

Summary

In this study, I did not attempt to solve pending communication problems or eliminate barriers with provisioning mobile devices; instead, I explored how the IT

culture supported the provisioning process with a phenomenology approach. The e-Government Act of 2002 may be inadequate for today's IT and communication standards. My purpose in this study was to identify, describe, and analyze the benefits and challenges of provisioning a mobile device, and to emphasize some resolutions. After President Obama urged high tech and law enforcement leaders to combat security threats by utilizing encryption methods, the Chairman of the House DHS Committee called for a commission to address the matter. According to Peterson (2015), digital encryption is used in two ways: on computers and smartphones, to lock-up data and protect information stored elsewhere. Through this study, I identified challenges to the provision of a mobile device and discovered opportunities for leadership to reflect and collaborate on the best process to secure mobile devices in the future.

Chapter 1 introduced the study. Chapter 2 will present an in-depth literature review that includes the: (a) research strategy; (b) conceptual framework; (c) Mobility's onboarding process; (d) knowledge sharing; (e) federal agencies' policies; (f) IT information sharing struggles; (g) IT processing and provisioning struggles; and (h) research methods. Chapter 3 will cover the methodology, Chapter 4 will cover the results, and Chapter 5 will cover the discussion, recommendations, and conclusions.

Chapter 2: Literature Review

In the event of a terrorist attack (domestic or foreign), in accordance with Intelligence Reform and Terrorism Prevention Act of 2004, government organizations must change the way they communicate, collaborate, and share knowledge in a secure environment Risk communication is a distinct philosophy that supports an event phase to communicate and share knowledge for positive change. There are three phases defined by risk communication: preparedness, response, and recovery (Sheppard et al., 2012). According to Sheppard et al., the executive summary: understanding risk communication best practices and theory, highlighted the government's failure to implement effective risk communication guidelines and standards before 9/11. In my study, I focused on the lived experiences of government IT organizational culture after 9/11. In Chapter 1, I addressed challenges to secure communication, detail the provisioning process, determine policy guidelines, and understand the IT culture from the stakeholders' perspective. Despite the risks, there is a need for government agencies to change from a "stovepipe" communication environment to an environment that is more open to collaboration. The provisioning process is inextricably linked to sharing information, acknowledging communication risks, and recognizing the cultural challenges of past and present. Government IT stakeholders are customers and MP, who rely on secure mobile services. Therefore, I used Schein's (2010) organization culture theory to examine the government's IT culture and the stakeholder's perspective, which, in turn, met my goal for the study's primary theory.

Previous research surrounding 9/11 focused on terrorism, communication risks, and the government's failure to share information. The focus of prior research was on how much information should be provided to government officials and the public. According to Sheppard et al., the focus should be how organizations and institutions effectively share information, avoid threats, and securely communicate. I focused on the perspectives and perceptions of government IT analysts based on an organizational culture theory. Organizational culture theory supports the culture of a government IT analyst's work life, values, system processes, and sustainment in support of the Mobility Directorate. This theory supports three levels of culture: artifacts, beliefs, and assumptions.

According to Schein (2010), first, artifacts are the structures and processes of the organization. Second, beliefs and values support the associated aspirations, policies, and goals. Third, the underlying assumptions are based on perceptions and feelings of an individual or group. The three levels of culture are analyzed at different degrees and rules for communication and organization. I focused on the sustainment of a process to provision mobile devices. There is no one way to resolve or combat events such as the terrorist' attacks of 9/11. Organizational culture theory supported a change in approach by defining the underlying phenomena of how things work. The theory provides communication managers with a framework to address problems of knowledge sharing within the current Mobility provisioning process. Through this study, my purpose was to understand the IT culture of provisioning devices for internal and external mobile users. The federal government must find effective ways to securely communicate and share

knowledge with support agencies and MP in order to protect the public and the Warfighter.

Chapter 2 presents an in-depth literature review that includes the: (a) research strategy; (b) conceptual framework; (c) Mobility's onboarding process; (d) knowledge sharing; (e) federal agencies' policies; (f) IT information sharing struggles; (g) IT processing and provisioning struggles; and (h) research methods.

The Research Strategy

I obtained articles for this review from the following databases: Google Scholar, Walden University Library databases and peer-reviewed articles generally listed under Military, Information Systems and Technology, and Policy and Business Databases. I obtained articles from other reference sources, including C4ISRNET.com, DISA (DISA.mil), FCW.com, AFCEA.org, strategy-business.com, and the washingtonpost.com. I researched by reviewing a specific support agency under the DMUS' concepts and objectives. The DoD support agency's objectives, as directed by DoD CIO, was to create an implementation plan to support Controlled Unclassified Information (CUI) Mobility requirements by leveraging commercial carrier infrastructure.

As capabilities increase, security policies for mobile devices must grow to meet the needs of the users. The Mobility provisioning process must expand and be transparent to support the user's requirements and needs. The concepts and objectives included the creation of a mission statement, function statement, and an objective statement based on current conditions. I examined whether new policies may need to adapt to specific

standards that are dynamic and ongoing, depending on the user's environment and protocols. I used the following databases to search for primary sources for this study: Thoreau, ProQuest Central, EBSCO, military archives, and Google Scholar. I examined the primary sources that I found, including peer-reviewed and scholarly journals and interviews with key military leaders.

I performed iterative searches using several keywords, program concepts, and phrases in Boolean fashion: *mobility, relationship, communication, customers, mobile government, risk, IT, security policy,* and *mobile device*. I retrieved 101 articles for this study. For example, the terms communication and mobile government were used to search Walden University's military and government databases. I developed the research terms, acronyms, and phrases before April of 2014, and I used them through the duration of this study. Most of the reference materials that supported the study were from 2010 through 2019. However, I also used historical information before 2010.

I identified and tracked noteworthy articles in a Microsoft Excel spreadsheet then imported into QSR International NVivo v.12 and used the NVivo tool to collect, organize, and analyze my research data. Initially, I reviewed 10 articles but only used five for core research. I identified 51 additional articles for a total of 93 articles; 40 of these articles support core research. Because the government's strategy to add additional mobile devices to MP is relatively new, articles specific to provisioning mobile devices to field/end users were limited. After identifying reasons why there was a need to share knowledge securely, the additional articles presented new trends in technology, identified

policy gaps in provisioning mobile devices, and examined the culture of IT helpdesk analysts and their need to adapt to changes or remain the same.

In the age of social media and information sharing, the goal is to instantly share information and provide feedback to the right person anywhere, at any time. As global marketplaces expand to serve more people and governments increase their cybersecurity, the goal is not only to share information and collaborate but also to protect citizens. After the terrorist attacks of 9/11, the U.S. government, and governments around the world grappled with how to collect, analyze, and distribute intelligence to protect their homeland against terrorists' attacks (Randol, 2010). Homeland security became the number one priority after 9/11. According to Heighington (2011), "Crises are unpredictable events that demand adaptation and flexibility" (p. 1). The U.S. government had to figure out the best strategy for the country and its citizens at the local, state, and federal levels. The new strategy would encompass all stakeholders, for example, combatant commands, services, agencies, and MP, to develop new ways to share and distribute information securely to protect the Warfighters and the entire nation. The new strategy involved many agencies with their knowledge and ability to communicate securely across the board.

After the events of 9/11, government officials determined that preparation and response to potential threats to the United States must be clearly addressed. In short, the government must change its cultural environment to interoperable communications. The DHS was created in 2002 in response to the attacks of 9/11. Mabee (2007) stated,

> The creation of DHS involved an enormous reorganization of government bureaucracy: consolidating 22 government agencies involving an enormous reorganization of government bureaucracy: consolidating 22 government agencies involving 180,000 employees, for the purpose of, as President George W. Bush stated, ensuring that our efforts to defend this country are comprehensive and united. (p. 386)

The reorganization and realignment of government agencies continued after 9/11. DHS's primary mission is to protect and defend the United States; thus, the institution must realign the focus and goal of several agencies into one. I identified three key challenges to supporting the goals of DHS by the Government Accountability Office (GAO), which, according to Jenkins (2006) are fundamental to support interoperable communications:

> (1) clearly identifying and defining the problem; (2) establishing national interoperability performance goals and standards that balance nationwide standards with the flexibility to address differences in state, regional, and local needs and conditions; and (3) defining the roles of federal, state, and local governments and other entities in addressing interoperable needs. (p. 321)

GAO identified the challenges of interoperable communication by identifying the problem, establishing the goals, and defining the role of government. Although DHS goals are varied, the main objective is to keep the United States safe by securing the borders and airports and protecting the country's information systems network with emergency response and recovery (Randol, 2010). DHS and other federal agencies now focus on not only how to protect against terrorist threats but how to collect, communicate,

and disseminate information to leadership, agencies, and the Warfighter. According to Randol (2010), before 9/11, there was a division between domestic and foreign intelligence security threats. Per Randol, after the establishment of HSINT, threats are viewed as national security threats, regardless as to whether the information is gathered inside or outside the country. As noted by Randol, "HSINT includes human intelligence collected by federal border security personnel or state and local law enforcement officials, as well as (SIGINT [signal intelligence]) collected by the NSA" (p. 284). All efforts to gather and analyze security threats are considered pertinent to securing the United States. Based on research, effective crisis communication requires the transmission of concise information, timely responses, and open communication to and from credible sources (Heighington, 2011). I found that the collaborative approach to secure the United States supports knowledge sharing.

I identified and studied communication among CAMs and external stakeholders, specifically IT analysts and Mobility users who supported and utilized DoD Mobility concepts and programs. Many federal agencies partnered with the NSA to enable commercial mobile technology support solutions. However, the process to securely share knowledge through provisioning mobile devices to internal and external users can be problematic if the process is still under development. Therefore, my literature review presents deficiencies in knowledge sharing in two distinct areas: infrastructure and IT culture. First, the lack of knowledge sharing and infrastructure plans that support a dynamic, online customer base; and second, the lack of a cohesive IT culture-base designated to Mobility's onboarding process and customer support.

Mobile device management (MDM) will ensure secure and cost-efficient devices by providing configurations, establishing permissions, and enforcing policy for the end user. Commercial service providers such as Sprint, AT&T, T-Mobile, and Verizon, must be on a government contract purchased through a blanket purchase agreement (BPA) to utilize the DMUC. In other words, mobile devices must be government furnished equipment (GFE) and purchased through a government contracting office or BPA. Security policies for standard information systems were defined. However, the functional requirements for mobile devices must adapt to various sensory capabilities, for example, visual, audio, motion, location, and signals.

Conceptual Framework: Organizational Culture Theory

According to Schein (2010), organizational culture theory examines culture at three levels: visible artifacts, espoused beliefs and values, and basic underlying assumptions. As a researcher, I analyzed the culture of sharing knowledge in Mobility's provisioning process. It is crucial for government officials to understand and embrace new technologies that combat terrorism now and in the future. According to Schein, how individuals or groups conceptualize their external environments, explore assumptions of shared experiences over time, and communicate to share relevant information helps reduce organizational "stovepipes" or "silos."

External environment plays a significant role in how an organization will react internally to bureaucratic pressures. Due to inflexible cultures, some government agencies were slow to respond to advancements in mobile technology and cyber threats (Aldrich, 2008). Therefore, some bureaucratic models assume the organizational goals

are wholly laid out versus vaguely defined and in need of group consensus (Aldrich, 2008). A cultural group must be informed and actively participate in strategic improvements to maintain or improve an organization' goals or mission. According to Aldrich, an organizational strategy may be considered open or confined, but group participation is crucial to overcome challenges or improve system processes for success.

Schein's (2010) organizational culture theory has been used to identify organizational risks and challenges, explore interrelationships, and describe critical elements that support the mission. According to Schein, culture is prevalent in all facets: mission and goals, surroundings, and internal process and procedures. Ashkanasy, Wilderom, and Peterson (2011) acknowledged that errors happen in organizations, but how they manage mistakes to positively affect cultural change is what makes the results positive or negative Leaders influence culture change, but leaders must realize and understand the processes of organizational change before managed culture is pertinent (Schein, 2010). A shared assumption by a group over time sustains organizational culture and motivates change. According to Schein, various stages support change:

- Unfreezing – creating motivation to change by identifying the problems, goals not being met, and future consequences
- Learning new concepts, new meanings for old concepts, and new standards for judgment – by restructuring and learning a new skill set and evaluation method
- Internalizing new concepts, meaning, and standards – by fixing the problems and defining a new way to achieve positive results. (p. 300)

Stakeholders who support the provisioning process attempt to identify the problems, assess the policy and processes, and communicate to MP future goals for efficiency. If the new way of doing things is better and achieves positive results, change is inevitable. Ashkanasy et al. (2011) noted that to promote stability, organizations must better define their strategies and processes to promote error management prevention instead of focusing on the error itself. If an organization does not adapt, learn, and communicate; it runs the risk of isolation and the eventual elimination.

Risk Communication Philosophy

Risk communication philosophy encompasses three phases: preparedness, response, and recovery (Sheppard et al., 2012). The word risk identifies a threat or an area of weakness that could be avoided. One way to avoid an imminent threat or warning is through communication. Therefore, risk communication philosophy supports numerous emergency managers, communicators, and leaders in information systems who protect and defend the United States public against terrorism. According to Sheppard et al., after a threat launches, each phase provides a process for how leaders can communicate and recover from a terrorist attack.

Although a consortium of researchers, devoted to improving human causes and the consequences of terrorism, developed risk communication, the theory does not highlight the perspectives of those in government IT who support and secure the networks. START is a DHS Center of Excellence, University of Maryland, research and education center. START uses state of the art theories that provides homeland security policymakers and practitioners with data on human causes and consequences of terrorism

to ensure security policies and operations reflect an understanding of human behavior (Sheppard et al., 2012). To review or revise policy, the perspectives of those who work to secure the systems must be considered. For this study, I used risk communication as a research reference point for human behavior when there is a threat to IT systems, and communication is needed.

Organizational culture was the primary theory used to support the government IT culture, process, and policy. After identifying one of the policies and laws (PL 107-347) created after (9/11), communication was vital to the government's recovery. This policy supports a federal agency's ability to provide IS based on each agency's risk assessments. According to Souppaya and Scarfone (2013), mobile devices (due to their open use) should be secured from an assortment of threat possibilities as recommended by NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (p. vi). Explicitly, risk communication and organizational culture theories support a collaborative environment for future changes. In other words, the changes that need to occur now, and in the future, will need to support the Mobility program's provisioning process, cybersecurity, and communication efforts.

Mobility's Onboarding Process

The onboarding process for a mobile device has four main sections: preparation, ordering, end user registration, and device provisioning. First, preparation for MPs means that the MP will start the process by going to a designated onboarding website to procure a mobile device, choose a carrier service plan, and smart card reader, if necessary. Also, MPs or new users will complete the EMMC training, complete and submit 2875 access

forms, and submit a training certificate for access to the Mobility console. Second, ordering means creating a telecommunication request through a Direct Store Front website. MPs submit a user list to the Mobility CAM, which contains email addresses, job order numbers, and personal identification numbers (PINs). Third, end user registration is submitted for final approval of configuration and then uploaded as a user (DMUC Implementation and Sustainment Process, 2015). Lastly, if security approves the 2875s and the configurations are successful, the end user license agreement is signed per device.

Mission and Goals of Mobility

The onboarding process was created to support the provisioning of mobile devices and overall sustainment. According to a DoD combat support agency (2015), their goals are to support the Warfighter with systems engineering, infrastructure, and a device and android applications (APPS) framework. According to DISA (2016), their mission is to

> deliver wireless DoD Information Infrastructure and services to operate secure mobile enterprise services to DoD. Institute mobile devices policies and standards for use across DoD. Promote standard development and use of mobile and web applications across DoD (para. 1).

These goals support DoD policy standards and DISA's onboarding process. If there are no significant issues or hold-ups, the onboarding process should take no more than a week. However, many federal agencies rely on the General Services Administration (GSA) contract vehicles for mobile device solutions. Each government agency or organization is responsible for a general policy that will support the services and

capabilities to secure the management of mobile devices. Government organizations deploying mobile devices must choose the general policy restriction for mobile device security.

National Institute of Standards and Technology General Policy Guidelines

NIST provides guidelines for managing the security of mobile devices. According to NIST (2014), the Federal IS Management Act (FISMA), Public Law (P.L.) 107-347, requires each federal agency to develop an agency-wide program to provide IS, support operations, and policies and procedures based on risk assessments (para. 1). An effective IS program must support agency-wide enterprise systems. According to Keblawi and Sullivan (2007), NIST issued new information system security (ISS) standards in 2006 to regulate security controls for all federal agencies' information systems. The current provisioning process utilizes commercial off the shelf (COTS) products. COTS products must comply with the new standards. However, every agency has a unique mission and goal in support of the public or Warfighter. According to Keblawi and Sullivan, Kerr, Chief Learning Officer, General Electric Company made a point that, without adequate funding, the new standards could be ineffective and harm organizations as well as personnel. The current environment is one of uncertainty for federal managers faced with the challenges of estimating what is needed and then implementing practical standards.

Public Law 107-347 supports a wide range of IS programs, but it does not explicitly outline knowledge sharing plans to support site infrastructure, onboarding or collaboration protocols for government IT analysts, engineers, and customers in provisioning mobile devices. Because of the nature of the business of IS, there is the

possibility of a communication risk in sharing information that is deemed classified. I only used unclassified information for my research. Therefore, open communication is essential. The support models for my research will encompass one theory: organizational culture. NIST SP 800-53 provides a more holistic and tailored approach to IS and privacy controls for agencies. SP 800-53, revision 4, represents the latest updates to IS systems to combat ongoing cyber attacks to federal agencies. According to NIST (2014), SP 800-53 addresses specific security control needs to support the mission and preserves a level of flexibility for technology upgrades and innovations for government organizations. Knowledge must be shared with all government stakeholders and MPs to achieve success.

Security and privacy controls are emphasized not only in NIST SPs but also in guidelines resulting from legislation, Executive Orders, policies, directives, and regulations that support the specific needs of an organization. Organizations and agencies must adhere to the protocols and procedures needed to secure IT data and systems. To accomplish this level of security and privacy, to share information and to collaborate with those who support IT and the global community is critical.

Knowledge Sharing

Knowledge sharing and collaboration supports community intelligence. IT agencies must utilize all avenues of communication that is at their disposal, which includes Internet-enabled devices, social media, and wireless devices such as mobile phones. Social and community intelligence (SCI) is new to the stage of research and IS, but their influence could change the landscape for technology requirements. Zhang,

Wang, Guo, and Yu (2012) forged ahead with a new system framework that supports further research in human behaviors and community life, but still more tools and applications must be developed to bridge the gap in technology.

Although mobile devices are being utilized by government MPs in various capacities, articles are still limited in scope that support new policies for military and government officials beyond making sure the devices are secure. Therefore, I sought to understand the culture of the government IT analysts and engineers who provide support to customers who utilize a Defense Agency's Direct Storefront online website to process and purchase mobile devices. With innovations but constrained resources, the quest is to use mobile devices to share knowledge, securely collaborate, and distribute information and applications at a lower cost with minimal impact to network performance, serves the market and stakeholders alike.

The marketplace continues to evolve with new technologies, but questions remain to address how federal agencies stay connected, share information securely, and support the Warfighter and public. These questions help highlight the gaps in the provisioning process for government agencies and organizations that support the literature review. The literature is organized to support three additional sections: (a) how federal agencies utilize current policies to connect and collaborate with new mobile devices, (b) how government IT culture struggles to share information with customers, and (c) how government IT customer support teams struggle to process and provision secure mobile devices to customers. It is vital to eliminate accidental spillage (information leaks) and to prevent unauthorized users from potentially corrupting network systems or transferring

sensitive information to foreign adversaries. Part of the ordering components used in provisioning devices includes a private sector consisting of a carrier service plan through government contracting. This study examined the connection and collaboration between government personnel and non-government entities' ability to provide secure mobile service through the provisioning process.

Federal Agencies Utilize Current Policies to Connect Mobile Devices

In keeping with trends, mobile devices, specifically, smartphones, will continue to expand in the marketplace to be used by business professionals and the public. Three are roughly 400 million smartphone users worldwide and still growing (Lee & Shin, 2014). DoD and other government entities are also utilizing smartphones and mobile devices with one additional caveat: security. Government agencies are trying to determine the best way to provide information via smartphones while also securing enterprise networks access. According to Brown (2012), NIST is looking to update current guidelines for mobile devices. By using software technology to consolidate management at the organizational level, the new NIST guidelines offer recommendations to better secure mobile devices and to protect access to the organization's computer network (Brown, 2012). The new guidelines will act as a supplement SP 800-53 (security controls federal information systems and organizations). Although the revised guidelines offer a way to strengthen security for mobile devices, laptops are not included because the security controls and operating systems are different.

The E-Government Act (Public Law 107-347) title III, of FISMA, states that each federal agency develops and implements a security program that uniquely addresses their

IS needs (NIST, 2014). Securing mobile terminals against leaks, attacks, and threats by hackers is vital to national security. All attack points of entry, for example, servers, android applications (APPS), malicious codes, and network terminals for mobile devices, must be examined. Patten and Harris (2013) estimated that in the year 2012, roughly 18 million users would be faced with malware issues. According to Lookout (as cited by Patten and Harris), based on the popularity of two types of smartphones (Android and Apple iOS), there was a surge in malware risks for Androids versus iOS. Overall, the Android platform is open source (the programming code is open to the public), while Apple's iOS platform is closed and entirely controlled by Apple. Android's open platform is less secure than Apple's iOS (Patten & Harris, 2013). However, if any entry point fails, the chain reaction could be catastrophic to government and business systems alike. The federal government (not private industry) is responsible for ensuring all defense networks are secure. That responsibility includes maintaining a Non-classified Internet Protocol (IP) Router Network (NIPRNET) and the Secret IP Router Network (SIPRNET).

A new policy whereby employees can use their personal mobile devices for, example, Armando, Costa, Merlo, and Verderame (2015) proposed smartphones and tablets, to access their organizations' proprietary network environments. This new policy is called BYOD. There is a security risk involved when allowing any device, personal or otherwise, to connect an organization's network infrastructure. BYOD policies support stakeholder involvement, which is the organization's authority to define and describe an acceptable policy, and combat cyber-attacks and malicious threats from entities

worldwide. However, this is not likely to happen due to access controls and threats to the overall network system. All devices must be approved and issued by government officials to connect mobile devices to government network enterprise systems. Therefore, the devices must be GFE purchased by MPs and approved by the government.

The approved list of GFEs should provide confidentiality, integrity, and authenticity for Defense users from anywhere in the world. Hence, cyber warfare (computer programs and networks used to attack and disable information services) includes implementing safer measures and securer networks to protect the communication environment for mobile users. The goal is to conduct business anytime and anyplace, now and in the future. This effort supports DoD's ability to not only secure the location of a Warfighter, but also, with secure mobile communication; it helps to protect the United States public from future terrorist attacks.

The popularity of mobile devices has provided a new method for sharing information worldwide. With the need for greater communication, comes a higher likelihood for thefts and security leaks. Organizations and governments alike are utilizing wireless technology not only to conduct business and provide vital information but also to ensure a secure infrastructure is in place. After the events of 9/11, communication and collaboration were found to be deficient across specific government agencies per the *9/11 Commission Report* (National Commission on Terrorist Attacks Upon the United States, 2004). Therefore, the focus to share knowledge securely and to help combat terrorist attacks was at the forefront of discussions. Many approaches were proposed to share knowledge with the use of mobile devices. Yoo, Park, and Kim (2012) proposed a

common authentication approach related to verification access process that encompasses asymmetric cryptographic key (a secret key not stored in any way), a user-known password and the service provider's secret key. Yoo et al. were developing the technology to better secure file transmission through mobile devices. Based on a secure file system and set protocols, Yoo et al. proposed how the service provider server and the mobile device would communicate. Although Yoo et al. discussed the proposed system relationship between the server and the mobile device, they did not mention the relationship between IT service providers and device users (customers).

The question of authentication has become more relevant because DoD CIO Halvorsen announced that he wants to phase out the Common Access Card (CAC) over a period of two years (Miller, 2016). Most DoD users access their network systems with CACs. Currently, there are more than 4.5 million CAC users (Miller, 2016). Due to the challenges of using a CAC with wireless technology and mobile devices, the current system needs to be changed or updated for security purposes. CACs – are typically used to authenticate unclassified emails, but the cards can be lost or misplaced. Biometric-based authentication is a new method used to identify the physical characteristics of an individual to verify, access, and secure sensitive information (Jain et al., 2006). The challenge with wireless technology is to securely share confidential information with government IT customers and DoD personnel by using the best technology available.

Government IT Culture Struggles to Share Information with Mission Partners

Next generation mobile computing will need to incorporate new designs and innovative approaches to support customers. As stated by Levendovsky et al. (2014), the

demand for collaboration anyplace anytime supports mobile cloud computing and all the challenges to manage system applications securely. Distributed Real-time Managed Systems (DREMS) supports two areas: (a) a design-time tool for analyzing applications, and (b) a runtime software platform for software application deployments. DREMS approach encompasses a rapid application deployment and reuse (Levendovsky et al., 2014). DREMS component/architecture provides actor-to-actor secure communication which supports a Multilevel Security (MLS) policy in the U.S. domain. The MLS policy rules are defined by each government organization based on security categories or classifications. For example, for unclassified systems, the hierarchy is confidential, secret, top secret. Therefore, information can flow up depending on the category level (confidential to top secret), but not down (top secret to confidential).

Organizational culture affects the outcome of e-government's future initiatives and whether the analysis is based on the public or private sector. According to Welch and Feeney (2014), the interplay or interface of social media, organizational assets, and new technologies play an essential role in effective communication and adopting new technologies. The culture of the organization is a significant factor as to how rules and policies are shaped and adopted. According to Welch and Feeney, "organizational culture will be shaped by not only the organization's mission, its members but also the external influences that exert pressure on the organization – in the case of local governments, the public and external governing bodies" (p. 508). Whether public or private, federal or local government, social and technological changes affect how organizations create and sustain policies and processes. According to Sheppard et al. (2012), managers must

realize that there is no one-way or single conceptual framework to be a great communicator. Managers must be aware of the critical factors that affect risk communication and organizational environment. Sheppard et al. identified five crucial factors that support the risk communication philosophy:

- Public perceptions: Know your audience and know their specific environment whether the variables are age, racial, social, or cultural differences.
- Spokesperson/spokespeople: Use a person to deliver a message with whom the public feels is trustworthy and represents their interest and values.
- Message content: Provide an action plan or process for behavior and feedback that make sense to the public. Acknowledge the need for change to include a new process or new information.
- Unique risk characteristics: Understand how to prepare, respond, and recover in order to communicate effectively to different events that may occur.
- Communication channels: Find the best venue, site, or social media format to communicate with the target audience. Focus on the needs of the public. (pp. 2-3)

Computer technology and information networking have evolved and become more innovative; thus, creating an environment where individuals can obtain information through the Internet. Mobile devices allow for convenience and feedback, which allows for information sharing. The next phase for DoD is not only about the practicalities of new technology, but also about being relevant in the modern age of security and cyberspace.

For DoD agencies that provision mobile devices, the agencies not only support the business process, they also establish an internal Mobility policy. To fully support knowledge sharing for an enterprise mobile device, a policy must be established and adopted. Mobility policies are designed to support mobile device customers. The current regulations and policies fall under the Commercial Mobile Device (CMD) Implementation Plan. The CMD Implementation Plan promotes the development and use of mobile devices and applications for DoD. Specifically, this plan supports a combat support agency's ability to provide information sharing to the Warfighter and stakeholders. Therefore, a combat support agency is partnering with the NSA to enable commercial devices in support of data requirements. In addition, this partnership will work to secure DoD DMUC as directed by the CIO CMD Implementation Plan.

The objective is to purchase devices through the DMUC Infrastructure Service – SharePoint site. However, the SharePoint site for DMUC Storefront purchases and provisions is still in the development stage. Although the website is up, specific parts of the infrastructure are under construction. For example, the process to onboard and provision 'multiple' mobile devices is still under development. According to one of the site portfolio managers, the long-term goal is to process multiple orders in an hour versus waiting two weeks. Al-Akkad and Zimmerman (2011) related that

> carrying smartphones people can collect data in ways being previously not possible. This approach is called mobile sensing. … Further, mobile sensing can provide coverage in areas where it is hard to deploy and maintain static sensors due to natural conditions or industrial constraints. (p. 2)

In this time, where terrorist's activities have increased globally, cell phones could prove to be very useful for federal agencies, specifically DoD.

Government IT Support Struggles to Process and Provision Devices

Mobility continues to be a transitional process for government agencies. Mobile technology moves forward to evolve and expand; while some steps are planned, others are not. According to Elzen, Geels, and Green (2004), various actions, such as war, crisis, or significant events, can accelerate transitional processes. Per Elzen et al., to manage the transition to sustainable mobility, there are four phases:

- Predevelopment phase is experimentation, testing, and investigation;
- Take-off phase is when change begins, and a process is underway;
- The breakthrough phase is directly linked to institutional, and structural changes are accelerated into defined processes;
- The stabilization phase is where environmental and societal changes have been reduced, and efforts have reached a balance. The stabilization phase re-enforces the idea of an evolving change that reaches a point of steadiness.

SharePoint Storefront

The SharePoint Storefront site is a secure and stable centralized point of entry for new users to request a secure mobile device. The webpage (DoD Mobility User Corner) is hosted by DISA for internal and external users to support the DoD Mobility Program Office. The Storefront site is just one method for sharing knowledge via a website. There are many network systems used to share knowledge. Hardware and software applications and arrangements are used to protect vital information for federal agencies. To create a

culture of security awareness and understanding, all employees must be aware of the IS programs and policies. According to Paulsen and Coulson (2011), business intelligence (BI) systems support organizational security operations by monitoring systems activities, setting goals for users, and providing accountability system operations.

Business Intelligence Systems

BI systems are not relegated to support IT only, but rather to view IS management from an all-encompassing, large-scale perspective. Therefore, IS encompasses the customers, stakeholders, analysts, leadership, and technology. The next generation of BI systems has expanded to mobile devices in the quest to support the information gap to connect customers anytime, anyplace, at any time. Verkooij and Spruit (2013) revealed the need to develop value creation, application deployment, IS, workforce mobilization, information delivery, and device management through a framework called Mobile BI implementation (MOBII; p. 23). Ultimately, the goal is to enable mobile users to have access to information through applications designed for mobile devices.

Customer and Service Relationship

Future communication and collaboration require more than a connection to a landline or an internal network; rather, they require access to a virtual or cloud environment for a new frontier for aerospace engineering and wireless technology. According to Noor (2011), the challenge is to merge communication, virtual, robotics networks, and smart mobile devices into collaborative learning environments now and for the next generation. The current environment for government IT analysts, engineers, and mobile device customers is a noncontractual business relationship via a website called

Storefront. Currently, the government' customer support team and mobile customers collaborate to provision the right cell phone. However, the relationship between the customer/stakeholder and government IT analysts and engineers does not support or emphasize a seamless transition from cell phone purchase to delivery. According to Polo and Sese (2013), there is an increase in awareness to support and develop a better relationship between the contractual side for the customer and the analysts' side for service. Typically, the customer and service relationship is considered a low priority in comparison to potential security and privacy risks associated with mobile devices.

In the event, there is a breach of security; government officials want to make sure their internal networks and data are secure. Although Ohme (2014) addressed privacy and security issues separately, he acknowledged that one of the most significant obstacles to the adoption of a government Mobility program were issues of privacy and security risks. Specifically, personal information potentially lost to hackers, compromised by personnel, staff members, or unauthorized third parties were the biggest threats to mobile device use. Ohme defined privacy risks as a loss of power over personal information to another party without the owner's consent or knowledge. Security risks were identified as an attack by outside entities to the network to hack or steal data. Current government Mobility policies, which include privacy and security issues, are a significant part of the overall support when provisioning mobile devices to customers. However, the culture of government IT analysts and engineers who support the provisioning process is equally important but not always at the forefront of discussions. Instead, a website called Storefront is the first stop for customers who need to register mobile devices for field use.

Research Methods Used in Literature

The studies conducted on the perception of stakeholders, government IT analysts, engineers, and MPs, who support Mobility's provisioning process, included quantitative methods and qualitative methods. There were multiple approaches to consider when examining the experiences of government IT in Mobility's provisioning process. Based on the experience of those who are internal or external to the phenomenon, the method of reflection supports several event phases (Moustakas, 1994). There is a relationship between internal and external perceptions of an organization or group. According to Creswell (2009), qualitative research explores the phenomenon experienced by a group of individuals who can articulate their lived experiences. In the research literature examined, quantitative studies utilizing survey questionnaires were a general method. Based on research, there was little new information specific to the subject of my research paper. One study collected preliminary quantitative data to support a user study of mobile applications involving civilians with smartphones during emergencies (Al-Akkad & Zimmermann, 2011). Other research articles did not mention quantitative methods in support of a Mobility provisioning process. I used a qualitative method with a phenomenological approach to interviewing IT stakeholders who are hands-on and can provide sound feedback on Mobility's provisioning process.

There are five qualitative approaches: Narrative, ethnography, grounded theory, case study, and phenomenology. The narrative focuses on individual stories versus a group of individuals. Ethnography observes the culture of group sharing over time rather than to discern a new study. The grounded theory looks to find an explanation to develop

a theory instead of describing an event. The case study explores a unique, real-life case(s) collecting data from various sources but focused solely on the case. Phenomenology studies an event experienced by a group of individuals as lived, to understand the phenomena of the human experience (Moustakas, 1994). The phenomenological approach was the most logical choice and supported the research participant's perspective, while the other four approaches did not. Wertz et al. (2011) explained that "good phenomenological knowledge has a genuineness and fidelity to life that I do not find in any other approach" (p. 135), and I agree with their claim.

I chose a phenomenological approach for my research to support the exploration of the provisioning process and perspectives from IT analysts to understand better the social phenomena of knowledge sharing within the government IT culture. Suorsa and Huotari (2014) explored "the effect of interaction in research on knowledge creation and its dependence on the conceptualization of a human being" (p. 1042). The researchers explored three areas: an interactive event, construction of the human experience in interaction, and modes of being in interaction using a conceptual framework. This framework supports a hermeneutic phenomenology, which highlighted the knowledge, interpersonal relationships, community processes, ideas, and past experiences.

Knowledge-based Organization's Approach and Methods

According to Suorsa and Huotari (2014), knowledge creation supports innovation, creativity, and it is essential to knowledge-based organizations' approach to handling traumatic events and competition. Additionally, the phenomenon of knowledge creation as a process is used to examine an organization's internal and external information tools

and employee experiences. Phenomenology provides the best approach to exploring the concepts of events and human interaction by reviewing the events based on the organizations' culture, processes, and policies. According to Smith (2013), "phenomenology is the study of consciousness as experienced from the first-person point of view" (para. 1). It describes the way human beings experience life and the events that build and sustain life experiences. In the reviewed literature, qualitative methods were used to analyze interviews from stakeholders who were most familiar with the provisioning process and the challenges of sharing internal and external information. These challenges affect Mobility's government IT culture, policies, and processes now and in the future.

Qualitative research methodologies consist of observations collected from participants in groups or small sample sizes. Therefore, a qualitative approach captures the time and place of an event and describes the lived experiences of an individual or group (Patton, 2002). Qualitative research methods support open-ended interviewing that provides a more in-depth study of an individual, organization, culture, and other groups. Russell (2013) noted that qualitative research supports in-person interviews using open-ended questions, which target a specific population. Mobile devices provide convenience and flexibility. I analyzed the impact of Mobility' provisioning process, policy gaps, and the challenges government IT face to share information in the current culture.

The mobile phone is used for many things. Mainly, it has allowed people to stay connected from anyplace at any time. Although having a cell phone is mostly an individual choice, companies and government agencies are re-examining the need for

mobile devices on travel, in the field, and at work. Individuals can connect to systems, applications, and networks away from the office and great distances (Cowley, 2010; Watson and Lightfoot, 2003). Because mobile phones offer a wide variety of communication features, they have the potential to change the social dynamic of individuals and security measures for government operations. Therefore, I explored the infrastructure and provisioning process for government staff, government IT analysts and engineers supporting external customers' ability to obtain an approved mobile device for use in the field or onsite by government personnel or agency. My study focused on the learned experiences of the customer support team and MPs who are part of the IT culture.

Due to the growth of wireless technology in both the public and private sectors, another study slightly similar to my topic provided information about how government agencies could utilize wireless technology for e-government applications. According to Chang and Kannan (2002), the Department of Interior, Army Corp of Engineers, DISA, and the United States Postal Service are looking to share information and improve efficiencies at all levels of government. Chang and Kannan examined the role of wireless technology contributions to e-government applications. The study identified four goals: understanding the distinctive characteristics of the mobile environment, linking the characteristics to specific applications, defining the wireless technology role, and evaluating the readiness of the government workforce to employ and use wireless technology.

Additionally, Chang and Kannan's (2002) study contained a survey that collected federal employees' responses as they related to their attitudes and perspectives regarding

the use of wireless technology. Based on the four initial goals, the key findings were that wireless technology provided another avenue to share information; however, security and privacy issues were still a significant concern. Due to aging and outdated technologies, governments should support the wireless rollout. Employees appear to have a positive attitude of integrating wireless technology into their work processes; however, providing training would have a significant impact and positive appeal for employees.

Training is one of the many steps required for government IT stakeholders to support and participate in the Mobility program process and procedures. To efficaciously on-board an MP as a user in the Mobility program, the MP must first procure their own device, service plan, and card reader, if necessary. They must also take EMMC training and go through a series of steps to obtain a training certificate for Mobility console access. After the MP completes the initial enrollment phase and receives a program designator code to fund the service, a Direct Authorized Request Official (ARO) is obtained to submit orders. The MP will use the designated Storefront website to provision the device and communicate with government IT analysts, engineers, and Tier I helpdesk support to complete the ordering process.

Storefront and other sites that are similar and support DoD users will increase in the next few years due to the demand to connect and collaborate with anyone, anytime, from anyplace. DoD's Mobile Device Strategy under the CIO Executive Board is using a phased approach to support and improve mobile (unclassified and classified) capabilities. The phased approach leverages the commercial carrier's infrastructure, but a DoD

support agency creates an enterprise solution entry point. This new approach creates a new relationship within the IT culture and the customers they support.

My research provides historical guidance for other agencies to utilize as a foundation to create Mobility programs specific to their needs in support of stakeholders and end users. As technology integrates with society and is used more by the average user, defense leaders, and strategists will require greater flexibility to communicate with secure mobile devices worldwide. Mobile phones aid and serve the environment through planning and sensing platforms that support communication and collaboration. In other words, phones detect and distribute sensor information across multiple locations (Cowley, 2010). Therefore, business models and infrastructure are developed through an onboarding process called Storefront. Storefront is a website that is hosted by a defense support agency that MPs and customers utilize to order telecommunication products. To complete an order request, customers may need to interact with the government IT analysts, engineers, or CAMs for assistance with onboarding.

CAMs and IT analysts not only manage certain aspects of the Storefront site; they also provide customer service support to MPs and new customers who join the Mobility Program. Because the Storefront site is hosted by a combat support agency and is located on the Defense Enterprise Portal Service (DEPS), you must have a CAC to log-on to the site. The Mobility Program Management Office (PMO), business operations team, strategic outreach representation (SOR) tracks and coordinates how customers want to join the program. Therefore, the CAMs receive completed user lists from customers and follow-up with any adjustments needed or system delays. Although the Defense

Technical Information Center (DTIC) is considered one of the most substantial resources for information analysis, products, and services, DoD is looking at multiple ways to collaborate and share information (Schwalb, 2013). There are pockets of people, for example, customer portfolio managers, who support the process from different locations within an agency and from across the United States. Therefore, the need for cohesiveness is significant across the ranks, but there are no known plans to bring all groups together.

Conclusion

This chapter focused on a comprehensive review of common themes in the literature regarding the challenges and gaps in knowledge sharing and customer relations with government IT shareholders in Mobility. The theory of organizational culture sets up a framework to analyze and examine these themes. Organizational culture theory was used to identify and assess the organization's risks and challenges, explore stakeholder relationships, and define the provisional process and procedures. The difficulties of sharing knowledge with government IT, understanding the provisioning process, and describing common themes were based on the stakeholders' perspectives. My research included the perspectives of MPs from command controls and other federal facilities. I discussed specific policies focusing on IS. Additionally, due to an increase in cyber threats and the use of mobile devices, there is a need to update current policies.

NIST policies (SP 800-53) and (Public Law 107-347) were provided to support not only the need to secure information but to acknowledge the need for possible revisions in the future. Mobile devices (specifically cell phones) have changed the institutional role of formal meetings and official locations. The new role of behavior and

interactions are to communicate from anywhere and anytime. Therefore, according to (Geser, 2006), mobile devices may undermine, or make it more difficult to control; the previously centralized communication systems bound by walls and computer hardware/software systems.

Due to budget restraints, stakeholder timelines, cyber attacks, and process delays, the defense community cannot afford to start a Mobility program from scratch. So instead, they utilize existing ideas, concepts, and solutions by leveraging the infrastructure of commercial carriers. It is essential to see what other government organizations are doing versus duplicating efforts. However, the defense community should utilize tools like DEPS that allows for knowledge sharing and creativity. DoD encourages the IT culture to document, develop, and support internal Mobility projects that offer the latest capabilities to the larger communities. There have been long-standing cultural barriers and "stovepipe" mentalities that have prevented information sharing. However, after 9/11, the goals changed to a more open and collaborative environment with the focus being geared toward greater security to combat insider threats and terrorist attacks. Therefore, I researched the issues surrounding knowledge sharing through the Mobility program's infrastructure and provisioning process. Protecting the government's communication networks now and in the future are a vital part of sharing information and program policy support. The literature gap exists because there is no easy solution to cultural barriers or a seamless process that effectively provisions mobile devices to the customer base. The process appears to be dynamic and supported and controlled by many groups. However, many questions remain unanswered regarding the process and standard

operating procedures. Therefore, research was needed to provide clarity and understanding to support Mobility programs in the future.

Chapter 2 covered an in-depth literature review that included the: (a) research strategy; (b) conceptual framework; (c) Mobility's onboarding process; (d) knowledge sharing; (e) federal agencies' policies; (f) IT information sharing struggles; (g) IT processing and provisioning struggles; and (h) research methods. Chapter 3, the research methodology, includes the: (a) qualitative and phenomenological approaches; (b) research design; (c) research question; (d) methodology justification; (e) researcher's role; (f) specific methodology; (g) data collection procedures; (h) population and sample size; (i) participants and interviewees; (j) data analysis; (k) presentation of results; and (l) ethical considerations. Chapter 4 will detail the results, and Chapter 5 will cover the discussion, recommendations, and conclusions.

Chapter 3: Research Method

After the events of 9/11, an important goal was to extend communication and share knowledge across various agencies (Randol, 2010). If government employees (IT analysts) are to determine the best mobile device approach, they must first understand the role of the employee and their job function to determine the best mobile device (Solution Spotlight, 2013). According to Solution Spotlight, government agencies must consider the challenges, including seeking out the best operating system, determining the best security methods, and building good relationships with vendors and stakeholders. To effectively provision mobile devices for stakeholders, knowledge must be shared, policies created, and processes and procedures supported (Solution Spotlight, 2013). I designed this study to describe, identify, and analyze the gaps and challenges to government provisioning of mobile devices.

I used a qualitative methodology and a phenomenological approach to study government IT analysts and stakeholders' lived experiences to support a new process to provision mobile devices. The new process may support enhanced communication and knowledge sharing for field commands and MPs. I explored the lived and cultural experiences, engagements, and communication through observations and interviewees between the CAMs and online users/MPs who utilize the Storefront website. The Storefront website is designed to act as a central hub in support of the MDM process for provisioning mobile devices. Specifically, according to Randol (2010), the focus of government Mobility's leadership is the provisioning of cell phones to share knowledge with internal and external stakeholders now and in the future.

After the events of 9/11, government officials re-examined the appropriate methods of communication to use in response to terrorist attacks (Randol, 2010). However, there remains a gap in knowledge on this topic because, as reported by Solution Spotlight (2013), mobility devices are relatively new to government field users and commands. The provisioning and security measures are in the early stages of development for a "four-letter" agency under DoD. The agency's Mobility Directorate promotes support, collaboration, and information sharing with MPs via provisioned mobile devices through an online direct storefront website (DMUC Implementation and Sustainment Process, 2015). The effort to provision mobile phones must be a seamless and secure process that supports commercial frameworks and the agency's network system environment. The goal is to effectively share knowledge via mobile phones with MPs, stakeholders, and field users with very limited callbacks or service issues. According to the DMUC Implementation and Sustainment Process (2015), the responsibility of having a seamless provisioning process falls to leadership, CAMs, MPs, and stakeholders.

Chapter 3, the research methodology, includes the: (a) qualitative and phenomenological approaches; (b) research design; (c) research question; (d) methodology justification; (e) researcher's role; (f) specific methodology; (g) data collection procedures; (h) population and sample size; (i) participants and interviewees; (j) data analysis; (k) presentation of results; and (l) ethical considerations.

Qualitative and Phenomenological Approaches

According to Al-Akkad and Zimmermann (2011), individuals claiming to be part of civil society must be willing to take responsibility and support crisis management by supporting the appropriate information and communication technology, now and in the future. I utilized a qualitative, phenomenological approach to conduct an empirical study of the lived experiences of the customer support team that supports new technologies and the provisioning process of mobile devices. Al-Akkad and Zimmermann explained that, for state emergency employees, such as police officers, firefighters, and medical staff, there are emergency guidelines and procedures to follow. However, federal agencies, that support IT and security are still in the development stages for creating policy standards for sharing information using mobile devices.

The design of this qualitative research supports the ability to explore and identify why seamless communications and knowledge sharing is essential when it comes to provisioning mobile devices. According to the DoD CMD Implementation Plan (2015), because cell phones are convenient, reasonably priced, and universal communication devices, DoD agencies are at the cutting edge of employing commercial cell phones for MPs and stakeholders in the field. The devices can be used for many things and carried almost anywhere the user goes. Therefore, programs and policies are at the core of sharing information and protecting government telecommunications networks.

I used a phenomenological framework to study and examine the lived experiences and perspectives of the customer support team as they relate to provisioning mobile devices to field users. I used the framework for interviews, observations, and personal

interpretations of those who are involved with the provisioning process. According to Patton (2002), transcendental, existential, and hermeneutic phenomenology provides individual experience, group reality, and the management or structure of communication.

The provisioning process adheres to the U.S. Department of Commerce, NIST (2013) Public Law (P.L. 107-347) by the NSA National Security Directive 42 (1990). While NIST provides guidelines for managing the security of mobile devices, Directive 42 established objectives, policies, and guides in the early 1990s to secure national security systems. This Directive included information assurance while supporting collaboration and cooperation among various technical organizations and government agencies that defend against national security threats (National Security Directive 42, 1990). Directive 42, as well as the Federal Bureau of Investigations' (2010–2015) IT strategic plan, identified future goals and objectives that will support collective IT enterprises' implementing, supporting, and securing new IT capabilities across multiple geographical areas. Information "silos" of the past will be transformed into collaborative, virtual, and mobile information enterprises in the near future.

There is a concerted effort to keep information systems and networks secure and free of the risk of being compromised by foreign intelligence (DoD Commercial Mobile Device Implementation Plan, 2015); DoD requires a method of communication that is handy and versatile for its workforce. According to the Memorandum for Secretaries of the Military Departments (DoD Mobile Device Strategy, v 2., 2012), DoD CIO Takai stated

> Its mission requires the provision of forces over air, land, and sea, across foreign borders, and into adverse conditions… The mobile workforce's ability to access information and computing power can improve information sharing, communication, and action response time for greater mission effectiveness (p. 1).

I used the literature review and research question to support this study. Additionally, I utilized multiple interviewing techniques to support this study. I used the qualitative phenomenological approach to address the main research question. Through the research and subsequent interview questions, I gained insight into the lived experiences of stakeholders.

Research Design

I explored the Mobility process using a qualitative phenomenology approach, from the perspective of government IT analysts and engineers, based on the events they encountered in provisioning cell phones. According to Patton (2002), phenomenological analysis is used to investigate and understand the meaning of a structure or process from the lived experience of an individual or group. Therefore, I used the best approach to explore a government IT provisioning process, policy, and culture from the viewpoint of those who support mobility development and expansion. Phenomenology provides the best approach for exploring events and human interaction by examining individual perspectives through one-on-one interviews.

I sought to understand the provisioning process mainly from the perspective of the internal stakeholders, government IT analysts, engineers, managers, and leadership, but from perspectives of external stakeholders. The assumed gaps that internal and external

stakeholders come across limit efficiency and knowledge sharing. The internal stakeholders are on the frontline with developing a direct Storefront website for ordering devices and supporting customers through the onboarding and provisioning process. The external stakeholders and MP users utilize mobile devices in the field to support Warfighters.

I used semistructured interviews for a level of flexibility to understand past process issues and ongoing provisioning challenges. Open dialogue is needed to give interviewees a level of confidence that all information is valuable, demonstrable, confidential, and unclassified (Patton, 2002). I used the phenomenological approach to explore the provisioning process and lived experiences of stakeholders. Additionally, the phenomenological approach addressed the primary research question for this study.

Research Question

The primary research question was: What are the lived experiences for end-users in the government IT culture using the Mobility provisioning process for the sharing of information?

Justification for Qualitative Methods

I explored the obstacles that limited knowledge sharing in provisioning cell phones to stakeholders and MPs. Specifically, as explained in Chapters 1 and 2, the barriers to provisioning mobile devices are current policies that vary from agency to agency, and an organizational culture that depends on leadership and various processes. The current NIST policies vary depending on an agency's security needs and ongoing risk assessments. It is imperative that a reliable provisioning process is in place that will allow

field users and MPs to utilize secure cell phones. Sharing knowledge means that several people must be able to dialogue and exchange unclassified information.

For this study, I solicited participants for interviews to gather information for analysis. Primarily, I conducted interviews with some of those identified as users in addition to the support team members who have a direct connection with the Mobility provisioning program. The support team includes CAMs, MPs, field users, engineers, Storefront web designers/managers, and directorate leadership. The research goal was to utilize a qualitative research approach to explore the Mobility provisioning process, then discuss and ask open-ended questions of interviewees regarding the overall vision to share knowledge securely via cell phones.

According to Al-Akkad and Zimmerman (2011), with the widespread availability of cell phones, which includes standard components such as Internet browsers, internal networks, and commercial infrastructure services, cell phones support the principles of collecting data and sharing knowledge. The infrastructure development's Mobility team appreciated the standard components that are already in place through commercial vendors (AT&T, Verizon, and T-Mobile) versus building entire infrastructures from scratch.

I used Schein's (2010) organizational culture theory to support my research. Schein's organizational culture theory supports and provides a lens through which the lived experiences of stakeholders, government IT analysts, managers, customer support, and MPs, can be interpreted. With the creation of FISMA, current government IT measures drive expanded communication levels beyond one-on-one government (IT

analyst to IT analyst) communication to support collaboration between federal agency's MPs using agency-wide mobile devices (P.L. 107-347). The lack of communication in the past triggered events for advanced communication in the future (Randol, 2010). Patton (2002) posited that a qualitative approach lays the foundation for understanding previous events to transition and explore innovative processes for the future. A qualitative approach allows a researcher to be a historian with greater flexibility to understand and explore questions related to past events, as well as to examine new objectives for the future (Janesick, 2011). According to Al-Akkad and Zimmerman (2011), the preferred interview technique is face-to-face, semistructured, open-ended questions. Open-ended questions allow for more comprehensive dialogue to probe with greater focus and understanding of the internal culture. The interview questions are intended to tap answers from a broad range of interview participants, including internal and external leadership, managers, engineers, designers, and users.

My interviewees were individuals who had direct contact and support of the MDM process. MDM's designers and managers' goal were to identify the clichés, slowdowns, and barriers that undermine communication and a seamless provisioning process. I utilized a qualitative approach to, not only identify the goals in the provisioning process but to examine the experiences of government IT analysts and MPs to better identify gaps in communication. While a qualitative approach is based on exploration, identifying, and describing research data, a quantitative approach looks to answer questions, measure, and compare variables that already exist. Once a hypothesis is identified, researchers use a hypothesis-testing tradition to identify the variables and

statistical information at prearranged or fixed level (Rudestam & Newton, 2007). Because the process is a relatively new directorate, there are no reliable quantitative metrics to address some of the questions. A qualitative method was better suited to explore, question, and examine a new process for provisioning mobile devices versus a quantitative method used to test the impact through statistical surveys and questionnaires.

Qualitative Approaches

There are multiple approaches to research. According to Creswell (2009), qualitative research may explore the features of a dominant phenomenon and then divide the subject matter into meaningful topics. There are five qualitative approaches: narrative, ethnography, grounded theory, case study, and phenomenology. First, the narrative approach provides stories and documents the experiences of an individual's life (Creswell, 2013). Qualitative researchers examined the causes of a phenomenon to connect experiences and relationships (Johnson, 1997). The interviewees, or participants, are not being interviewed based on their individuality, but rather their lived experiences as a group of government IT stakeholders and customer support managers. The narrative approach was not deemed appropriate for the study.

Second, the ethnography approach focuses on the complete culture-sharing, ideas, and beliefs of an entire group (Creswell, 2013). Although this approach supports culture and sharing, the approach requires prolonged stays for research and interviews onsite (Creswell, 2013; Wolcott, 2008). Because the research site was open-storage, secure, extended stays were not permitted without an awarded contract and a security visitor's request approval. The ethnography approach was inappropriate for this study.

Third, the grounded theory approach focuses on a process or action that the researcher is trying to explain to customers (Creswell, 2013). Even though the research pertains to an action, movement, or process, the main goal was to develop a theory to support a specific action. The objective of my research was not to create or define a theory, but instead, support a Mobility provisioning process that is secure and user-friendly for all stakeholders' security. Grounded theory was not appropriate for the study.

Fourth, a case study approach identifies a specific case that has particular structures, locations, and limitations to gather and compare accurate research information (Creswell, 2013). Case studies require a chronological description of the themes and issues on a large but limited scale. The results of case studies are sometimes based on the analysis by the researcher. A case study was not appropriate for this study.

Finally, I determined that phenomenology was the best approach for my research study. Phenomenology is more oriented toward describing the lived experiences of the research participants (Creswell, 2013). With this approach, I explored the work environment of government IT personnel, their culture, their policies, and shared knowledge to provision mobile devices worldwide.

Phenomenological Approach

Mobile devices are used by consumers worldwide. However, the evolution of mobile devices is a phenomenon, and it is ongoing. According to Page (2005), qualitative research methods are used to identify users, requirements, techniques, methods, training, relationships, and locations worldwide. Phenomenological research studies are inquiries into the lived experiences of a group or individual. The relationship that develops

between individuals or groups is essential when it comes to building a process, structure, or organizational culture. Moustakas (1994) suggested that there is a relationship between human beings that provides understanding, unity, history, and the essence of lived experiences.

The experiences of government IT personnel, MPs, and stakeholders supported the Mobility provisioning process by identifying and describing past and present events. Currently federal agencies are provisioning mobile devices to field users or MPs; however, U.S. companies, such as Microsoft, with operations in Europe and Asia are looking to understand the cultural effect as well as new challenges with cybersecurity in the future. According to Creswell (2013), a phenomenon is to be explored based on a single concept or idea. A group of individuals experiences this basic idea through their lived experiences, which collectively are similar to each other. My research included analysis, observation, and interviews. For this study, a qualitative phenomenological approach was the best approach to observe the rise of mobility, wireless technology, and shared knowledge from the perspective of government IT stakeholders.

Researcher's Role

The role of a researcher is to gather information for analysis and remain unbiased in organizing and presenting the results (Creswell, 2013). Therefore, my questions and interviews had to examine the provisioning process, and the results serve as a communication platform for sharing information to leadership. After an initial examination of interviews, I set-up a Microsoft Excel spreadsheet and developed an NVivo v.12 database to capture participants' responses to analyze and store results. I

remained utterly open to discover any barriers that could pose potential problems during the study and in the future. It was essential to capture the interviews and opinions, as they existed and to construct a clear understanding of the challenges and possible solutions for all readers. The participants were varied Mobility stakeholders, including IT analysts, engineers, CAMs, and supervisors all familiar with the provisioning process, which helped eliminate any researcher bias concerning this subject.

Methodology

The purpose of my study was to identify perceptions about assumed barriers with communicating and sharing knowledge in the provisioning of cell phones to potential Mobility users who support a specific DoD agency. At the time of this study, the U.S. Department of Commerce's NIST provided some security guidelines, but little to no collaboration protocols for stakeholders. Therefore, a qualitative phenomenological approach was the most appropriate methodology to explore government IT personnel lived experiences, culture, policies, and Mobility provisioning processes for this study.

Data Collection Procedures

Approval to conduct the study was obtained from Walden University Institutional Review Board (IRB; # 01-13-18-0316817) and the leadership at DISA under the Infrastructure Development Directorate (formerly called the Program Executive Office – Mission Assurance [PEO-MA]). The previous deputy director of PEO-MA provided feedback concerning the current challenges and the POCs to contact for follow-up questions. I sent a consent form to the agency's director of the Business Development Center for permission to interview participants and to conduct the study. After leadership

approval, consent letters were sent, in approximately 5 days, via DEPS email to all potential participants. The consent letter followed the protocol and procedures approved by Walden's IRB and agency leadership. Off-site participants were contacted by phone or via email within 5 days for an initial pre-interview and then emailed the consent form in an encrypted, secure email. After receiving leadership approval, and after the participants submitted their consent forms, I scheduled participants for 17 to 60 minute face-to-face or teleconferenced interviews.

Interviews followed a set interview protocol (Appendix B) and the interview guide (Appendix C). The interviews began with a full description of the purpose of the study and a complete review of the consent form for their understanding and transparency. I orally administered a demographic questionnaire (Appendix D). The questions focused on demographic data about (a) the position they held as a customer support team member and (b) how many years they served as a team member. For confidentiality and security, I assigned the participants pseudonyms. When participants completed the demographic questions, I administered a semistructured interview with open-ended questions to participants to provide information and to recount their lived experiences within the Mobility provisioning process. I linked the interview questions to the primary research question.

Population and Sample Size

I interviewed 11 research participants from the prescribed population of Mobility stakeholders. All participants were free to select their interview time, and I sent an email confirmation. I reserved a conference or multimedia room for interviewing potential

participants. To limit potential biases, I used non-gender specific words and did not include leadership titles. The sample population encompassed various stakeholders, including IT specialists, engineers, site managers, Account Managers, and MPs who work with the DMUC implementation and sustainment processes. MPs were an organized global workforce of leaders and partners in the White House, Pentagon, military services, combatant commands, and defense and federal agencies (DISA, n.d.). The stakeholders were uniquely aware of NIST's current guidelines and policies. At the time of the study, the policies and guidelines generally supported multiple agencies but were not specific to the needs and risks of one agency. The participants were employees of DoD or MPs, and I ensured that all participants had an active CAC as an employee of DoD. Participants were assigned pseudonyms for confidentiality. All participants completed consent forms, which detailed the purpose of the study, the timeline, and additional information that helped eliminate bias

Participants and Interviewees

While random sampling provides statistical probabilities of large populations in quantitative analyses, purposeful sampling in qualitative approaches focus on smaller cases or groups with a specific drive to understand the relative issues (Patton, 2002). According to Patton, "The logic and power of purposeful sampling lie in selecting information-rich cases for study in depth" (p. 230). I based the sampling population for on participants who had direct involvement and knowledge of the provisioning process for mobile phones. The interviewees identified their years of service, education, career titles, and stated whether they considered themselves insiders or outsiders in the overall

process. The target population selected for this qualitative study included internal and external career personnel from the agency and MPs. Participants included in this study were employed during 9/11 through the time of this study. Participation was strictly voluntary and unpaid.

Data Analysis

Based on initial contact with Mobility leadership, the best approach to gather research information was through face-to-face and teleconference interviews. Due to prohibited items, for example, short-range wireless devices (Bluetooth), audio recorders, and personal computers, I used the public affairs onsite recorders. I recorded all the interviews. Off-site interviews were conducted in a conference room or multimedia room mutually agreed upon by the interviewer and participants. The results were captured in NVivo v.12, Microsoft Word, and Microsoft Excel to organize and code information with similar themes. I analyzed the data thoroughly using appropriate processes to capture the responses, whether they are words, comments, opinions, or facts. After collecting this data, I explored, and analyzed, any lingering questions. Answers to research questions were provided additional alternatives when designing future objectives. Data analysis supported the explorative study, whereby research questions highlighted patterns or themes. According to Patton (2002), credibility is increased when research collection is either random, systematic, or purposeful. Once the information was uploaded, the results were collected and organized in the NVivo software application, then coded, and analyzed.

Validity and Reliability

The research participants were voluntary. However, the entire research process was documented to support qualitative validity and reliability. According to Creswell (2009), validity is supported through strict procedures, outcomes, and results. Creswell posited that qualitative reliability supports consistent protocols, steps, and procedures for a trustworthy conclusion. Documentation, coding procedures, use of transcripts, and analysis met the standards of qualitative social science research.

Research validity and reliability supported a phenomenological exploration of the government IT, Mobility stakeholders, and participants' lived experiences and interpretation of events. According to Johnson (1997), there are twelve strategies used to promote qualitative research validity. One of the twelve strategies is triangulation. Triangulation is an essential strategy used to inquire and measure multiple methods and perspectives through hands-on, practical analysis (Patton, 2002). Qualitative researchers often analyze research data for what is plausible, credible, and trustworthy (Johnson, 1997). Research tools, documentation, and artifacts included multimedia recordings, field notes, and emails to authenticate all forms of responses from participants and to ensure clarity. Additionally, a coding scheme was used to identify participants and to capture common themes from my research analyses. I used a member checking process over the phone, and through email, to verify all participant responses, to seek any needed clarifications, and to ensure accuracy.

Trustworthiness

There are many strategies and research tools used to support trustworthiness with qualitative research. Researchers must remain unbiased and support all findings by cross-checking themes and codes (Creswell, 2013). Prolonged engagement and persistent observation support techniques in building trust with participants, understanding the culture, uncovering misinformation, and observing what is happening (Ely, Anzul, Friedman, Garner, & Steinmetz, 2003). Ethics and trustworthiness are focused on people. According to Marshal and Rossman (2016), trust specifically highlighted the relationships between the participants, stakeholders, and the community at large. Ethics exist as more than principles but rather actions to help guide researchers and participants.

I incorporated a coding scheme. For example, a pseudonym was used to identify participants and themes from the research analysis. Consent forms were provided to each participant in person or via email in advance of the interviews. Additionally, participants provided handwritten signatures or DoD digital signatures. To have a valid DoD signature, the participants had to have a CAC vetted and authorized DoD security card and the Trusted Association Sponsorship System (TASS). I collected all data and provided an unbiased assessment of that data. To maintain ethical standards, I password-protected data in Excel and NVivo, and I treated all participants equally. Although I documented my thoughts in field notes, I reserved any interpretive judgment until data collection was complete. I present a brief discussion of my biases and personal experiences as they relate to Mobility in Chapter 4.

Presentation of Results

The results of this study, based on interviews, descriptions, and interpretations from the lived experiences of research participants, are presented in Chapter 4. To ensure participant engagement in the process, and a secure interview location, I followed these protocols:

- Identified research participants' position, title, and role in the Mobility provisioning process.
- Identified an on-site agency's conference room with secure dial-in and multimedia video conference room for participant interviews.
- Confirmed the process to collect and analyze research participants' consent responses.
- Determined the software application used to identify, process, and store themes from research questions.
- Identified opportunities to address current dysfunctions in the provisioning process and the prospect of future benefits.

Moreover, I noted distinct differences between keyword phrases and themes generated from research analysis. I identify all adjustments and updates to my research methods in Chapter 4.

Informed Consent and Ethical Considerations

For this study to have, and maintain, ethical standards, all participants were provided the purpose of the study and advised of the informed consent protocols before any information was obtained or transferred. All data collected, shared, and documented

in this study remained confidential. Informed consent and confidentiality protocols were provided in a statement to participants before any interview took place. According to Patton (2002), "the basic messages to be communicated in the opening statement are (1) the information is important, (2) the reasons for that importance, and (3) the willingness of the interviewer to explain the purpose of the interview out of respect for the interviewee" (p. 407). I provided consent forms to each participant in person, or via email, before all interviews. After receiving approval signatures, I began interviews. To have an authentic DoD, valid digital signature, the participant's CAC was authorized by their security and the TASS system.

To limit biases, random selectees (DoD employees and stakeholders), who support Mobility efforts, with various backgrounds, were participants. No incentives or disincentives were used to motivate participation. All participation was voluntary, and any participant could choose to withdraw from the study at any time. All material and data obtained in this study was password protected in an Excel spreadsheet and NVivo v.12 database program. Participants were assigned pseudonyms to ensure anonymity and support confidentiality. All material relevant to the collection of information was retained and archived in a locked case file and will remain in such for 5 years after the publication of the dissertation, then be destroyed using secured DoD agency excess collection procedures. If a breach occurs, resulting in inadvertent release of collected information, I will notify all participants and agency leaders via encrypted email. In the case of participant questions, I listed my contact information on the consent forms.

Summary

Chapter 3 outlined the methodology steps taken for my research and included a description of identified barriers that limit knowledge sharing and process efficiencies government IT analysts and engineers face when provisioning mobile devices. I used a phenomenological approach to examine and explore the experiences of IT personnel and organizational culture that support the processes for MDM and Mobile Application Store (MAS). Phenomenology was the best method to understand how government IT analysts and the customer support team communicate and why sharing information with the team and the customer was essential. I protected the identity of participants and password-protected the interviewees, analyses, and results. I researched different perspectives and knowledge from internal and external stakeholders in expectation to support the future objectives of the mobile device provisioning program.

Chapter 3 the research methodology, includes the: (a) qualitative and phenomenological approaches; (b) research design; (c) research question; (d) methodology justification; (e) researcher's role; (f) specific methodology; (g) data collection procedures; (h) population and sample size; (i) participants and interviewees; (j) data analysis; (k) presentation of results; and (l) ethical considerations. Chapter 4 presents a summary of the results including: (a) research participant demographics; (b) data collection processes; (c) data analysis processes; (d) results; (e) themes; and (f) trustworthiness. Chapter 5 will cover the discussion, recommendations, and conclusions.

Chapter 4: Results

The purpose of this qualitative phenomenological study was to examine the lived experiences of the customer support team in support of the Mobility provisioning process. I designed the study to answer the following primary research question: What are the lived experiences for end-users in the government IT culture using the Mobility provisioning process for the sharing of information? I used the primary research question as to the basis for the interview questions. This chapter presents a summary of the results including (a) research participant demographics; (b) data collection processes; (c) data analysis processes; (d) results; (e) themes; and (f) trustworthiness.

Research Participants

The research population consisted of individuals who support DISA's mobile device provisioning process. I interviewed two engineers, four IT specialists/analysts, two branch leaders, and three CAMs. I identified the educational level of each participant, which included two with technical degrees, three with bachelor's degrees, four with master's degrees, one participant identified as 'other - attended college,' and one participant who did not provide an answer. Participants' years of service ranged between 1.5 years to 4 years: Two had 4 years of service, two had 3.5 years of service, three had 2 years of service, three had 1.5 years of service, and one did not provide an answer. I determined that all participants were employed at the time of the interview.

I identified three research participants as offsite staff, and their interviews were conducted and recorded in a private conference room over a secure phone line. I noted that the remaining eight research participants were onsite staff: Five interviews were

filmed and recorded in an audiovisual media room and three interviews were conducted and recorded on digital audio tape in a conference room over a secure phone line. For anonymity and confidentiality, I referred to the 11 research participants as Alfa P1, Bravo P2, Charlie P3, Delta P4, Everett P5, Forest P6, Gold P7, Hunter P8, India P9, Juliett P10, and Kilmore P11. Based on my field notes, I determined that 10 out of 11 participants were comfortable being interviewed, but one participant, Alfa P1, was uncomfortable providing information regarding demographics. As for the other participants, Kilmore P11 sounded a little nervous at first, but by the end of the interview, that participant's voice sounded calm and steady. Bravo P2 was very talkative and walked outside for a moment during the interview but quickly returned. Charlie P3, Forest P6, and Hunter P8 were talkative, funny, and appeared to be happy to participate. Everett P5 appeared to talk very fast throughout the interview. Delta P4, Gold P7, and India P9 were relaxed but had serious tones with their responses. Juliett P10 appeared comfortable, confident, laid back, and used many hand gestures throughout most of the interview.

Overall, the participants seemed receptive and willing to participate and share their experiences and knowledge regarding the Mobility provisioning process. I did not face any issues during the study. Furthermore, Forest P6 appeared to be very comfortable and jovial. Kilmore P11 seemed a little unsure of some answers because that participant's area of expertise did not line up with all the interview questions. I informed Kilmore P11 that any answers provided were fine because all were based on his/her knowledge and lived experiences. There were no right or wrong answers. When Bravo P2 stepped

outside for a moment during the interview, due to high winds, it was a little difficult to hear him/her, and the participant quickly walked back inside to the conference room. The distraction was short, and we continued the interview as scheduled.

Finding off-site interviewees to participate was more challenging than enlisting on-site interviewees. After I reached out to Mobility's leadership and points of contact from the PMO, 20 individuals were invited to participate. I contacted the participants via email. I initially recruited 11 participants: Seven on-site participants and four off-site users from the Mobility PMO Discussion Board website. The off-site users were chosen randomly based on a list of discussion board users identified by email addresses generated from Mobility questions. Only a few users listed their email addresses on the discussion board, so responses were limited and slow. The participants were not under my direct supervision, nor were they a part of my direct branch.

Data Collection Process

The data collection process for this study began when Walden University's IRB issued approval to proceed. I contacted the Mobility leadership to inform them of my study and to ask for permission to interview and explore the lived experiences of the staff that supports knowledge sharing and customer relations in Mobility. I reached out to a broad range of participants who had direct relationships with customers and stakeholders with Mobility's provisioning process. The leadership provided an organizational chart of Mobility's PMO, and I randomly chose individuals from the engineering, capabilities, and programs branches. I initially sent out 13 email invitations, and then I sent another seven for a total of 20. As I received responses, I began scheduling interviews in a

conference room or the audiovisual media room. All staff listed on the PMO organizational chart and discussion board pre-qualified due to the organization, directorate and workgroup they were associated with; thus, each met the eligibility requirements to be a participant. I confirmed eligibility for the study by including and collecting demographic questions regarding position and title, years of service, and level of education.

I interviewed 11 participants. I collected the interview data between February 22, 2018, and April 16, 2018. The interview locations included two different locations: onsite audiovisual media room and an onsite conference room. I interviewed five participants in the audiovisual media room, and six in the onsite conference room. Before I scheduled interviews, I gave all participants informed consent forms to review and sign. I explained the form, allowed the participants to ask questions, and informed them that they could choose to withdraw from the study at any time with no ramifications. I advised participants that I would ask them 10 questions, and they did not have to answer any questions that made them feel uncomfortable. I provided all participants with a copy of the informed consent form for their records.

I followed-up with each participant in person or over the phone. I established rapport before asking interview questions, making them feel at ease by assuring them that the information I collected would be secure and that I would adjust their names to pseudonyms. No participants withdrew from the study, and all participants answered interview questions except one participant who refrained from answering the

demographic information. Participants did not receive any compensation for participating in this study.

I interviewed the research participants only once face-to-face or over a conference room phone. During the interviews, I took notes and documented body language, visual cues, speech tones, and any other noteworthy responses. The shortest interview was approximately 17 minutes, and the longest was 60 minutes. After completing the interviews, I contacted all participants by phone or email to confirm and verify their feedback and responses. I asked some participants to verify their responses at the end of their interview if clarification was needed. During the interview, I recorded the participants using a digital voice recorder or videotaped in audiovisual media. Bravo P2, Alfa P1, Gold P7, Charlie P3, Delta P4, and Kilmore P11 were audio recorded on an Olympus Digital Voice Recorder. I also captured Participants Hunter P8, Forest P6, Everett P5, Juliet P10, and India P9's interviews on video and saved them to a compact disc.

I used ten interview questions to collect data to answer the research question for this study. I utilized the interview guide (see Appendix C) to ensure consistency with all participants' interviews. To ensure the accuracy of responses, I encouraged follow-up questions to clarify answers and open-ended responses from each participant. Probing and follow-up questions varied across participants according to their interview responses. At the end of every interview, I thanked each participant for their time, patience, and support. I stopped the recorder, and I informed the audio media support that the interview had ended.

Data Analysis Process

I transcribed and analyzed 11 sets of participant responses in this research study. I followed the three data analysis strategies outlined by Creswell (2013). First, I prepared and organized the participants' transcribed interview notes and video recordings. Second, I reduced the transcripts into table notes and themes. Third, I examined and interpreted data using a qualitative computer software program and created a matrix to compare and present the results in tables and figures. Before coding and condensing the data into themes, I organized and transcribed the audiovisual recordings into transcripts for each participant. These transcripts comprised the entire interview to include all interview questions and the participants' verbatim responses. After I transcribed all interviews, I contacted each participant and provided a copy of their responses for member checking confirmation. When the transcription process was complete, I coded the data by hand, highlighting common themes in Microsoft Word tables. I also used NVivo software to provide additional text structure, create nodes, query word frequency, and define themes to ensure the analysis was concise and accurate.

Bracketing

Bracketing is the process whereby the researcher must suspend their assumptions, interpretations, or experiences regarding the phenomenon of the research topic (Creswell, 2013). I identified my bias and did my best to keep an objective outlook. Although earlier in the interview process, specific keywords were mentioned, I made sure not to identify keywords or make any prejudgment in follow-up questions to the participants. To ensure

the study remained unbiased and free from prejudice, I made sure I did not acknowledge my beliefs, repeat information gathered, or detail upcoming developments.

A researcher's role supports reflexivity as a process where ethics, personal values, and background can shape and support biases during the research (Creswell, 2009). I remain certain of my role as a researcher, and my background experience did not taint the study or influence the participants' responses in any way. Although it is difficult to remove all biases, Creswell mentioned that a researcher should not marginalize or put the participants at risk and, when collecting data, the researcher should respect the participant as well as the research site. According to Chan, Fung, and Chien (2013), there are specific strategies that demonstrate how to validate bracketing; however, researchers can show how they have not influenced the data collection process.

Manual Data Coding

According to Creswell (2013), the coding process classifies interview responses from aggregated text into smaller categories of information, and then a label code is assigned. Before I began coding, first, I transcribed the recorded interviews of each participant to include the documented observations. Second, I read all interviews multiple times, and then I manually organized data in an Excel worksheet after which I transferred the data to side-by-side Word tables to recognize possible themes. Third, I looked for keywords and repetitive or similar statements to organize the data and generate ideas to support themes. Fourth, it was necessary to narrow down data to focus on reoccurring themes. Regardless of the size of the research, Creswell (2013) advised researchers to

condense and limit results to five or six themes that support the narrative. Once I developed themes, new labels and relationships emerged.

After organizing the data manually, I was able to import and upload data to NVivo v.12, a qualitative, data analysis computer software package. NVivo for Windows can import, manage, and analyze text, spreadsheets, and audiovisual data, as well as create charts, reports, and other useful functions. The fifth and final step supported the most important phenomenon. In this step, I analyzed and compared the reoccurring themes for meaning and was able to connect the lived experiences of the participants about the research questions and primary question. As I read over the data and deciphered themes, commonalities in the participants' responses emerged. According to Patton (2002), "A Phenomenologist assumes a commonality in those human experiences and must use rigorously the method of bracketing to search for those commonalities" (p. 106). The goal of a phenomenological study is to understand the lived experiences of the participants, as interpreted by the researcher.

Based on my data analyses, I conducted the following steps. I utilized Microsoft Excel for the first organization and analysis, and I transcribed field notes captured, and interview responses. I sorted the responses in tables using Microsoft Word and uploaded them to NVivo. This process provided a more detailed analysis with advanced queries to code and discover themes. For example, using Excel and Word, I listed the participants' pseudonym, captured demographic information, and reviewed their position, years of service, and level of education. Using NVivo, I imported transcribed interviews and demographic information. I used NVivo to store interviews responses, create container

nodes to query for specific data, and search for merging themes. For example, the initial responses to Interview Question 2 were coded as Simplify the Process (STP). The theme that resulted from this interview question was “I think the ordering process is a little clunky.” I documented and highlighted responses to the interview questions, and I removed responses that did not answer or support the questions. After re-reading responses, I noted how many times critical responses occurred. I compared participants’ responses to see similarities in meaning, to define or determine discrepant cases, and to develop themes.

Knowledge sharing and customer relations in Mobility described by the research participants through their lived experiences were vital to understanding the study. The research questions supported established literature and responses from the participants. I created themes from the participants’ responses based on their similar experiences, feelings, perceptions, and beliefs about sharing information and customer relations in Mobility. Furthermore, I selected themes based on the number of occurrences of related words, phrases, or statements from the research participants. I linked some reoccurring themes to other themes and discovered new themes by comparing the participants’ responses. A list of themes, including expanded communication, updated guidelines and policies, and streamlining and centralizing, is presented later in this chapter.

Discrepant Cases

According to Creswell and Creswell (2017), a researcher can present information that runs contradictory to a theme to validate the general perception of the theme. To add validity, I searched for unclear responses that were counter-active to themes that were

resolute and collected from multiple responses. I looked for unsupported responses based on uncertainties versus perspectives that connected to the demonstrated experience. Additionally, I captured irregularities and contradictions from the participants' responses that supported a discrepant or divergent statement. If one or two participants responded uniquely in comparison to all other participants' responses, I identified those responses as departures or differences and categorized them as discrepant cases. I summarize the discrepant cases in the themes section.

Study Results

I examined how government agencies share knowledge securely utilizing mobile devices as they relate to policy, culture, and process. Based on the finding from these data analyses, the participants' responses provided insight, mirroring previous studies with slight differences, in addition to multiple themes and challenges, to fill in the holes from analyzed literature. My objective was to explore the lived experiences from the perspectives of IT analysts and stakeholders to better understand Mobility's provisioning environment.

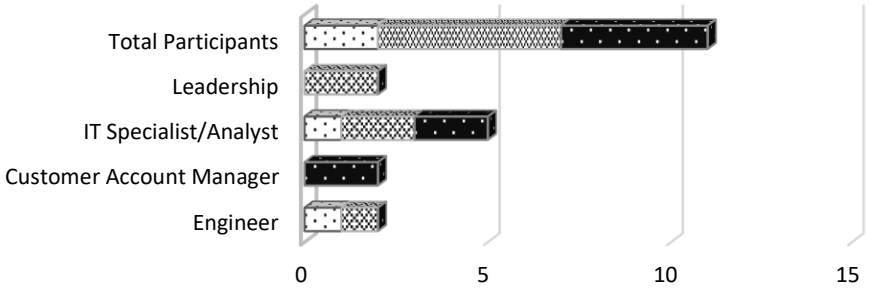
I captured several results that provided greater insight into sharing knowledge with stakeholders within the Mobility process. First, several participants were adamant about expanding communication, engaging customers more, and obtaining more feedback from leadership to solidify the Mobility process. Second, I identified a continuing resolution (CR) as a contributing factor to reduced or limited funding. Third, I found that there were guidelines provided by the NSA, but the guidelines were not standardized across all agencies. Fourth, the participants mentioned the benefits of using

automated systems and streamlining the process. For some participants, streamlining the process meant the customer should complete most of the steps on their side of the process, leaving one remaining step to be completed from the government side: final approval. The next section presents a collection of results developed from research questions. Participant interview quotes help to narrow and identify themes.

Research Question

The research question was a motivating factor for this study: What are the lived experiences for end-users in the government IT culture using the Mobility provisioning process for the sharing of information? Interview Questions 1, 2, 8, and 10 provided the most information to answer the research question by identifying process and communication concerns. Interview Question 1 detailed the interconnected communication goals required to share information faster and securely worldwide. Interview Question 2 connected participants' concerns about the things that limit or threaten the Mobility program. Interview Question 8 captured participants' feelings regarding the most significant dysfunction in the provisioning process. Interview Question 10 detailed participants' most significant benefits and achievements in the Mobility process.

Overall, the participants who took part in the research study were broken out in percentages (see Figure 1). In-person was the preferred interview method. The federal government employs all participants identified by their generic role in Figure 1. Figure 2 depicts the interview method by the percentage of in-person (conference room), in-person (multimedia conference room), and over-phone (conference room).



	Engineer	Customer Account Manager	IT Specialist/Analyst	Leadership	Total Participants
In-Person Conf Rm	1	0	1	0	2
In-Person VM Conf Rm	1	0	2	2	5
Over-Phone Conf Rm	0	2	2	0	4

Figure 1. The number of participants identified by their role

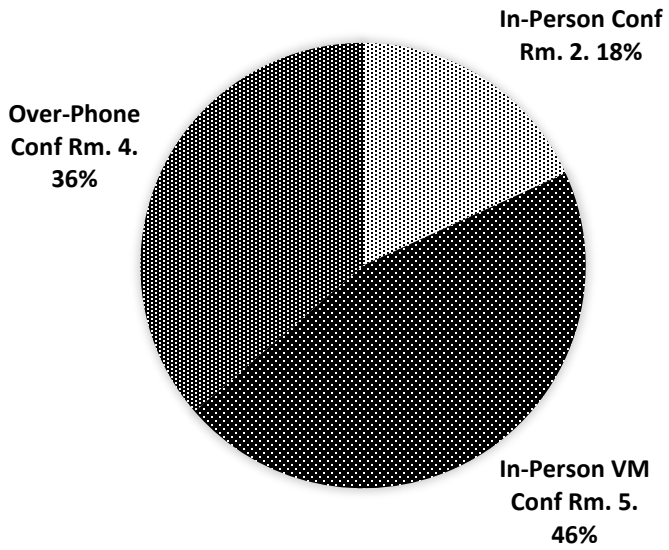


Figure 2. Participants interviewed by percentage

Based on interview participation, there were several methods of communication (over the phone and in person) all conducted onsite in a secure conference room. All roles

were represented based on the original demographic survey except for web designer architect. Most of the participants worked with the Mobility process versus web designing.

The participants' collective responses concerned expanding communication, customer feedback, leadership participation, policy guidelines, and centralizing and streamlining the Mobility process. Participants wanted to make sure customers' concerns were heard and examined by leadership to support the provisioning process. In response to interview Question 2, Charlie P3 noted that the Mobility program is threatened if there are process changes, and the information is not shared. When asked what the thing(s) that limit or threaten the Mobility program's ability to fulfill requests are, Charlie P3 responded,

> For instance, I signed up on the DoD Mobility user corner mailing list, and I have never received a single email from that announcement list. So not communicating with those who may have signed up with that mailing [list] is part of the problem.

Participants highlighted communication as one of the organizational goals to support and protect the Warfighter. Forest P6 stated, "certainly mobile is so heavily dependent on [secure communication], and it is very diverse and helpful. … So all of our goals support secure communications really."

I also noted a challenge to working in a bureaucratic system with rapid changes in technology. In response to interview Questions 1, 2, 8, and 10, participants spoke of new technologies that the NSA would need to evaluate and identify if the requirements meet standards. Kilmore P11 stated,

> You have a device that is owned by another company, so we don't own it. ... If you are bringing it into the government, it must have those security measures set up by NSA or DoD CIO to come up with the policies – [then] implementing those policies.

Teamwork and having a good relationship with NSA helps with the process to streamline research and development of new technologies. When asked what major organizational goal(s) support secure communication within the Mobility program as an interview question, Kilmore P11 responded,

> In reference to the Mobility program provisioning process, the best [way] to secure a mobile device is through the government. So [I am] going off the standards set forth by DISA and NSA.

Also, the participant's experience with the end-users sharing information and utilizing the Mobility provisioning process was a need for better communication, policy improvements, and standardization. Participants highlighted the fact that new and improved platforms help to expand and support secure communications and better relationships with stakeholders.

Participants mentioned the need to support security requirements by emphasizing the need for MDM and consistent policies to standardized mobile operations. There appeared to be a positive outlook for the future due to program automation and new improvements with the addition of the programs Mobility Onboarding Request Fulfillment Enterprise User System (MORFEUS) and Purebred. MPs use MORFEUS to submit their user list for Mobility support. Purebred is a management server that provides

a secure method to distribute software certificates for use on mobile devices. With the new improvements, the participants reported a reduction in the processing timeline.

Due to the latest techniques with automation, the participants' noted that the Mobility process must streamline their efforts and enhance their relationships with stakeholders and leadership. In response to interview Question 7, participants were concerned with the automation of the Mobility process and the amount of time it took to onboard a new user. Participants described the need to improve the provisioning and onboarding process because using spreadsheets was old and unsustainable to track users. Participants noted MORFEUS (located on DISA Storefront ordering system used to track users), and other systems may help streamline and reduce the processing time. For instance, instead of sending individual licenses through DISA Storefront and email system one at a time, the question arose if other systems automate or reduce the processing time. Participants believed that there were better, more straightforward methods to process, onboard, and support mobile users, which could reduce backlogs, communication gaps, and delays. When asked about the plans to support the automation of the Mobility process as an interview question, Hunter P8 stated,

> Now there is more of an automated process to upload and configure end users. In the past, we had to put in the order, send out a user list, and input scripts overnight for six to seven hundred users from multiple organizations. If there was one error, it would take a day to follow-up with the user and another day to correct the issue. With MORFEUS, a list is submitted through DEPS, and in real time, all is

> configured the same day. Now that the MPs can check the accuracy of submissions, you save a lot of time and effort.

Several participants voiced their opinions concerning interview Questions 3 and 4 to verify and list how federal, NIST, and standard agency policies impact end users and stakeholders. There is a broader perspective regarding a standard policy across agencies. In other words, there are policies specific to DISA, and there are policies or regulations for mobile devices in general. Forest P6 explained,

> The policy for DISA is camera off when provisioned. No one entering DISA's facility with a mobile device can get a camera. DISA is an open classified facility, but the rules vary from agency to agency, customer to customer. So, standardization, in general, would help.

Answered to Interview Question 6 demonstrated the participants' perspectives as to the best method to secure a mobile device. India P9 shared,

> As for a security for unclassified devices, I would say that users should be using their Public Key Infrastructure (PKI) certificates to sign and encrypt emails when they send emails from their mobile devices.

Participants shared several methods to help to ensure devices were secure, including security technical implementation guides (STIGs), MDM, and the national information assurance partnership (NIAP). All methods provided the government with specific guidance, compliance, and standards for IT products.

Participants' concerns included policy standards in conjunction with a greater need for customer feedback and leadership participation. In response to Interview

Question 5, participants describe what role leaders and MPs should play to provide consistency standards across agencies. Several participants noted that leadership should spend more time 'one-on-one' and communicate with users to understand their experiences and perspectives. Brave P2 stated,

> The greatest dysfunction is probably a lack of a constant feedback from the MPs to DISA leadership. I have the greatest respect for leadership, but I don't think they have heard all the facts.

Several participants noted that leadership across agencies should be sharing information and discussing lessons learned to improve the Mobility program process. Leadership, MPs, and users in the field emphasized the need for extensive feedback. India P9 reported,

> The key is feedback from the MPs… It is also important that DISA's leadership understand their role as a service, capability provider in order to access what the MPs are dealing with on the user's end.

Participants provided suggestions as to how to acquire customer feedback daily or through a one-day workshop or conference. Hunter P8 expressed,

> You bring everyone together and find out who has the most time with customer, and then find out what customers have the most issues, and how realistically can we take those issues to improve upon them, and do we have a mobility summit talk about all the high-level things to get feedback.

The main idea was to get feedback, whether it is with an individual (one-on-one) or an advertised day for group feedback and discussion. Interview Question 9 provided input as

to how the participants would address and resolve the problem with Mobility's provisioning process. Gold P7 offered,

> It starts with communication. It starts with being able to lay out clearly what the expectation is to the customers or whoever is trying to get something provisioned to make sure that they understand the processes and the expected timelines… If everybody understood it well enough, I think you can start to identify how to fix it and what parts need to be worked on.

Participants noted that they are looking beyond the manual process of provisioning devices and are streamlining and automating the process. Alfa P1 pointed out,

> In the past, there [was] a manual process, we are actually automating it now… Now we can do in a few hours what took us a week to accomplish. So now, we are streamlining and automating the process.

Although the participants acknowledged the manual process problems, they also identified streamlining, automation, and greater communication to support knowledge sharing in the future.

Summation of Results

Participants noted specific dysfunctions and benefits of knowledge sharing and customer relations in Mobility. Chapter 5 includes a more detailed discussion of particular dysfunctions and benefits to previous studies. Only one participant stated that contributing factors to dysfunctions were costs, delays, and funding limitations due to CRs. All participants acknowledged that the provisioning process could be more streamlined or centralized to have an automated process. Additionally, all participants

believed that more communication and feedback between users and leadership were vital components.

Most participants identified the need for better communication, customer feedback, leadership participation, policy guidelines, and process streamlining and automation. More than half of the participants acknowledged that policy guidelines, whether handed down from internal leadership or the NSA, and standardization is needed across agencies. Leaders, IT analysts, engineers, MPs, and various customers noted that better communication and process requirements were significant concerns.

Each interview question provided information to answer the primary research question. Also, the interview questions allowed participants an open-ended platform to describe their lived experiences with customer relations and knowledge sharing in Mobility from their perspective. Based on the responses from several interviews, the findings suggested the participants' experiences were varied, but there were a few shared experiences. After several reviews and analysis of the research data, several themes evolved.

Themes

I originally discovered seven themes, and then later, I integrated and combined themes, discarding those that were infrequent. I reduced the number of themes to three major themes. Creswell (2013) stated that themes in qualitative research are called categories that encompass several codes combined to form an idea.

There were several responses to interview questions to correspond; therefore, the same theme developed for more than one interview question. For this reason, I further

narrowed down the themes for specificity. For consistency, I described the themes in detail and determined if conflicting ideas existed as well as logical connections.

I documented the participants' lived experiences throughout the data collection process. I based the themes that evolved from this research study on the lived experiences of the research participants who utilize and support the Mobility program (see Table 1). Based on the data analysis process, three critical themes evolved throughout the interview process. According to Creswell (2013), the process

> begins with the development of the codes, the formulation of themes from the codes, and then the organization of themes into larger units of abstraction to make sense of the data. Several forms exist, such as interpretation based on hunches, insights, and intuition. (p. 187)

Table 1

Themes Confirmed from Data Analysis of Interview Responses

Themes	Number of Participants	Percentage
Expand Communication with Customers and Leaders	9	81.8
Identify Policy Guidelines	8	72.7
Streamline and Centralize the Process	11	100

Note. Themes in correlation to the number and percentage of participants.

Expand Communication with Customers and Leaders

The theme of 'Expand Communication with Customers and Leaders' evolved from the research data collected from Interview Questions 1, 2 and 8, which supported the central question of this study (see Table 2).

Table 2

Expand Communication with Customers and Leaders

Participant Responses	Perceptions	Observation
Bravo P2: I think that DISA leadership should get or coordinate with MPs' leadership to find out what the real requirements are and the real pain points are, and they could focus on what the MPs need and lock down the Mobility portions of the enterprise… I think there were a lot of assumptions. We never really got it defined what the customer really needed… Talk to the customer.	Coordinate with MPs	Participant's voice sounded calm over the phone.
Gold P7: It starts with communication. It starts with being able to layout clearly what the expectation is to the customers or whoever is trying to get something provisioned to make sure that they understand the processes and the expected timelines.	Expectation better communication	Participant's arms were down, calm steady voice.
Charlie P3: Well, when processes are changed and go unannounced. For instance, I signed up on the DoD Mobility user corner mailing list, and I have never received a single email from that announcement list. So not communicating with those who may have signed up with that mailing is part of the problem. There are no updates, so when there are changes, you don't know about it until there is a change.	Need timely communication	Participant cleared his throat and sounded a little nervous.
Hunter P8: The way we give information to new user is a problem, in my opinion. Where do they start? We don't communicate well with our customers. In other words, we do a bad job of coming back or following-up with our customers, we send them to a website, and with all these links they get lost. We need more verbal communication. We need to reach-out and talk to people.	Follow-up procedures	Participant looked straight ahead and made eye contact.

Note. Responses including the researcher's perceptions and observations.

After analyzing research data and rereading the interviews, communication, feedback from customers, and leadership emerged as being essential to research participants. Participants noted that feedback was vital to being an effective capability provider, and they found it frustrating that channels of communication were narrow.

Identify Policy Guidelines

The theme “Identify Policy Guidelines” emerged from Interview Questions 3, 4, and 6 and also provided data to answer the main research question. Equally important were policy standards derived from the theme ‘Policy Guidelines’ to include requirements and standards.

Based on interview responses, some participants wanted consistency in policy standards. Everett P5 was a discrepant case related to identifying policy guidelines because this participant reported that devices processed must be NIAP certified through NSA program evaluation and listed on an approved product list. Everett P5 was the only participant that mentioned NIAP as a standard across the board; thus, this unique response rendered it discrepant by the analysis guidelines presented for this study.

Overall, policy guidelines were valid concerns by participants who felt the need for consistent standards in provisioning a mobile device. For example, standardization may be needed on what to secure, what format, and APPs to utilize for unclassified devices. Currently, MPs or agencies determine their Mobility security needs (see Table 3).

Table 3

Identify Policy Guidelines

Participant Responses	Perceptions	Observation
Hunter P8: A standard across agencies... I think first you would have to determine who would be in charge of creating the standards. I think you would need to get buy-in across all the agencies. If you can standardize a template, the agencies could follow a generic pattern within Mobility.	Standardize policies across agencies	Participant made eye contact and looked at ease.
Forest P6: For DISA, we have camera off that is the policy and the way it is provisioned and the labels set. No one at DISA with a Mobility device gets a camera because when we walk in the building, it is an open classified area and little rules like that vary from agency to agency, customer to customer... So some standards would help across that front as well… just standardization in general.	Standardization across agencies	Participant smiles and sighs, while keeping hands folded, he looks straight ahead.
Delta P4: They [DISA] should maintain a level of consistency, and the policies should be to maintain STIGs, and they need a gatekeeper for license obviously... DISA should have a hard cap on the number of licenses distributed. There should be a policy in place to apply consistency.	Need more control over access privileges	Participant sounded very relaxed, a lighthearted voice at times with a serious tone.

Note. Responses including the researcher's perceptions and observations.

Streamline and Centralize the Process

The theme of "Streamline and Centralize the Process" emerged from Interview Questions 2, 4, 7, and 8. Participants referenced this theme the most. Streamlining and centralizing encompasses various participants' perspectives. This theme includes automating the provisioning time (eliminating manual spreadsheets), centralizing the order ticketing system, and updating the approval process. The theme highlights the influences of automation and the delays of a typical approval process (see Table 4).

Table 4

Streamline and Centralize the Process

Participant Responses	Perceptions	Observation
Juliett P10: Today, we have over 100,000 users under our unclassified capability. So we have had months where we have brought on six or seven thousands users per month. So tracking orders by spreadsheet was unsustainable, so we moved to an automated provisioning system.	Automated the provisioning process	The participant looks up slightly and talks with his hands to make an obvious point.
Juliett P10: We have employed a system internally MORFEUS on the unclassified side that dramatically decreased our provisioning time on the unclassified. We went from spreadsheets to DEPS SharePoint system that was created by a government employee out in OKC.	Processing time reduced due to an automated system	Participant looked up slightly and talked with his hands to make an obvious point. Taped his thumbs and fingers together.
Juliett P10: So it was unsustainable to have the ordering systems down to spreadsheets that someone could misplace or lose. Getting the automated MORPHEUS [Mobility onboard request fulfillment and user system] has helped us. It was not optimal for us to have spreadsheets, so we moved to an automated system.	New system automation reduced the need for spreadsheets tracking	Participant's voice was calm as he used very expressive, open hand gestures to make a point.
Alfa P1: In the past, there has been a manual process, we are actually automating it now... Where the automation is taking place and the time to provision that automation is less than what is used to be... Now we can do what took us a week can be done in just a few hours. So now, we are streamlining and automating the process. We are automating it, and everything is in accordance with NSA's requirements.	Streamlining and automating the process What customers preferred	The participant used hands gestures while talking calmly.
Charlie P3: The people who create the DMUC account… the people who creates the PINs… the people who create the Purebred components, together with TIER II Admins. Bring them all under the same umbrella of command instead of having individual umbrellas of command…	Combine and centralize people who secure network systems	Serious tone
Secure encrypted mail is pretty awesome when it works. Purebred is the additional component that runs on top of the DMUC program that allow people to send and receive encrypted mail.	Collaboration needed across the board	Voice calm, no hesitation in speech [continued]

Participant Responses	Perceptions	Observation
Charlie P3: A standard policy would be [a] centralized management system. So I don't have to talk to six different groups of people in order to get something fixed. They would all have a standardized ticketing system across the board... You must open up a ticket with somebody, who then opens up a ticket with somebody else, who opens a ticket with somebody else, who does some work on their end, and then writes you back and tells you they have to open up a ticket with somebody else.	Centralize the management ticketing system	Participant's phone voice had a little hesitation.
Hunter P8: Back to Storefront, I think the biggest dysfunction is in the ordering in how the mission partner sets up their approval chain… We would tell them that it was at level two of the approval process… You got four more levels at [at the local facility] before it gets to us. Actually, that kills a lot of people.	Streamline the approval process	Participant's arms were down, but later, he used hand gestures, and passionately spoke as he looked forward with an expression of great thought.
Delta P4: The DISA Mobility team has a piece in that an entire process has caused delays in the past. If we use the Blackberry stuff and let say NorthCom has several Blackberry licenses, we would not need DISA's approval to add a military member to the list… The approval process that we have with DMUC are major issues.	Need one-day turn-around; Re-vamp the approval process; Use Blackberry's platform.	The participant was very relaxed, with a lighthearted voice.
Delta P4: I would say the greater Dysfunction is the approval chain… Storefront and the MOEPHEUS page [have] to go through my command chief to validate. The approval process is tedious [with] MORPHEUS [you] have to wait until the Storefront is approved by them and the Mobility team gets it. Even for the Mobility team, it has to go back and forward for approval. It is time intensive. The routing of an approval process is tedious.	The approval process is slow	Participant's voice was lighthearted with a serious tone.

Note. Responses including the researcher's perceptions and observations.

According to Mathi (2018), with mobile Internet protocol, it is crucial to receive service without disruptions and to balance security services and efficiency. Participants suggested that the challenge to streamline and centralize the process was vital to efficiencies within Mobility. Using NVivo, I captured 78 references that highlighted the need to focus on process efficiencies. Based on the data collected, many participants responded to Interview Questions 2, 3, 7, 9, and 10 that supported better process efficiency. For example, India P9 stated,

> Efficiencies need to be improved because MPs can spend weeks to months trying to get an order filled. Even though some MPs are not following the right procedures or using the wrong codes for billing, the process itself takes time.

None of the other participants mentioned the need to have a new centralized ticketing system, reduces time, and works across the board. These omissions led me to believe that the other participants were not affiliated with the ticketing process issue from a CAM's perspective. I considered this a discrepant case because it related to a government helpdesk TIER I and TIER II support problem; not just to Mobility, but indirect systems as well. In addition, Charlie P3 emphasized,

> A standard policy would be good so that he would not need to talk to six different people to get something fixed; everyone would be on the same team supporting the Warfighter.

Additionally, statements in Table 4 identify the need to have a streamlined and centralized process. Kilmore P11 stressed,

> We didn't make the device so now we have to work with them [manufacturers] regarding certain devices needed to control or add limits to the device… We cannot do it alone, so we have to work with them. Bottom line is we are not the manufacturers of the device so that limits what we can do.

In this section, I presented the data collected, which includes the three themes that emerged from this research study. The next section will describe the reliability and validity of the research.

Trustworthiness of the Study

According to Creswell (2013), researchers should use several methods to validate their study irrespective of the qualitative approach. The researcher has a responsibility to the participants, the public, and to public policy experts, to make sure the research is valid and trustworthy. Creswell stressed, "prolonged engagement and persistent observation in the field include building trust with participants, learning the culture, and checking for misinformation that stems from distortions introduced by the researcher of informants" (p. 250). To validate research information, how the information is gathered, analyzed, and summarized must be confirmed. Creswell provided four terms used to validate qualitative studies: credibility, transferability, dependability, and confirmability. Each provided reliability and validity to my study.

First, I expected credibility since each participant was an active employee of DoD. I made sure all participants were listed in the DISA Global email address book. Also, I made phone calls and sent out follow-up emails to confirm interview responses were final. I confirmed all responses during the interview process, and I sent follow-up

emails to each participant to review their responses and make updates through member checking. I reviewed all responses and personally checked with a few participants to ensure acronyms were accurate. I also made a few minor changes to the transcripts where there were misspellings, and to correct and confirm acronyms.

Second, transferability is a generalization of findings from data collected to ensure the findings described and interpreted from participant to the researcher are credible (Creswell, 2013). The sampling size was small, and I purposefully selected participants due to direct involvement with the Mobility program. Thus, findings may not be transferable outside the Mobility program. Third, I established dependability by being consistent throughout the entire research and interview process. I was the only researcher and interpreter of research information; therefore, the analyses of data were consistent and reliable. All interviews were conducted with the same instructions and protocols, listing observations of participants, and noting any themes and irregularities. The interview guide was referenced and utilized throughout the semistructured interview process.

Fourth, I achieved confirmability by reviewing the interviews captured by audiovisual recordings. I reviewed all of the participants' interviews multiple times. I also transcribed notes from data collected, transferred all information collected into tables to review, and edited for accuracy. I Also utilized NVivo to help identify, capture, organize, and describe themes. Finally, bracketing was used to suspend and remove my assumptions, and I relied solely on data analyses from the lived experiences and perceptions of research participants. Reflexivity is a bracketing technique that I noted

previously. All four terms promote qualitative methods that support trustworthiness, contribute to research that is comprehensive, reliable, and valid.

Summary

After analyzing the results, three key findings stood out and were relevant to my research. First, more than 80% of the participants believed that better communication and feedback was a significant concern across the board. Second, a few participants felt that more policy standards to support Mobility guidelines would require assistance with consistency across agencies. Third, most of the participants believe that the streamlining and centralizing the system for automation using MORPHEUS versus using spreadsheets improved processing time. Specifically, the participants felt that the Storefront and MORPHEUS approval chain was long and tedious and should be shortened.

Out of all the results, I asked the participants what the most significant benefits or achievement in the provisioning process were. Participants believed that Mobility should support customers through communication, building relationships, and working as a team to automate, streamline, and utilize the best solutions. This belief tied together all the themes as a way forward. This chapter included three themes that described participants' perception of sharing knowledge and Mobility's provisioning process. The themes and patterns that emerged were: Expand Communication with Customers and Leaders, Identify Policy Guidelines, Streamline and Centralize the Process.

This chapter presented a summary of the results including: (a) research participant demographics; (b) data collection processes; (c) data analysis processes; (d) results; (e) themes; and (f) trustworthiness. Chapter 5 covers the discussion, recommendations, and

conclusions including: (a) interpretation of findings; (b) research question; (c) support for the conceptual framework; (d) limitations to the study; (e) implications for social change; (f) recommendations for action; (g) recommendations for further research; and (h) researcher experiences.

Chapter 5: Discussion, Recommendations, and Conclusions

Since the events of 9/11, DoD organizations and support agencies continue to evolve as to how they share information in support of the Warfighter (Randol, 2010). According to Jones (2007), information sharing is needed to address environmental challenges by diversifying tools that expand connectivity and assist analysts to better interpret information creatively. The purpose of this qualitative phenomenological study was to describe the lived experiences of a government IT customer support team's ability to share information and support MPs within the Mobility provisioning process. I recruited eleven research participants to participate in this study. I conducted in-depth semistructured interviews to collect data for the study with seven onsite and four offsite participants. All participants were government employees who supported the Mobility Directorate. One main research question was the basis for the research study and was used to devise the ten open-ended interview questions asked of each participant.

This chapter includes my interpretation of findings using an interpretive lens Schein's (2010) organizational culture theory and a description of the study's limitations. Specifically, I compare the interpretation of findings to the literature I reviewed in Chapter 2. I also discussed the implications for social change, recommendations for action, and recommendations for further study. The chapter covers the discussion, recommendations, and conclusions including: (a) interpretation of findings; (b) research question; (c) support for the conceptual framework; (d) limitations to the study; (e) implications for social change; (f) recommendations for action; (g) recommendations for

further research; and (h) researcher experiences. The chapter concludes with my experiences conducting the study and reflections upon my findings.

Interpretation of Findings

The findings from this qualitative study present fresh insights and a better understanding of Mobility's provisioning process from the perspectives of government IT analysts, MPs, and users. One main research question guided the research. In addition to submitting answers to the research questions, the findings were discussed and compared to the literature review, and I supported my interpretations by other researchers, studies, and the conceptual framework.

Research Question

What are the lived experiences for end-users in the government IT culture using the Mobility provisioning process for the sharing of information? The answer to this question was that government IT end-users utilizing the Mobility provisioning process must share information and, to a large extent, more automation is needed to streamline and centralize the order ticketing system and chain of approval processes. Based on the data collected, I found that new policies were needed, existing policies need to be consistent across agencies, and communication between leadership and customers strengthened. The results of this study suggested that Emad-ul-Haq et al. (2015) were correct when they stated that the overall idea is to have a safe connection and communication with Mobility devices for end users and customers.

Based on data collected, my findings contradicted claims by Noor (2011). Noor declared that the next challenge is to merge communication, virtual robotics networks,

and smart mobile devices into collaborative learning environments. The participants in my study did not support this declaration. The data I collected indicated that the participants' main concerns were to streamline and centralize the provisioning process, reduce the approval process, and improve communication up and down the chain of command. However, some participants proclaimed that automated systems dramatically reduced the provisioning process timeline on the unclassified environment, but for now, a standard policy to centralize the management ticketing system would be more beneficial than virtual robotics networks.

The primary research question encompassed the IT culture, process guidelines, and the sharing of information. According to Schein (2010), to understand the observed group, you must talk to the insiders and examine their members' behavior and daily operations. Due to using Schein's organizational culture theory, I found themes that emerged from research that aligned with the theoretical constructs to support the study. Table 5 shows the themes that align and theoretical constructs.

Table 5

Research Themes and Schein's Theory (Levels of Culture) Alignment

Research themes	Schein's theory (levels of culture)
Expand communication with customers and leaders	Artifact – culture/symbols
Identify policy guidelines	Beliefs – policy/rules
Streamline and centralize the process	Assumptions – processes/behavior

Note. Themes in correlation to Schein's (2010) organizational culture theory.

The second most noted theme was to expand communication with customers and leadership. Using NVivo, I captured 56 references that supported the need to examine

cultural behavior when sharing knowledge with users throughout the chain of command. According to Sutcliffe (2005), cultural methods encompass values, assumptions, and behaviors that support and guide how people think, do, and act. Culture provides benefits and risks. For example, some members bring communication skills, wisdom, and experience to resolve a problem in which sharing knowledge can serve to improve a process and eliminate the uncertainty. There are examples of those who follow the book and chain of command versus communicating with experienced team members with in-depth expertise on the frontlines. If there is more than one problem, and the challenges are specific to each area of concern, coming to a resolution could be complicated and time-consuming.

Many participants noted the symbolism of a government facility following the procedures, protocol, and chain of command when communicating with leadership. Schein (2010) indicated that organizational processes whereby behavior is observed as predictable and repetitive are considered an artifact. “In other words, observers can describe what they see and feel but cannot reconstruct from that alone what those things mean in the given group” (p. 24). Based on data collected, several participants responded to Interview Questions 1, 2, 5, and 8 with the need for better communication between leadership and customers. For example, Hunter P8 offered that, for some customers, the approval process is three steps, and for others, it is a seven-step process. In other words, the user may need help, but their order is at level two of the approval process, and they have several more levels of approval before the order is processed. This process is not communicated well to the customers, as it is tedious and mundane. Although the users

were following an ordering process, participants felt that the goal should be better customer service, which means reviewing policy guidelines.

Participants conveyed that the key to good customer service is to have effective organizational processes and policy guidelines in place, as well as choosing a standard policy to serve agencies across the board. According to Yoonho (2016), “Government Agencies vary according to their policy missions” (p. 1017). Thus, organizational structures and policies differ according to the goals and missions designed by each agency. Being that mobility is considered new innovative technology, Basant (2018) offered that policies that complement new knowledge could also create demand and support for innovation. For example, according to DISA (2015), the end goal and mission of a combat defense agency is to support the Warfighter to include innovations and new technology.

Several participants mentioned the need for policy standards and consistency across agencies. Schein (2010) offered that beliefs and values are created within new groups; however, leaders share knowledge and influence actions that validate guidelines and rules as shared values. Using NVivo v.12, I captured 36 references that mentioned NSA requirements, STIG guidelines, NIAP, and NIST policies. Based on the data collected, participants responded to Interview Questions 3 and 4, which brought attention to the need for policy standards. For example, Forest P6 indicated that it would be nice if provisioning knew that every mobile device was standardized because the devices vary from agency to agency, so having specific standards like the camera on or camera off would be helpful.

The most critical and most noted theme was to streamline and centralize the Mobility provisioning process. With the thought of implementing new processes and guidelines, participants listed several new developments and automation (for example, MORPHEUS and Purebred.) Participants stated that automation and streamlining had a significant effect on the provisioning process. In other words, from a centralized credentialing email process with Purebred to decreasing the provisioning timeline utilizing MORPHEUS, automation has brought about some improvements. To improve performance for mobile social networks to include categorizing data attributes, Chen, Kang, Yin, and Kim (2016) proposed a new clustering method of algorithms that helped with accuracy and efficiency. After interviewing and observing the participants, I determined that the underlying assumptions were to add efficiencies, streamline actions, and incorporate improvements.

All participants believed that the overall Mobility process needed improvements. The underlying assumption was that only the provisioning process required improvements, but the research data I collected provided additional details regarding people and process structures. According to Schein (2010), "the power of culture comes about through the fact that the assumptions are shared and, therefore, mutually reinforced" (p. 31). From observing the Mobility process to interviewing leaders, customers, and the support team, the assumption was that process improvements were needed to influence communication and cultural behavior. Using NVivo, I captured 78 references acknowledging a need for new platforms, automation, and standardized

processes. Based on the data collected, participants responded to Interview Questions 5, 9, and 10 that detailed the need for standardization and process streamlining.

Support for the Conceptual Framework

I based my research on Schein's (2010) organizational culture theory as the conceptual framework for thematic interpretation. Interview Questions 1, 8, and 10 provided the data I used to support the conceptual framework for this study. Participants' perspectives and answers to Interview Questions 4 and 5 also provided additional data. As stated in Chapter 1, one of the basic tenets of organizational culture theory is that a researcher can observe the behavior of stakeholders, define the underlying structure, and predict how the future may look (Schein, 2010). The participants' responses were consistent with Schein's theory, which identifies three levels of culture: artifacts (culture/symbols), beliefs (policy/rules), and assumptions (processes/behavior).

All 11 participants' responses to questions regarding their stakeholder experiences and their role in the Mobility provisioning process fully supported this tenet. As stated earlier in this chapter, all participants believed the underlying assumptions that process improvements were needed and the research collected supported information about people and process structures. The findings indicated that most of the participants wanted streamlined processes, approvals shortened, better communication throughout the command culture, and specific policies to be consistent across agencies.

The cultural aspects of new technology played an essential role in the participants' values, beliefs, and assumptions with provisioning mobile devices. Schein (2010) stated, "…that technological seduction and innovation changes behavior,

reexamines assumptions, and embraces new values and beliefs" (p. 284). Unlike Sheppard et al. (2012), who acknowledged risk communication philosophy in phases that found threats, rules, responses, methods, processes, and assumptions; I found that Schein's organizational culture theory recognized organizational environments, rules, and behaviors. Based on the research data I collected, Schein's organizational culture theory supports the research.

The participant responses included a reference to future improvements. Cultural factors such as the role of leadership, level of education, years of service, and shared beliefs did not distract from process guidelines but had a significant impact on the research. Specifically, leadership and customer support had some similar views about the provisioning process, and participants' views were not different due to their level of education. In this study, the participants' lived experiences and beliefs about knowledge sharing and customer relations in Mobility had a more significant influence than their role, years of service, or education.

Limitations of the Study

The first limitation of this study was that many onsite participants had scheduling conflicts due to the demands of their jobs. Even though initially, there were recruitment issues due to reorganization and scheduling conflicts, after speaking with a Mobility team leader regarding my concerns, a team member provided an internal organizational chart that proved to be helpful. Second, my objective was to send emails to all individuals in the Mobility Directorate, but due to a directorate re-organization, the names and positions changed. I recruited five members from the organization chart. Third, due to offsite

locations and time zone differences, interview timelines were adjusted to accommodate the participants' schedules. I extended the interview timelines to occur after 4:00 pm to capture the participants' responses. I received emails from four offsite individuals willing to participate and share knowledge. The participants worked for military services or commands, but most participants worked for a DoD agency. Fourth, while collecting and reviewing research data, the competitive education program's (CEP) appropriated funds that supported my coursework and research was delayed. The delay postponed the completion of my research. After several months, I received an email that CEP funds would be available to support my research course again.

Additionally, I recruited two participants from an internal Mobility user website (Mobility PMO Discussion Board). I asked respondents if they knew of individuals who would be willing to participate. Two respondents (one onsite and the other offsite) suggested that I reach out to one of their associates. I followed up with the associates via emails and phone calls, and both agreed to participate. My goal was to confirm 12 interviews (two additional individuals in case of dropouts). I accepted and interviewed a total of 11 participants for the study. Two participants were unaware of NIST policies that have an impact on Mobility stakeholders; they were unable to provide a detailed response to an interview policy question. All participants were competent to share their perspectives and lived experiences. At face value, I trusted their responses regarding Mobility's knowledge sharing and customer relations phenomenological approach.

Implications for Social Change

My research detailed government IT stakeholders' experiences, perspectives, attitudes, and beliefs regarding the Mobility provisioning process, knowledge sharing, and customer relations at a DoD combat support agency at Fort Meade, Maryland. If the recommendations for action are considered and implemented, there could be several implications for enacting positive social change. As mentioned in Chapter 1 and stated by Roesener et al. (2014), some cybersecurity policies clarify positions and responsibilities, but they do not sufficiently address imminent threats. With provisioning secure mobile devices, the government can extend communication, streamline the process, support additional standards/policies, and expand knowledge sharing across agencies. Efficiencies can be added to the Mobility provisioning process with a modernized order ticketing management system, updated approval process to reducing sign-offs and timelines, and improved communication with stakeholders. Based on my results, there are several implications of social change that have the potential to transform society:

- Unclassified mobile devices will be on an approved NIAP products list before provisioned to the customer, which will help standardize mobile systems.
- Federal agencies can consolidate to a single service provider for MPs and stakeholders as opposed to individual groups, services, or agencies doing their own thing.
- The next generation of improvements is to automate Mobility's configuration process by allowing MPs to utilize MORPHEUS;

stakeholders will save time and increase efficiency. Specifically, having a VPN available with credentialing enterprise email, and using Purebred will add a layer of security at the secret level. Therefore, the next generation improvements have the potential to increase capacity, quality, and security for mobility solutions.

- Combatant commands require secure solutions; that is, fast and reliable communication in the field. Mobility solutions are diverse, interconnected, and utilized internationally. Mobile devices can be attractive to combatant commands who can provide feedback to leadership to improve upon capabilities for the future.

Also, public policymakers can use my findings for greater insight into knowledge sharing and customer relations within the government's IT Mobility provisioning process from the stakeholder's perspectives. Policymakers could require centralized standards and add greater consistency across agencies based on stakeholders' feedback. The government may benefit from increased communication and improved relationships with stakeholders, as well as save significant funds and staff-hours to expand Mobility's capability and automation.

Recommendations for Action

Based on my findings, I have three recommendations suitable for government officials, stakeholders, and policymakers. First, more communication between the customers and government leadership is needed so that necessary changes can be implemented. I based this recommendation on the theme of "Expand Communication

with Customers and Leaders." More specifically, providing adequate feedback to government leadership is a necessity to fulfill requirements and address stakeholders' concerns. The theme reflects the goals of Mobility users, stakeholders, and leadership. A significant relationship between leaders and stakeholders supports ideas, shared assumptions, and beliefs in the organizational culture.

If the relationship between the business organization and customer lacks trust, the willingness to share or exchange information decreases (Rice & Sussan, 2016). Security and governance procedures for IT's privacy data supports a level of trust between two individuals or between an individual and an organization. The Mobility support team and leadership could share information through securely organized video conferences. Effective communication technology is necessary where diverse systems and interoperable systems work together for increased efficiency and functionality (Sobanski & Nicolai, 2011). The impact of Mobility expands communication, social media, and international governments to partner, protect, and defend networks against cyber attacks. Being that we are a global community, Kumar, Yadav, Sharma, and Singh (2016) noted that, due to the increase in cyber attacks and unethical cybercrimes, governments must work together to strengthen their security policies.

My second recommendation is for leadership and stakeholders to agree to utilize a standard policy across the board for consistency with all Mobility users. I based this recommendation on the theme "Identify Policy Guidelines." For participants to have stability, there needs to be uniformity when provisioning unclassified mobile devices. In other words, participants wanted additional guidelines or policies for consistency across

agencies regarding device formats, availability of APPs, helpdesk ticketing, and whether the device camera should be turned on or off for all agencies.

According to Sanchez-Esguevillas, Carro-Martinez, Khasnabish, and Gupta (2009), there is a lack of industry standards for customers with mobile devices from various manufacturers (that is, user endpoints or public IP networks) that allow continuous connectivity and standardizations that are forthcoming. Mobile device policies are critical to the security of the device for industry and government. When governments support mobile standard-setting processes globally, define specifications for mobile Internet services, ensure consistent display systems, and offer additional options, competition increases (Funk, 2009). Finally, the need for additional standards, policy guidance, and a centralized process are not to create bureaucracy but also to build stability.

My third and final recommendation for action is that leaders and stakeholders' beliefs and assumptions are that the Mobility process and structure could be less cumbersome, but more efficient. I based this recommendation on the theme of "Streamline and Centralize the Process." Based on lived experiences, all participants responded to this theme. It arguable that the participants and stakeholders could share knowledge, add automation, streamline the approval process, and centralize the management helpdesk ticketing systems. MORPHEUS is just one example of using automation in the provisioning process that eliminates bulky and time-consuming spreadsheets. By utilizing MORPHEUS, the onboarding process timeline has improved from taking several weeks to roughly two days.

Currently, MORPHEUS and Purebred are used to optimize the process, reducing the time it takes to provision a mobile device. MORPHEUS replaced the manual uploading of spreadsheets, and Purebred is a component that allows individuals to encrypt email messages all on unclassified systems. According to the IASE (2018), Purebred is a management server that was developed by PKI Engineering to enable DoD staff credentials on mobile devices such as, Apple iOS and Android. In other words, both MORPHEUS and Purebred are examples of efficiencies added to the Mobility provisioning process.

It is important to note that communication, policy, and streamlining efficiencies were at the forefront of the participants' experiences versus finance, security, and privacy issues. The significance of these items does not mean that the participants did not mention finance or security, or that those subjects were not significant. In fact, According to Rajaei, Chalmers, Wakeman, and Parisis (2018), most "users are very concerned when it comes to giving away their privacy in terms of mobility patterns, future destinations or social interactions for the sake of a more efficient routing protocol" (p. 107). Participants did mention security requirement guidelines and financial accountability during their interviews; however, those factors were not among the three most critical. For this research, the focus was more toward the experiences of government IT customer support and stakeholders within the organizational culture of Mobility's provisioning process. Participants in this study were steadfast in their belief that process improvements were needed to secure the device effectively.

Recommendations for Further Research

Based on my experience conducting this research and reviewing the literature on sharing information in Mobility, I would make the following recommendations for further research. My findings identified new gaps in governmental IT provisioning of mobile devices to users and stakeholders. One possible new research question could be: How can government IT support the consolidation of mobile device provisioning requirements? A second research question could address stakeholder feedback to improve communication within Mobility's government IT culture. For example, sharing knowledge through mobility conferences to provide information to global stakeholders. Specifically, how does the Mobility culture affect the Warfighter's ability to communicate in the field? My study identified ways to be consistent in provisioning mobile devices across the board but did not determine why provisioning cannot be the same for all government departments. Standardization is one of the critical traits to increasing efficiencies, reducing short unstable short cuts/workarounds, and reducing operating risk. The government already has a long-standing reputation as a bureaucratic machine full of redundancies and inefficient processes; thus, improving on that reputation would indeed be social change.

Other government authorities, such as combatant commands and services that support the Warfighter, should be interviewed to provide their lived experiences with the Mobility process. Additionally, interviewing stakeholders from different agencies may provide support from different perspectives that can add credibility to knowledge sharing in Mobility. Since my research provided information that supports the Warfighter, it

would bring another level of trustworthiness to interview the Warfighter in the field. Finally, researchers could use a different methodology, such as a mixed methods approach, to include a quantitative study to measure the effectiveness and impact of the Mobility provisioning process.

Researcher's Experience

My experience as a researcher was very positive and enlightening. I learned a great deal from conducting the research and even more from the lived experiences of the participants. My lived experiences and interactions with the participants provided an in-depth understanding of the governments' IT culture with provisioning mobile devices. Some could argue that, because I interviewed several people who worked in the Mobility Directorate of which my Directorate supports several of their contracts, I could have biased the study by influencing the participants. I would counter that notion to say that I do not personally endorse any Mobility contracts, but instead, I had access to several participants through interviews only. My professional association enriched the credibility of this study because participants were familiar with the directorate structure and felt more relaxed sharing their lived experiences with onsite personnel instead of an outsider.

I took measures to ensure the study's validity and reliability. I used bracketing, member checking, and triangulation to ensure that my professional relationship and lived experiences with the phenomenon did not drastically alter the participant's ability to respond objectively. I also followed the interview protocol with every participant and used probing questions when necessary. I vacated my preconceived notions about

provisioning mobile devices, as much as possible, so that I could be open to learning everything I could from my interactions with the participants.

My reflections on the ideas and concepts associated with knowledge sharing and customer relations in Mobility led me to several conclusions. Although there is a Storefront website and a Mobility discussion board, there is no guarantee that users who utilize the services are aware of the latest information or updates. Also, I learned that stakeholders prefer more verbal communication ensuring they are on the right track, following procedures, and responding to customer feedback promptly. I learned that there is strength in numbers. When the stakeholders' beliefs, experiences, assumptions, and processes are shared goals, it enhances the organizational culture and promotes greater efficiency and communication for the entire team. Although the relationship between leaders and customers exist, their real power is the ability to define processes, share information, and influence goals for the future.

Through the participants' experiences, I learned that process changes are not easy; it takes time to determine the best techniques to test, approve, and implement a new system. Specifically, participants noted that it is pivotal to involve stakeholders from the beginning with all process upgrades versus trying to predict what their needs are later. From the beginning of the process, everyone should ask, what is the most important change needed? For example, most of the participants believed that to improve standards meant you required more communication and feedback with the users. In other words, you would need to be consistent across the board, know who the users are, know what they were experiencing, and determine how their issues could be resolved or improved.

Overall, this experience expanded my research, interviewing, and evaluation skills. Equally, I gained a greater appreciation and understanding for the Mobility process to provision secure mobile devices to combatant commands, services, and agencies. I was aware of the MDM ability to enforce security policies but unaware of the provisioning process guidelines for customers and stakeholders. From my perspective, this experience highlighted my gratitude to the Mobility team for the time it takes to provision a device now compared to the beginning, and how stakeholders could share knowledge in the future. Also, the opportunity to learn more about Mobility gave me a better understanding of the importance of the process involved and the amount of collaboration needed to securely contact a person from anyplace at any time.

Conclusion

My research focused on the beliefs, attitudes, values, experiences, and perceptions of knowledge sharing from stakeholder participants who utilize mobile devices from a DoD combat support agency. The Mobility Directorate continues to grow to automate their processes and streamline services in support of their stakeholders. For example, years ago, the process was to track unclassified orders by a spreadsheet but later through automation utilizing the Morpheus system. Thus, the processing time was reduced by 50 percent. Mobility, like the cell phone industry, is one of the fastest growing communication industries today. People can use their cell phones to do almost anything, including communicate, make purchases, or banking. The DoD MPs and the Warfighters want the latest technology for an agile deployment environment, greater productivity, ease of use, and convenience in the field.

My results confirmed many of the views reported in the literature. I also discovered new ideas where leaders and stakeholders could collaborate to expand their relationship to better support the Warfighter. My discoveries can lead to positive social change, process streamlining, increased engagement between leaders and stakeholders, and standardize policies across agencies, combatant commands, and services. Stakeholders, including the Warfighter, deserve a secure and simplistic way to obtain a mobile device. The process to provision mobile devices should be a benefit, not a hardship, to users. The leadership provided the vision and resources to achieve the overall mission, but stakeholders' ideas and contributions provided experience and feedback that supports the customers and users. As a result, it is imperative that the relationship between government IT leaders and stakeholders is a two-way system of communication versus a top-down, "stovepipe" form of sharing information based on old cultural barriers.

I did not discover as much as predicted about securing mobile devices or sharing information that could pose cultural challenges in a secure government environment. Securing a mobile device can only be as effective as the process to provision the device to users. With each new technological advance, comes more challenges; therefore, to secure a mobile device is an ongoing process.

Finally, the challenge for government IT leaders, customer support, stakeholders, and MPs could be to promote knowledge sharing through several mobility day summits or conferences. The conferences could provide a platform to share updates, identify issues, and bring awareness to the Mobility program in support of the Warfighter. My

research could help ensure that government leaders and stakeholders often communicate to better define Mobility's cultural environment, policies, and process behaviors.

References

Al-Akkad, A., & Zimmermann, A. (2011). User study: Involving civilians by smart phones during emergency situations. Proceedings of the 8th International ISCRAM Conference – Lisbon, Portugal, May 2011.

Aldrich, H. (2008). *Organizations and environments*. Stanford, CA: Stanford University Press.

Armando, A., Costa, G., Merlo, A., & Verderame, L. (2015). Formal modeling and automatic enforcement of bring your own device policies. *International Journal of Information Security*, *14*, 123–140. doi:10.1007/s10207-014-0252-y

Ashkanasy, N., Wilderom, M., & Peterson, M. (2011). *The handbook of organizational culture and climate* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Basant, K. (2018). Exploring linkages between industrial innovation and public policy: Challenges and opportunities. *VIKALPA: The Journal of Decision Makers, 43*, 61-76. doi:10.1177/0256090918774699

Brown, E. (2012). NIST updates guidelines for mobile device security. Retrieved from https://www.nist.gov

Brown, K. (2015, November). Enhancing battlefield communications through 4G LTE+ cellular technology. *Journal of Battlefield Technology*, *18*(3), 5-16. Retrieved from http://www.argospress.com

Bush, S. (2016). Risk markets and the landscape of social change. *International Journal of Political Economy*, *45*, 124-146. doi:10.1080/08911916.2016.1185315

C-SPAN (Producer). (2015, October 29). *Christian Science Monitor breakfast on military cybersecurity* [Report video issue]. Retrieved from https://www.c-span.org

Chan, Z., Fung, Y., & Chien, W. (2013). Bracketing in phenomenology: Only undertaken in the data collection and analysis process? *The Qualitative Report, 18*(59), 1-9. Retrieved from http://www.nova.edu/tqr

Chang, A., & Kannan, P. (2002, October). Preparing for wireless and mobile technologies in government. *Center for the Business of Government: e-Government Series*. Retrieved from http://www.businessofgovernment.org

Chen, Z., Kang, H., Yin, S., & Kim, S. (2016). An efficient privacy protection in mobility social network services with novel clustering-based anonymization. *EURASIP Journal on Wireless Communications and Networking*, *275*, 1-9. doi:10.1186/s13638-016-0767-1

Coombs, W. (2015). *Ongoing crisis communication: Planning, managing, and responding* (4th ed.). Thousand Oaks, CA: Sage Publications.

Coombs, W., & Holladay, S. (2012). *The handbook of crisis communication.* Chichester, UK: John Wiley & Sons.

Cowley, J. (2010). Planning in the real-time city: The future of mobile technology. *Journal of Planning Literature*, *25*, 136-149. doi:10.1177/0885412210394100

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Thousand Oaks, CA: Sage Publications.

Department of Defense Commercial Mobile Device Implementation Plan. (2015). *Memorandum for Secretaries of the Military Departments.* Office of the DoD Chief Information Officer, 1-26. Retrieved from https://iase.disa.mi

Department of Defense Mobile Device Strategy, v 2. (2012). *Memorandum for Secretaries of the Military Departments.* Office of the DoD Chief Information Officer, 1-11. Retrieved from https://apps.dtic.mil

Defense Information Systems Agency. (2015). The IT combat support agency. Retrieved from http://www.disa.mil/AboutDefense Information Systems Agency. (2016). DoD mobility program. Retrieved from https://www.disa.mil

Defense Information System Agency. (2016). DISA: Mobility division (ID7). Retrieved from https://disa.deps.mil/

Defense Information System Agency. (n.d.). DISA's mission partner support. Retrieved from http://www.disa.mil

Defense Mobility Unclassified Capability Implementation and Sustainment Process (2015). Retrieved from https://disa.deps.mil

E-Government Act of 2002, Pub. L. No. 107-347, 44 U.S.C. § 101 H.R. 2458, 107th Congress.

Elzen, B., Geels, F., & Green, K. (2004). *System Innovation and the transition to sustainability: Theory, evidence and policy.* Northampton, MA: Edward Elgar Publishing.

Ely, M., Anzul, M., Friedman, T., Garner, D., & Steinmetz, A. (2003). *Doing qualitative research: Circles within circles*. Philadelphia, PA: Routledge Falmer.

Emad-ul-Haq, Q., Aboalsamh, H., Belghith, A., Hussain, M., Wadood, A., Dahshan, M., & Ghouzali, S. (2015). Challenges and solutions for Internet of things driven by *IPv6. KSII Transactions On Internet and Information Systems, 9,* 4739-4758. doi:10.3837/tiis.2015.12.001

FCW Staff. (2015, November 11). OPM gets cyber hiring nod: DISA moves on classified mobile and more. Retrieved from FCW Insider at https://fcw.com

Federal Bureau of Investigation (2010 – 2015). Information technology strategic plan: Achieving the vision. Retrieved from https://www.fbi.gov

Funk, J. (2009). The co-evolution of technology and methods of standard setting: The case of the mobile phone industry. *Journal of Evolutionary Economics*, *19*, 73-93. doi:10.1007/s00191-008-0108-6

Geller, T. (2012). DARPA shredder challenge solved. *Communication of the ACM, 55* 16-17. doi:10.1145/2240236.2240242

Geser, H. (2006). Is the cell phone undermining the social order? Understanding mobile technology from a sociological perspective. *Knowledge, Technology, & Policy, 19*(1), 8-18. Retrieved from http://geser.net/intcom/t_hgeser28.pdf

Heighington, A. (2011). Homeland Security in real-time: The power of the public and mobile technology. *Homeland Security Affairs*, *7*(13), 1-6. Retrieved from https://www.hsaj.org

Hughes, R., & Stoddart, K. (2012). Hope and fear: Intelligence and the future of global security a decade after 9/11. *Intelligence and National Security, 27,* 625-652. doi:10.1080/02684527.2012.708518

Information Assurance Support Environment (2016). IASE: Policy and Guidance. Retrieved from http://iase.disa.mil

Information Assurance Support Environment (2018). IASE: Purebred. https://iase.disa.mil

Infosec. (2015, June 8). Insider vs. outsider threats: Identity and prevent. Retrieved from Infosec at https://resources.infosecinstitute.com

Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L No. 108-458, S. 2845, 108th Congress.

Jain, A., Bolle, R., & Pankanti, S. (2006). *Biometrics: Personal identification in networked society*. New York, NY: Springer.

Janesick, V. (2011). "Stretching" exercises for qualitative researchers (3rd ed.). Thousand Oaks, CA: Sage Publications.

Jenkins, W. (2006). Collaboration over adaptation: The case interoperable communication in Homeland Security. *Public Administration Review*, *66,* 319-321. doi:10.1111/j.1540-6210.2006.00588.x

Jones, C. (2007). Intelligence reform: The logic of information sharing. *Intelligence & National Security*, *22*, 384-401. doi:10.1080/02684520701415214

Johnson, R. (1997). Examining the validity structure of qualitative research. *Education, 118*(2), 282-290. Retrieved from https://www.questia.com/library/p5118/education

Jontz, S. (2015, October 1). U. S. Navy moves toward mobility. Retrieve from Signal at http://www.afcea.org

Keblawi, F., & Sullivan, D. (2007). The case for flexible NIST security standards. *Computer, 40*, 19-26. doi:10.1109/MC.2007.223

Kumar, S., Yadav, S., Sharma, S., & Singh, A. (2016). Recommendations for effective cyber security execution. *2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH),* 342-346. doi:10.1109/ICICCS.2016.754237

Lee, B., & Shin, S. (2014). The study of privacy security in mobile traffic control environment. *International Journal of Security and Its Applications, 8,* 173-182. doi:10.14257/ljsla2014.8.2.18

Levendovsky, T., Dubey, A., Otte, W., Balasubramanian, D., Coglio, A., Nyako, S., … Karsai, G. (2014). Distributed real-time managed systems: A model-driven distributed secure information architecture platform for managed embedded systems. *IEEE Software, 31,* 62-69. doi:10.1109/MS.2013.143

Lookout. (2013, December 13). Mobile threat predictions [Press release]. Retrieved from Lookout, Inc. at https://www.lookout.com

Mabee, B. (2007). Re-imagining the borders of US security after 9/11: Securitization, risk, and the creation of the Department of Homeland Security. *Globalizations, 4*, 385–397. doi:10.1080/14747730701532567

MacGowan, J., Lofgren, M., & Vachal, K. (2009). Supplemental information for NRMR MPOs integrating security into small MPO planning activities. *Journal of Transportation Law, Logistics, & Policy, 76*(2), 174-209. Retrieved from http://www.atlp.org

Manalo, C., Noble, T., Miller, K., & Ferro, C. (2015). Control systems cybersecurity: Lessons learned from Virginia assessments. *Journal: American Water Works Association, 107,* 60-67. doi:10.5942/jawwa.2015.107.0174

Marshall, C., & Rossman, G. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage Publications.

Mathi, S., & Srilakshmy. (2018). An optimized and secure BUTE – binding update using twofold encryption for next generation IP mobility. *Journal of Intelligent & Frizzy Systems*, *34*, 1311-1322. doi:10.3233/JIFS-169427

Miller, J. (2016, June 20). Halvorsen 'firing for effect' in calling for the end of CAC. Retrieved from Federal News Network at http://federalnewsnetwork.com

MITRE. (2013). Supply chain risk management. Why SCRM is important. Retrieved from http://www.mitre.org

Moustakas, C. (1994). *Phenomenological research methods*. Thousand Oaks, CA: Sage Publications.

National Commission on Terrorist Attacks Upon the United States. (2004). *9-11 Commission Report*. Retrieved from http://www.9-11commission.gov

National Institute of Standards and Technology. (2014). Computer security division: Computer security resource center. Retrieved from http://csrc.nist.gov

National Security Agency Central Security Service. (2009). Defending our nation. Securing the future. Retrieved from https://www.nsa.gov

National Security Directive 42. (1990). National policy for the security of national security telecommunications and information systems. Partially declassified/released on 11/22/1996 under the provisions of E.O 12958 by D. Van Tassel, National Security Council. 1 - 11

National Security Strategy. (2010). *Obama Administration's 2010 National Security Strategy*. Retrieved from http://osce.usmission.gov

Noor, A. (2011). Intelligent adaptive cyber-physical ecosystem of aerospace engineering education, training, and accelerated workforce development. *Journal of Aerospace Engineering*, *24*, 403-408. doi:10.1061/(ASCE)AS.1943-5525.0000128

Ohme, J. (2014). The acceptance of mobile government from a citizens' perspective: Identifying perceived risks and perceived benefits. *Mobile Media & Communication*, *2*, 298-317. doi:10.1177/2050157914533696

Page, C. (2005). Mobile research strategies for a global market. *Communications of the ACM, 46,* 42-45. doi:10.1145/1070838.1070864

Patten, K., & Harris, M. (2013). The need to address mobile device security in the higher education IT curriculum. *Journal of Information Systems Education*, *24*(1), 41-51. Retrieved from http://www.jise.org

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Paulsen, C., & Coulson, C. (2011). Beyond awareness: Using business intelligence to create a culture of information security. *Communications of the IIMA*, *11*(3), 35-54. Retrieved from http://www.iima.org

Peterson, A. (2015, December 8). Everything you need to know about encryption: Hint, you're already using it. Retrieved from https://www.washingtonpost.com

Polo, Y., & Sese, F. (2013). Strengthening customer relationship: What factors influence customers to migrate to contracts? *Journal of Service Research*, *16*, 138-154. doi:10.1177/1094670512471584

Rajaei, A., Chalmers, D., Wakeman, I., & Parisis, G. (2018). Efficient geocasting in opportunistic networks. *Computer Communications*, *127*, 105-121. doi:10.1016/j.comcpm2018.05.014

Randol, M. A. (2010). The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress (Report No. R40602): Perceptions, statutory definitions, and approaches. Washington, DC: Congressional Research Service. Retrieved from https://fas.org

Rice, J., & Sussan, F. (2016). Digital privacy: A conceptual framework for business. *Journal of Payments Strategy & Systems, 10*(3), 260-266. Retrieved from https://www.ingentaconnect.com/content/hsp/jpss

Roesener, A., Bottolfson, C., & Fernandez, G. (2014). Policy for U.S. Cybersecurity. *Air & Space Power Journal, 28*(6), 38-54. Retrieved from http://www.au.af.mil

Rudestam, K. E., & Newton, R. R. (2007). *Surviving your dissertation: A comprehensive guide to content and process* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Russell, T. (2013). *Electronic government barriers and benefits as perceived by citizens who use public services* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Thesis Database. (UMI No. 3554782).

Sanchez-Esguevillas, A., Carro-Martinez, B., Khasnabish, B., & Gupta, A. (2009). Applications and support technologies for mobility and enterprise services. *IEEE Wireless Communication, 16,* 6-7. doi:10.1109/MWC2009.5109458

Schein, E. H. (2010). *Organizational culture and leadership*. San Francisco, CA: John Wiley & Sons.

Schwalb, S. (2013). Research collaboration tools for the U.S. Department of Defense. *Information Services & Use, 33,* 243–250. doi:10.3233/ISU-130710

Sheppard, B., Janoske, M., & Liu, B. (2012). Understanding risk communication theory: A guide for emergency managers and communicators (Report). Retrieved from Human Factors/Behavioral Sciences Division, Science and Technology Directorate, U.S. Department of Homeland Security: College Park, MD at https://www.start.umd.edu

Smith, D. (2013). Phenomenology. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Winter 2013 Edition). Stanford, CA: Center for the Study of Language and Information, Stanford University. Retrieved from https://stanford.library.sydney.edu.au

Sobanski, E., & Nicolai, B. (2011). Mobility of a disaster recovery communication system. *2011 IEEE Global Humanitarian Technology Conference*, 450-461. doi:10.1109/GHTC.2011.50

Solution Spotlight. (2013). Samsung: Tablet tipping point. *Government Technology*, *26*(5), 34-34. Retrieved from http://www.govtech.com

Souppaya, M., & Scarfone, K. (2013). NIST special publication 800-124 revision 1: Guidelines for managing the security of mobile devices in the enterprise. Guidelines for managing the security of mobile devices in the enterprise, publ. 800-124, 1–30. doi:10.6028/NIST.SP.800-124r1

Suorsa, A., & Huotari, M.L. (2014). Knowledge creation and the concept of a human being: A phenomenological approach. *Journal of the Association for Information Science and Technology*, *65*, 1042-1057. doi:10.1002/asi.23035

Sutcliffe, K. (2005). Information handling challenges in complex systems. *International Public Management Journal*, *8*, 417-424. doi:10.1080/10967490500439875

U.S. Department of Commerce, National Institute of Standards and Technology. (2013). NIST special publication 800-53, revision 4: Security and privacy controls for federal information systems and organizations. doi:10.6028/NIST.SP.800-53r4

U. S. Government Publishing Office. (n.d.). Public law 107-347 - e-Government Act of 2002. Retrieved from https://www.gpo.gov

Unlu, A., Matusitz, J., Breen, G., & Martin, L. (2012). The impact of 9/11 on information policy in the United States: A current perspective on homeland security and emergency management. *Journal of Applied Security Research*, 7, 320-340. doi:10.1080/19361610.2012.686095

Verkooij, K., & Spruit, M. (2013). Mobile business intelligence: Key considerations for implementations projects. *Journal of Computer Information Systems*, *54*, 23-33. doi:10.1080/08874417.2013.11645668

Watson, I, & Lightfoot, D. J. (2003). Mobile working with connexions. *Facilities*, *21*, 347-352. doi:10.1108/02632770310508006

Welch, E., & Feeney, M. (2014). Technology in government: How organizational culture mediates information and communication technology outcomes. *Government Information Quarterly*, *31*, 506-512. doi:10.1016/j.giq.2014.07.006

Wertz, F., Charmaz, K., McMullen, L., Ruthellen, J., Anderson, R., & McSpadden, E. (2011). *Five ways of doing qualitative analysis: Phenomenological psychology, grounded theory, discourse analysis, narrative research, and intuitive*. New York, NY: Guilford Press.

Wolcott, H. F. (2008a). *Ethnography: A way of seeing*. Lanham, MD: Altamira Press.

Yoo, S-G., Park, K-Y, & Kim, J. (2012). Confidential information protection system for mobile devices. *Security and Communication Networks, 5*, 1452-1461. doi:10.1002/sec.516

Yoonho, K. (2016). The relationship between policy types and organizational structures in U.S. federal agencies: An analysis focused on formalization, span of control, headquarters ratio, and personnel mobility. *Administration & Society, 48*, 988-1030. doi:10.1177/0095399713519327

Zhang, D., Wang, Z., Guo, B., & Yu, Z. (2012). Social and community intelligence: Technologies and trends. *IEEE Software, 29*, 88–92. doi:10.1109/MS.2012.96

Appendix A: Interview Questions

Mobility's provisioning process provides knowledge sharing, capabilities, and services to the enterprise, which supports MPs, stakeholders, and the Warfighters. The interview questions are as follows:

1. From your experience, what major organizational goal(s) support secure communications within the Mobility program?
2. Based on your lived experiences, what are thing(s) that limit or threaten the Mobility program's ability to fulfill requests?
3. As you think about your daily work, what federal or NIST policies have the greatest impact on you as an end-user and stakeholder in the process?
4. From your perspective, if uniform policy standards are needed to support Mobility, what should be a standard policy across agencies?
5. As you think about yourself as a leader, what role should DISA leaders and MPs play to provide consistent standards for all agencies?
6. From your perspective and current experience, what is the best method to secure a mobile device?
7. As you think about the plans to support the automation of the Mobility onboarding process, please give your perspective of the plan, your role, and when you expect the process to be up and running? (List Date: _____ Support information: _____)
8. From your perspective, if there is dysfunction in the Mobility provisioning process, what is the greatest contributor to the dysfunction(s)?

9. As you reflect on Mobility's provisioning process, how would you address and resolve the problem(s)?
10. From your perspective, what has been the greatest benefit/achievement(s) in Mobility's provisioning process?

Appendix B: Interview Protocol

Overview

1. Tape-record the interviews if approved by leadership.
2. Interview in a neutral setting.
3. Utilize video conferencing, media streaming or conference calls if permitted.
4. Each interview is scheduled to last 30 to 45 minutes.

Interview Methodology

Interviews will be executed with a tailored approach to investigate the lived experiences of a defense IT agency's Mobility customer support team and leadership. Follow-up questions will be used to support and inspire the interviewee's knowledge of current and past events. The researcher will use a semistructured format for questions. Interviews will encompass:

1. Ten predetermined questions.
2. The questions will be the same for all interviewees and respondents.

Designation of Interviewee:

Interview Location: DoD agency or the Participants' conference room

Date: To be determined

Start Time: the researcher and participants will arrange the time set for interviews. I will ask the participants what they deem to be an appropriate time for the interview.

Finish Time: Interviews will last from 30 to 45 minutes.

Appendix C: Interview Guide

1. Structure of the Interview
    a. Introductions (5 – 10 minutes)
    b. Review and confirm confidentiality and consent form
    c. Create a relax and secure environment
    d. Dialogue to set the tone and to answer any remaining questions

Question: Have you received preliminary correspondence from me explaining the nature of my research and the format to be used?

Question: Are there any questions thus far?

2. Explain the purpose of the interview to participants

The purpose of this interview is to explore factors that have influenced your choices and decisions. For the time of this interview, I would like to understand and know your experiences as they pertain to the subject of this study.

3. Ask permission to record the interview

With your authorization, I would like to record via tape or video the discussion and interview to capture what is said in order to support my notes and observations. Only I will listen and have access to the recording and records. My research will describe and summarize what you and other interviewees have said based on your knowledge and experiences. No responses will be associated to your name; pseudonyms will be used. Your name will not be used in the collection of research data or in the results.

The open-end questions are intended to obtain your lived experience and perceptions. The interview time will be between 30 and 45 minutes. If you agree to

volunteer and participate in the research process, please sign the informed consent page and confidentially agreement.

Compensation: Interviewees will not receive any compensation for their participation in the study.

Appendix D: Demographic Survey

This survey was designed to collect information about the lived experiences of a government IT customer support team as it relates to their ability to share information, communicate and support MPs through the Mobility provisioning process. After 9/11, defense agencies' IT culture utilized many methods to share information, and now the process has expanded to include mobile devices to share information from any place at any time. I will use data collected for dissertation research purposes only.

1. Please identify your position, title, or role in support of the Mobility provisioning process. Circle the answer that best describes your responses.
    a. IT Specialist/Analyst
    b. Engineer
    c. Web Designer/Architect
    d. CAM
    e. Leadership
    f. Other (please describe) _____
2. How many years have you supported this effort as a team member?
    a. List the number of years: _____
    b. No reply or prefer not to say: _____
3. What is your highest level of education completed?
    a. Technical degree
    b. Bachelor's degree
    c. Master's degree

d. Doctoral degree

e. Other (please describe) _____