



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**COMMERCIAL MOBILE DEVICE TECHNOLOGY
IMPLEMENTATION IMPLICATIONS IN UNITED
STATES MARINE CORPS PROCESSES: A CASE STUDY
APPROACH**

by

Buddy J. Ellis

September 2016

Thesis Advisor:
Second Reader:

Glenn R. Cook
Thomas J. Housel

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

| | | | | |
|--|---|--|---|--|
| REPORT DOCUMENTATION PAGE | | | <i>Form Approved OMB No. 0704-0188</i> | |
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503. | | | | |
| 1. AGENCY USE ONLY (Leave blank) | | 2. REPORT DATE September 2016 | | 3. REPORT TYPE AND DATES COVERED Master's thesis |
| 4. TITLE AND SUBTITLE COMMERCIAL MOBILE DEVICE TECHNOLOGY IMPLEMENTATION IMPLICATIONS IN UNITED STATES MARINE CORPS PROCESSES: A CASE STUDY APPROACH | | | 5. FUNDING NUMBERS N/A | |
| 6. AUTHOR(S) Buddy J. Ellis | | | | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000 | | | 8. PERFORMING ORGANIZATION REPORT NUMBER | |
| 9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A | | | 10. SPONSORING / MONITORING AGENCY REPORT NUMBER | |
| 11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____. | | | | |
| 12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited. | | | 12b. DISTRIBUTION CODE | |
| 13. ABSTRACT (maximum 200 words) <p>The United States Marine Corps is operating in an increasingly resource-limited and fiscally constrained environment while simultaneously becoming more dependent on information technology systems to efficiently train and operate. Balancing budget and mission requires innovative solutions to current problems. One such innovation that could potentially save the Marine Corps money, while increasing its ability to prepare for and conduct its mission, is the use of commercial mobile devices.</p> <p>This research used case study methodology to describe three processes that could benefit from the implementation of commercial mobile devices in the Marine Corps. Each independent case study was presented with three courses of action with implementation strategy variations. Socio-technical systems theory was used to analyze the intersection between the proposed new technology and the user. The technology acceptance model was used to analyze the likelihood of actual usage based on implementation strategy used. Finally, each course of action was analyzed with regard to confidentiality, integrity, and availability of organizational data.</p> <p>The conclusion of this research is that no "one-size-fits-all" implementation strategy of these devices will minimize risks and maximize benefits in all processes. This is likely due to the variations in confidentiality, integrity, and availability requirements of each process.</p> | | | | |
| 14. SUBJECT TERMS commercial mobile device, bring your own device, BYOD, change management, application-based access, United States Marine Corps, USMC, confidentiality, integrity, availability, technology acceptance, sociotechnical systems theory | | | 15. NUMBER OF PAGES 127 | |
| | | | 16. PRICE CODE | |
| 17. SECURITY CLASSIFICATION OF REPORT Unclassified | 18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified | 19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified | 20. LIMITATION OF ABSTRACT UU | |

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**COMMERCIAL MOBILE DEVICE TECHNOLOGY IMPLEMENTATION
IMPLICATIONS IN UNITED STATES MARINE CORPS PROCESSES: A CASE
STUDY APPROACH**

Buddy J. Ellis
Major, United States Marine Corps
B.S., United States Naval Academy, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
September 2016**

Approved by: Glenn R. Cook
Thesis Advisor

Thomas J. Housel, Ph.D.
Second Reader

Dan C. Boger, Ph.D.
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The United States Marine Corps is operating in an increasingly resource-limited and fiscally constrained environment while simultaneously becoming more dependent on information technology systems to efficiently train and operate. Balancing budget and mission requires innovative solutions to current problems. One such innovation that could potentially save the Marine Corps money, while increasing its ability to prepare for and conduct its mission, is the use of commercial mobile devices.

This research used case study methodology to describe three processes that could benefit from the implementation of commercial mobile devices in the Marine Corps. Each independent case study was presented with three courses of action with implementation strategy variations. Socio-technical systems theory was used to analyze the intersection between the proposed new technology and the user. The technology acceptance model was used to analyze the likelihood of actual usage based on implementation strategy used. Finally, each course of action was analyzed with regard to confidentiality, integrity, and availability of organizational data.

The conclusion of this research is that no “one-size-fits-all” implementation strategy of these devices will minimize risks and maximize benefits in all processes. This is likely due to the variations in confidentiality, integrity, and availability requirements of each process.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

| | | |
|-----------------|--|---------------|
| I. | INTRODUCTION..... | 1 |
| A. | BACKGROUND | 1 |
| B. | PROBLEM STATEMENT | 2 |
| C. | PURPOSE STATEMENT | 2 |
| D. | RESEARCH QUESTIONS..... | 3 |
| E. | RESEARCH GOALS | 3 |
| F. | THESIS ORGANIZATION..... | 3 |
| II. | LITERATURE REVIEW | 5 |
| A. | COMMERCIAL MOBILE DEVICE TECHNOLOGY | 5 |
| B. | IMPLEMENTATION STRATEGY CATEGORIES..... | 6 |
| C. | INFORMATION SYSTEMS STRATEGY TRIANGLE..... | 11 |
| D. | INFORMATION SYSTEMS STRATEGY AND POLICY IN THE DOD | 13 |
| 1. | Current Strategic Focus of DOD/DON/USMC Applicability | 13 |
| 2. | Plans and Policies..... | 15 |
| E. | SOCIOTECHNICAL SYSTEMS THEORY | 21 |
| F. | TECHNOLOGY ACCEPTANCE MODEL | 23 |
| G. | CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA) TRIAD..... | 24 |
| 1. | General Issues..... | 26 |
| 2. | General Solutions | 27 |
| H. | PREVIOUS CASE STUDIES AND RESEARCH ON CMD IMPLEMENTATION POLICY | 29 |
| 1. | CMD in Commercial Sector (Intel Corporation)..... | 30 |
| 2. | CMD in Government | 30 |
| 3. | Previous Research on CMD in DOD..... | 32 |
| I. | SUMMARY | 33 |
| III. | METHODOLOGY | 35 |
| A. | RESEARCHER BIAS | 35 |
| B. | CMD IN MARINE CORPS EDUCATION AND TRAINING CASE STUDY (CASE 1)..... | 36 |
| 1. | Background and Organization | 36 |
| 2. | Researcher Experience | 38 |
| 3. | Case Explanation | 39 |

| | | |
|-----|---|-----------|
| 4. | Potential Courses of Action..... | 42 |
| 5. | Case Summary | 44 |
| C. | CMD IN SQUADRON FLIGHT SCHEDULE DEVELOPMENT CASE STUDY (CASE 2)..... | 44 |
| 1. | Background | 45 |
| 2. | Researcher Experience | 48 |
| 3. | Case Explanation | 48 |
| 4. | Potential Courses of Action..... | 50 |
| 5. | Case Summary | 52 |
| D. | CMD IN AVIATION MISHAP INVESTIGATION CASE STUDY (CASE 3)..... | 52 |
| 1. | Background | 53 |
| 2. | Researcher Experience | 56 |
| 3. | Case Explanation | 56 |
| 4. | Potential Courses of Action..... | 58 |
| 5. | Case Summary | 60 |
| E. | SUMMARY | 60 |
| IV. | ANALYSIS | 63 |
| A. | GENERAL ANALYSIS OF CMD IMPLEMENTATION IN THE USMC | 64 |
| 1. | Cost Related Risks and Benefits | 65 |
| 2. | Productivity Related Risks and Benefits..... | 67 |
| 3. | Gaining Organizational Competitive Advantage..... | 72 |
| 4. | General Analysis Summary | 73 |
| B. | CASE 1 ANALYSIS..... | 74 |
| 1. | Sociotechnical Systems Theory Analysis | 74 |
| 2. | Technology Acceptance Model Considerations | 76 |
| 3. | Confidentiality, Integrity, and Availability Analysis..... | 78 |
| 4. | Analysis Summary | 79 |
| C. | CASE 2 ANALYSIS..... | 79 |
| 1. | Sociotechnical Systems Theory Analysis | 80 |
| 2. | Technology Acceptance Model Considerations | 80 |
| 3. | Confidentiality, Integrity, and Availability Analysis..... | 81 |
| 4. | Analysis Summary | 82 |
| D. | CASE 3 ANALYSIS..... | 83 |
| 1. | Sociotechnical Systems Theory Analysis | 83 |
| 2. | Technology Acceptance Model Considerations | 84 |
| 3. | Confidentiality, Integrity, and Availability Analysis..... | 85 |
| 4. | Analysis Summary | 87 |

| | | |
|----|--|-----|
| E. | SUMMARY | 87 |
| V. | CONCLUSIONS AND RECOMMENDATIONS..... | 89 |
| A. | CONCLUSIONS | 89 |
| B. | FINDINGS AND RECOMMENDATIONS | 89 |
| 1. | Case 1 Findings | 89 |
| 2. | Case 2 Findings | 91 |
| 3. | Case 3 Findings | 93 |
| 4. | Findings Summary..... | 95 |
| C. | RECOMMENDATIONS FOR FUTURE RESEARCH..... | 96 |
| | LIST OF REFERENCES | 97 |
| | INITIAL DISTRIBUTION LIST | 105 |

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

| | | |
|-----------|---|----|
| Figure 1. | Implementation Categories. Source: Grajar et al. (2013, p. 64). | 6 |
| Figure 2. | The Information Systems Strategy Triangle. Source: Pearlson and Saunders (2013, p. 24). | 11 |
| Figure 3. | Implementation Considerations. Source: DOD CIO (2012, p. 6)..... | 19 |
| Figure 4. | Secure Management Framework, Source: Anderson (2013, p. 6)..... | 21 |
| Figure 5. | Sociotechnical Systems Theory. Adapted from Bostrom and Heinen, (1977, p. 17). | 22 |
| Figure 6. | Technology Acceptance Model. Source: Davis et al. (1989, p. 985). | 24 |
| Figure 7. | Confidentiality, Integrity, and Availability (CIA) Triad. Adapted from (FISMA, 2002). | 25 |

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

| | | |
|----------|--|----|
| Table 1. | HYOD Army Usage. Source: Mercado and Spain (2014, p. 12)..... | 7 |
| Table 2. | Naval Aviation Mishap Severity Classifications. Adapted from OpNav (2014, pp. 3-14 – 3-15)..... | 54 |
| Table 3. | Case 1 Findings..... | 90 |
| Table 4. | Case 2 Findings..... | 92 |
| Table 5. | Case 3 Findings..... | 94 |

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|------|---|
| AAMO | Assistant Aircraft Maintenance Officer |
| AGM | aviation ground mishap |
| AMB | aviation mishap board |
| ASO | Aviation Safety Officer |
| | |
| BCC | blind carbon copy |
| BFT | Blue Force Tracker |
| BYOD | bring your own device |
| | |
| C4 | Command, Control, Communications, and Computers |
| CAC | common access card |
| CBRN | chemical, biological, radiological, and nuclear |
| CC | carbon copy |
| CDET | College of Distance Education and Training |
| CIA | confidentiality, integrity, and availability |
| CIO | Chief Information Officer |
| CMD | commercial mobile device |
| CNO | Chief of Naval Operations |
| COA | course of action |
| CUI | controlled unclassified information |
| CYOD | choose your own device |
| | |
| DISA | Defense Information Systems Agency |
| DOD | Department of Defense |
| DON | Department of Navy |
| DoSS | Director of Safety and Standardization |
| | |
| EEOC | Equal Employment Opportunity Commission |
| EF21 | Expeditionary Force 21 |

| | |
|-----------|--|
| FAA | Federal Aviation Administration |
| FISMA | Federal Information Security Management Act |
| FM | flight mishap |
| FOIA | Freedom of Information Act |
| FRM | flight related mishap |
| GFE | government furnished equipment |
| HQMC | Headquarters United States Marine Corps |
| HYOD | here's your own device |
| IT | information technology |
| JCS | Joint Chiefs of Staff |
| JTAC | Joint Terminal Attack Controller |
| MAC | media access control |
| MAGTF | Marine Air Ground Task Force |
| MarineNet | Marine Corps Distance Learning Network |
| MCBH | Marine Corps Base Hawaii |
| MCBul | Marine Corps Bulletin |
| MCEN | Marine Corps Enterprise Network |
| MCMAP | Marine Corps Martial Arts Program |
| MCRC | Marine Corps Recruiting Command |
| MCRD | Marine Corps Recruit Depot |
| MCRP | Marine Corps Reference Publication |
| MCU | Marine Corps University |
| MDM | mobile device management |
| MOS | military occupational specialty |
| M-SHARP | Marine-Sierra Hotel Aviation Readiness Program |
| NAVAIR | Naval Air Systems Command |

| | |
|------------|---|
| NAVMC | Navy Marine Corps |
| NAVSAFECEN | Naval Safety Center |
| NCO | non-commissioned officer |
| NPS | Naval Postgraduate School |
| NSC | National Security Council |
| ODO | Operations Duty Officer |
| OpNav | Office of the Chief of Naval Operations |
| OPNAVINST | Office of the Chief of Naval Operations Instruction |
| OpsO | Operations Officer |
| OYOD | on your own device |
| PCS | permanent change of station |
| PED | portable electronic device |
| PII | personally identifiable information |
| PKI | public key infrastructure |
| PME | Professional Military Education |
| PTO | Pilot Training Officer |
| QDR | Quadrennial Defense Review |
| ROI | return on investment |
| SecDef | Secretary of Defense |
| SIREP | Safety Investigation Report |
| SMF | secure mobile framework |
| SNCO | staff non-commissioned officer |
| SOP | standard operating procedures |
| STS | Sociotechnical Systems |
| TAD | temporary assigned duty |
| TECOM | Training and Education Command |

| | |
|--------|--|
| TPM | trusted platform module |
| TTB | Alcohol and Tobacco Tax and Trade Bureau |
| UAV | unmanned aerial vehicle |
| USMC | United States Marine Corps |
| VDI | virtual desktop infrastructure |
| WESS | Web-Enabled Safety System |
| WAMHRS | WESS Aviation Mishaps & Hazards Reporting System |

ACKNOWLEDGMENTS

First and foremost, thank you to my wife, Kim, for tolerating the hours I spent in the Dudley Knox Library and at our kitchen table researching and developing this thesis. Marriage to a military officer is not easy, and it is even more difficult when husband and wife both are military. Thank you for allowing me to pursue my education and for supporting me throughout the process, especially on the days that I felt I would not be able to complete this task. Thank you for providing the support when needed, and the tough love when necessary. You are truly a blessing from God, and daily I am thankful for your love and presence in my life.

I would also like to thank my thesis advisor, Glenn Cook, for the extensive time he spent guiding and encouraging me through this process. Thank you for the hours you devoted to helping me develop my thoughts, set deadlines, and realize my potential. Thank you to my co-advisor, Dr. Thomas Housel, for helping me develop a better understanding of research methodology, and for helping me to develop a research idea into a viable thesis proposal.

I would like to thank my parents, Barbara and Doug Ellis, for giving me a strong educational foundation, and for cultivating a persistent desire for knowledge in my life. I am thankful for the love and support of my family throughout my military career and during my time at Naval Postgraduate School.

Finally, I would like to thank God for his continued blessings on my life and the opportunities he has given me. “I can do all things through Christ who strengthens me” (Philippians 4:13). I pray for your continued blessings on my life, my family, and my career.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

In the 21st century, the United States Marine Corps (USMC) faces an increasingly complex geo-political climate while operating in a constrained budgetary environment. This situation requires the USMC to “balance fiscal responsibility and mission accomplishment” (Nally, 2013). Balancing budget and mission requires innovative solutions to current problems. One such innovation that could potentially save the USMC money, while increasing the ability to prepare for and conduct its mission is the use of commercial mobile devices (CMD).

Cebrowski and Garstka (1998) identified information technology (IT) as central to increasing return on investment (ROI) and competing in the modern economy, and that the use of IT would be central to meeting the demands of modern network-centric warfare. IT has the potential be a force-multiplier for the Department of Defense (DOD); IT also has the potential to be a significant limiter of productivity and effectiveness if new technology is not properly implemented.

The Director of the USMC’s Command, Control, Communications, and Computers Department (C4) recognized that:

The user requirement to access and share information from non-traditional workspaces will enable more efficient mission accomplishment. The ability to access, share and manipulate data and information from non-traditional workspaces will afford users with additional freedom of movement across and expanding information environment. (Nally, 2013)

This statement from the USMC Director of C4 directly addresses the Marine Corps need for mobility in the IT used by its workforce. Implementing a policy allowing CMD technology in the USMC has the potential to increase the mobility and efficiency of the workforce while decreasing costs.

CMD technology implementation has risks associated with legal ownership of data and the device itself, as well as issues in terms of security validation of users (Anderson, 2013, p. 10). The Marine Corps recognizes that the security of the

government network is a key tenet to implementing and realizing the potential benefits of this technology (Anderson, 2013, p. 10). From an IT security standpoint, the most secure course of action for the DOD could be to forbid the use of CMDs to conduct business. This could be the most secure choice, but this choice would deny the affected subordinate units the improved efficiency and effectiveness that CMD usage has enabled in other organizations. Intel Corporation knew that corporate oversight and security could be more easily assured by restricting CMD usage. They also recognized that such a policy would make it a less attractive employer in an industry that was seeing increased competition for talented employees (Chandrasekhar, 2013, p. 2).

The Clinger-Cohen Act (1996) directs the continuing assessment of the IT management experiences of other government organizations, international organizations, and the private sector. This research follows the Clinger-Cohen Act (1996) directive by assessing the implementation of CMD policies in a variety of organizations in order to better understand how implementation of similar policies could impact the DOD and, more specifically, the USMC. Using the experiences of these organizations, this research will develop three case studies that illustrate the potential effect CMD technology could have in various USMC business processes.

B. PROBLEM STATEMENT

There is little empirical data concerning the implications of the increased use of commercial mobile devices in the United States Marine Corps. This is a problem because the United States Marine Corps is operating in an increasingly resource limited and fiscally constrained environment while simultaneously becoming more dependent on information technology systems to efficiently train and operate. Leveraging the use of personally procured computing devices may allow the United States Marine Corps to become even more efficient, productive, and better positioned to carry out its mission.

C. PURPOSE STATEMENT

The purpose of this research is to explore scenarios where implementation of policies allowing the use of commercial mobile devices could allow the United States Marine Corps to achieve higher productivity while minimizing IT investment. This is

important because the United States Marine Corps now is carrying out more complex operations around the world, often under austere conditions. In order to be better prepared to conduct these operations, the United States Marine Corps may be able to benefit from better understanding how other organizations/companies address the use of commercial mobile devices and how United States Marine Corps could possibly implement the use of these devices.

D. RESEARCH QUESTIONS

This thesis seeks to answer the following questions:

- What are the organizational and policy implications of using personal commercial mobile devices in the Marine Corps?
- What are the organizational and policy implications of using personal commercial mobile devices on completing computer based training?
- What are the organizational and policy implications of using personal commercial mobile devices in scheduling and completing unit level training?
- What are the organizational and policy implications of using personal commercial mobile devices in conducting a safety or mishap investigation?

E. RESEARCH GOALS

The goal of this research is to increase the understanding of how the use of commercial mobile devices on Marine Corps networks may be implemented in a manner that takes into account confidentiality, integrity, and accessibility. Through the development of case studies and the analysis of potential courses of action, this research is intended to provide a better understanding of the social and technical implications of implementing this technology. The desired end-state of this research is that decision makers within the Marine Corps have a better understanding of the risks and benefits associated with implementing this technology.

F. THESIS ORGANIZATION

Chapter II is a discussion of CMD technology, implementation strategies, and the Information Systems Strategy Triangle in effort to understand the complexity associated

with implementing this technology. This discussion proceeds on into a discussion about the strategic focus, and plans and policies of the federal government, Department of Defense (DOD), Department of Navy (DON), and the United States Marine Corps (USMC) in order to better understand how the organizational and business strategy should drive the information strategy. Chapter II goes on to discuss the concepts of the sociotechnical systems theory, technology acceptance model, and the confidentiality, integrity, and availability (CIA) triad in order to provide a framework for analyzing the courses of actions developed in Chapter III.

Chapter III provides three separate case studies, which present particular scenarios that could benefit from the implementation of CMD technology through application based access. Each case is described in detail, as are the potential uses of CMD technology in each particular instance. Each case offers three potential courses of action that vary in terms of the implementation strategy and the responsibilities from the perspective of the organization and the end user.

Chapter IV analyzes each case and each course of action with emphasis on the risks and benefits in terms of confidentiality, integrity, and availability from the perspective of the organization and the end user. Using sociotechnical systems theory and the technology acceptance model, this chapter will address the interaction between the technology and the individual of each course of action.

Chapter V is a summary of the research, conclusions, and recommended courses of action for the individual cases. The recommendations will provide the reader a better understanding of the complex interaction between the individual and the technology. Additionally, this chapter offers recommendations for follow-on research in this area of study.

II. LITERATURE REVIEW

The Department of Defense (DOD) looks at information, digital or otherwise, as a strategic asset, which is a characterization of the way the information used and protected (DOD CIO, 2016, p. 2). Certainly any information that is “classified” or that contains Personally Identifiable Information (PII) must be safeguarded from exposure to threats as described in U.S. laws. However, decreasing or limiting availability of data comes at a cost in terms of employee productivity. The current resource limitations and the increasing complexity of the threats faced by the DOD could potentially benefit from the implementation of a new policy that embraces technology available to employees commercially.

A. COMMERCIAL MOBILE DEVICE TECHNOLOGY

The United States Marine Corps (USMC) and the wider Department of Defense (DOD) operate in a resource-constrained environment. One way that the DOD could possibly gain an advantage in this environment is by implementing a policy that allows the use of CMDs, either personally owned or government furnished. For the purposes of this research, CMDs will be defined as set forth in the Department of Defense Commercial Mobile Device Implementation Plan. In this definition, CMDs are described as a “subset of portable electronic devices (PED)” that:

provide one or more commercial wireless interfaces along with a compact user input interface (touch screen, miniature keyboard, etc.) and exclude PEDs running a multi-user operating system (Windows OS, Mac OS, etc.). This definition includes but is not limited to smart phones, tablets, and e-readers. (DOD CIO, 2013, p. 25)

CMDs can vary greatly in computing capacity, operating system, and security capability. For the purposes of this research, CMDs are characterized as having the ability to connect to the Internet, being highly portable, instantly accessible to the user, and having similar processing and data storage capability as desktop or laptop systems at a lower cost (Tucker, 2010, p. 1). Each of these commonalities of CMDs offers potential

benefits to the USMC and DOD in terms of workforce mobility and interconnectedness, but they also have potential negative aspects in terms of security of information.

B. IMPLEMENTATION STRATEGY CATEGORIES

With regard to implementation strategies, four categories of implementation are discussed, each having varying positives and negatives from the point of view of the employee and that of the enterprise. In Gajar, Ghosh, and Rai (2013, p. 64), the authors identified and described each of these implementation strategy categories as Here is Your Own Device (HYOD), Choose Your Own Device (CYOD), Bring Your Own Device (BYOD), and On Your Own Device (OYOD). Each of these categories will be discussed in detail, with the emphasis on the possible benefits to the DOD and USMC from each. These four implementation strategy categories span from low levels of enterprise control to higher levels, and from low employee satisfaction to high employee satisfaction, as displayed in Figure 1.

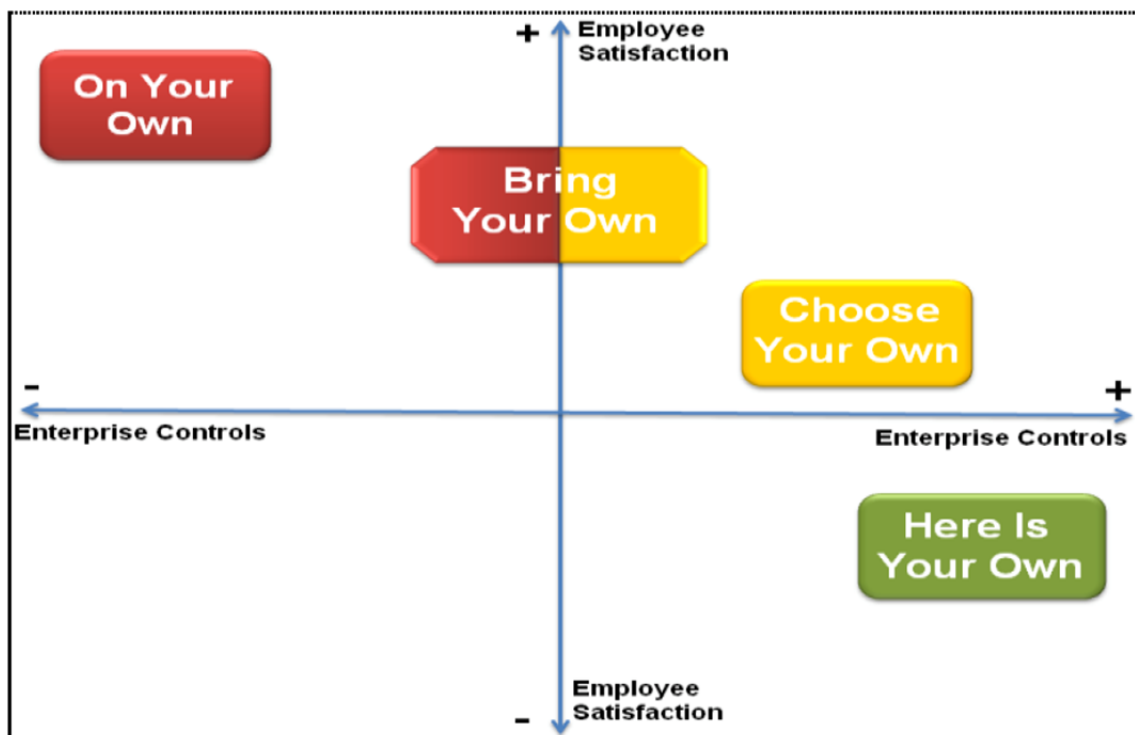


Figure 1. Implementation Categories. Source: Grajar et al. (2013, p. 64).

This research will look at each of these four implementation categories and assess the potential benefits and limitations of each using USMC specific case studies.

a. *Here is Your Own Device (HYOD)*

In this implementation category, the organization is responsible for providing the CMD. The enterprise has complete control over the device in terms of settings and configuration of the device. The organization is responsible for procuring the device, setting up the device, maintaining the device (Grajar et al., 2013, p. 64). From the point of view of the enterprise, this category provides the most control and leads to the best network security, comparatively (Grajar et al., 2013, p. 64). This implementation plan is essentially the same as the current DOD and USMC “privileged user” access program. In this program, “privileged users” are provided government furnished equipment (GFE) if they are identified as “being mission critical or mission essential” (Anderson, 2013, p. 11). In Mercado, and Spain (2014, p. 3), the researchers surveyed over 15,000 Active-duty Army Soldiers on, among other things, their willingness to use an “Army-issued smartphone.” The results showed that 80% of respondents would be willing to use the smartphone. The various activity usages, broken down by age group, are shown in Table 1.

Table 1. HYOD Army Usage. Source: Mercado and Spain (2014, p. 12).

Percentage of Activities Soldiers Reportedly Would Use An Army-Issued Smartphone For By Age

| <i>Variable</i> | <i>Official phone and email</i> | <i>Access to online training</i> | <i>Personal organizing</i> | <i>Social networking</i> | <i>Text messaging</i> | <i>Battle tracking</i> | <i>Access to technical/field manuals</i> |
|-----------------|---------------------------------|----------------------------------|----------------------------|--------------------------|-----------------------|------------------------|--|
| under 20 | 64% | 56.3% | 55.9% | 36.9% | 62.9% | 34.8% | 55.2% |
| 20-24 | 74.7% | 57.9% | 65.6% | 35.2% | 69% | 43.3% | 66.1% |
| 25-29 | 85.9% | 57% | 73.7% | 34.3% | 71.9% | 43.9% | 69.4% |
| 30-34 | 91.3% | 58.7% | 76.9% | 34.6% | 73.2% | 44.9% | 71.9% |
| 35-39 | 93% | 54.7% | 78.6% | 30.6% | 70.7% | 41.2% | 70.2% |
| 40-44 | 93.8% | 52.9% | 76.9% | 28.3% | 69.3% | 37.5% | 64.4% |
| 45-49 | 94.7% | 52.7% | 75.1% | 28% | 69.3% | 37.1% | 63.8% |
| 50 or older | 95.6% | 49.3% | 70.6% | 23.2% | 61.5% | 28.4% | 55.4% |
| Total | 80.1% | 66.9% | 73.6% | 31.9% | 70% | 40.8% | 66.9% |

From a review of Table 1, some interesting insights about potential use of a CMD in a HYOD implementation can be determined. First, the older users (Mid-Grade and up Officers, and Staff Non-commissioned Officers) show a higher percentage use of the CMD for “Personal Organizing” and “Official phone and email,” whereas the younger users (Junior Officers, and Enlisted) show a higher percentage use for “Access to online training.” This insight into usage could transfer over to the other implementation categories. One important consideration is that of “smartphone” ownership among the younger age demographics. In Mercado and Spain (2014, p. 7), the researchers determined that younger users were more likely to own tablet or e-reader, and less likely than their older counterparts to own a “smartphone.” The researchers believed that “smartphone” ownership was lower due to the high cost of service contracts in comparison to income in this demographic (Mercado & Spain, 2014, p. 23). It is not reasonable to expect that everyone owns a CMD, and therefore if a strategy of achieving total workforce mobility is desired, then the government will likely have to furnish devices or provide a CMD stipend to offset the costs to the user.

The expansion of the “privileged user” program to include a larger segment of the total workforce in the DOD or USMC would mean the government procuring a CMD for a larger number of people and then requiring the IT professionals in subordinate units to maintain that equipment. This could result in a considerable increase in cost in initial procurement, personnel training, and maintenance, as well as the commercial cellular access contract. That being the downside of this strategy, the benefit is the amount of security and control that the enterprise would have over those devices. In summary, a HYOD strategy provides maximum control to the enterprise while allowing the employee minimal freedom in choice of CMD, operating system, etc.

b. Choose Your Own Device (CYOD)

In this implementation category, the organization provides a portfolio of devices, and the employees are given the opportunity to choose the device they prefer (Grajat et

al., 2013, p. 64). This strategy capitalizes on the benefits of HYOD, in that the enterprise still has control on the portfolio of devices, and not all devices are allowed. Additionally, the organization owns the devices and still maintains the security and access allowed. This strategy seeks to allow a certain level of choice to the individual employees to pick a device that they are more comfortable or familiar with, in order to encourage employee, use and efficiency on the device. Mercado and Spain (2014, p. 8) reported that the three main smartphone types owned by Active-duty Army Soldiers varied with age, with over half of all younger respondents in each age group owning iPhone devices, and that percentage dropping steadily as age increased, with the Android devices showing greater ownership by older Soldiers. The key take-away from their survey results is that if given a choice no specific device would satisfy all customers; however, a portfolio of choices to include iPhone, BlackBerry, and Android devices would satisfy the vast majority. This strategy would mean additional cost to the enterprise in terms of procuring the devices, as well as additional cost in training and staffing an IT department for the capability of maintaining multiple CMDs, operating systems, configurations, etc. This cost is expected to be outweighed by the added benefit of allowing the employees to pick a device they are more comfortable and/or familiar with.

c. Bring Your Own Device (BYOD)

In this implementation category, the employee is either given some amount of financial resource (stipend) or expected to self-procure a CMD. The key difference from other categories is the employee owns the device, and is able to install software or applications that are not a violation of the organization policies. The employee is expected to maintain the device and the enterprise has less control over configuration, although it still has the ability to enforce standards as a pre-requisite for network access (Grajar et al., 2013, p. 64). The enterprise is still expected to provide some support to the employee in terms of helping the employee with configuration, and troubleshooting hardware-software issues that arise in the use of the device. This is riskier to the enterprise network, because the possible configurations of devices make the possibility of network intrusion much higher.

Naval Postgraduate School (NPS) uses a BYOD strategy allowing students to operate their personal laptops, tablets, mobile phones, etc., on the network. NPS provides support to the students through a self-help wiki website as well as a full staff of IT professionals who have knowledge of the various operating systems and devices commercially available. The students accessing the network are responsible for procuring their own device and complying with usage standards as well as maintaining the currency of the anti-malware software that is provided to them. For those students who do not have the fiscal means to purchase their own device, the school has a limited number of devices to be loaned out as well as community computers available throughout the campus in computer labs and the library.

The NPS BYOD strategy would likely not work on a wide scale in the DOD and the USMC because of the risk potential with regard to personally identifiable information (PII) and unclassified information that is potentially sensitive when aggregated. Some of the potential methods of providing additional security of a BYOD implementation, including the use of applications, trusted platform module (TPM), and virtual desktop infrastructure (VDI), will be discussed in greater detail in this research.

d. On Your Own Device (OYOD)

In this implementation category, the employee is given complete autonomy on the type of and configuration of the device used to access the organizations network. Under this category, the user is responsible for management, maintenance, upgrade cycle, and cost with no support from the organization (Grajcar et al., 2013, p. 64). “No support” is not intended to mean that the organization has no IT personnel; in this case, the organization maintains the network and access to the network. Any CMD implementation policy must be analyzed from the viewpoints of the enterprise and the employee. In some DOD and USMC applications, each of these categories is likely to apply. For example, in the case of USMC’s Training & Education Command (TECOM), an OYOD implementation plan could allow the largest benefit with the least cost. In this case, creating an application, or even a Virtual Desktop that the user could access from their personally procured CMD in order to complete computer based annual training or

Military Occupational Specialty (MOS) training. This specific case will be discussed in greater detail in the following chapters of this research.

C. INFORMATION SYSTEMS STRATEGY TRIANGLE

The Information Systems Strategy Triangle framework as developed by Pearlson and Saunders (2013, p. 24) is an effective way to analyze the interaction between the business, organizational and information strategies in an organization. The use of the triangle is important, because it shows how a change in any of the individual strategies has effects on the other strategies. The triangle is organized with the business strategy at the top of the triangle to show that under optimal circumstances it will be the overarching strategy, with the authors asserting that “successful firms have an overriding business strategy that drives both organizational strategy and IS strategy” (Pearlson & Saunders, 2013, p. 24).

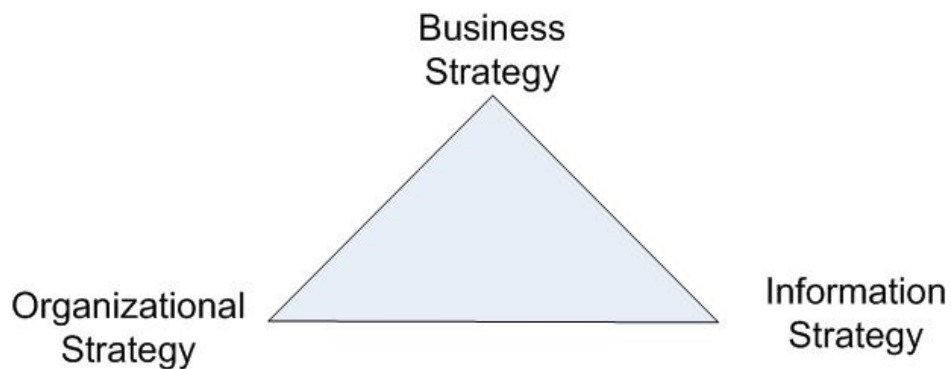


Figure 2. The Information Systems Strategy Triangle.
Source: Pearlson and Saunders (2013, p. 24).

Pearlson and Saunders (2013, p. 27) define the business strategy as “a plan articulating where a business seeks to go and how it expects to get there.” For the DOD this strategy comes down from the president through the National Security Council and is filtered through the echelons of command into what individual organizations within the DOD seek to accomplish and how they intend to accomplish their goals. The organizational strategy describes the design of the organization, how decisions are made in the organization, how coordination is accomplished, and how the work processes are

controlled (Pearlson & Saunders, 2013, p. 33). The DOD is recognized as highly hierarchical in its organization, but decision authority can be de-centralized in many cases, and collaboration and liaison between entities in the organization can vary greatly from unit to unit. Due to this organizational complexity, “one-size-fits-all” initiatives do not always succeed, and therefore individual organizations strategies must be considered when analyzing the Information Systems Strategy Triangle for CMD implementation.

The information strategy is defined as “the plan an organization uses to provide information services” (Pearlson & Saunders, 2013, p. 36). In the DOD, this strategy is found in various plans/policies/directives/instructions as published by the DOD CIO and subordinate CIO’s or IT professionals.

Misalignments between the two or more points of the triangle can lead to adverse effects on the strategy. In Shives and Pelz (2012, p. 69), the authors looked at the issue of organizational culture and structure, specifically the relationship between HQMC C4 and the acquisition process within the Marine Corps and how that relationship affects IT changes. Their research ultimately determined that significant issues exist in the relationship between HQMC C4 and the organizations responsible for acquisition of IT resources. These authors specifically determined that while HQMC C4 is responsible for developing and implementing the information strategy from the business strategy of the Marine Corps, HQMC C4 is not formally included in the acquisition process due to the organizational strategy. The authors found that this issue could lead to the acquisition of information technology systems that were not aligned with an information strategy that supports the business strategy (Shives & Pelz, 2012, p. 69). This is an example of how a misalignment between the business strategy and the organizational strategy affects the ability to successfully carry out the information strategy. Marine Corps-specific implementation would require policy change from HQMC C4; however, the structural issues, personnel, and political issues regarding acquisitions could impact implementation. The business strategies, organizational strategies, and information strategies of the DOD that are relevant to CMD are discussed in greater detail in the following section.

D. INFORMATION SYSTEMS STRATEGY AND POLICY IN THE DOD

The United States Marine Corps (USMC) and the wider Department of Defense (DOD) operate in a resource-constrained environment (Nally, 2013). These resource-constraints carry over into the information technology (IT) in the form of fewer and older computing devices. In many cases, the number of Marines and Sailors in an operational unit can greatly outnumber the computers and Internet connections assigned to that unit. These computing devices vary in age and capability from unit to unit. Equipment upgrade and replacement timelines are a function of the budget cycle as well as the government acquisition process. These IT systems must be seen as a capability multiplier that allows the warfighters to train, equip, and complete the missions that support the strategic focus of the president, down to the Combatant Commanders. The following subsections will address the strategic focus as well as the many different directives, instructions, and memorandums that govern and direct the use and implementation of IT systems in the DOD.

1. Current Strategic Focus of DOD/DON/USMC Applicability

The strategic focus of the DOD was developed by the Joint Chiefs of Staff (JCS) following a review of the guidance that is set down by the president and the National Security Council (NSC). These strategic focuses are intended to influence the operational level and tactical level focus in order to achieve a strategic goal or end-state. As such, the strategic level focus will not specify a particular information technology strategy that should be pursued; rather, the guidance must be derived through an understanding of the capability increase that certain elements of IT may provide. Connecting that potential increase in, or added capability to, a strategic area of focus is important to justify the allocation of resources to the pursuit of an IT strategy.

a. Department of Defense (DOD) Areas of Focus

The National Security Strategy as developed by the president and the National Security Council lays down the overall strategic focus for the country (White House, 2015). This strategy is then reviewed by the JCS and developed into the National Military Strategy (Chairman Joint Chiefs of Staff, 2015). The Secretary of Defense (SecDef)

developed the Quadrennial Defense Review (Secretary of Defense, 2014) in order to shape the focus of the DOD. In the National Security Strategy, the president described the focus as increasing security and prosperity through the use of all the resources of the United States government to include the DOD (White House, 2015).

The National Military Strategy (2015) discusses the need to seize on innovation and efficiencies that will allow the achievement of the strategic objectives. This strategy recognizes inherent resource shortfalls that occurred due to budgetary constraints as well as the vigorous deployment cycle of the recent future. The need for greater effectiveness and efficiency in order to achieve better preparation to conduct the required missions of the DOD is a common theme of this strategy (Chairman Joint Chiefs of Staff, 2015). The greater implementation and usage of IT solutions has the potential to help achieve better effectiveness and efficiency for the DOD while addressing some of the budgetary constraints that are likely to occur into the future.

In the Quadrennial Defense Review(QDR), the SecDef discusses many of the same issues as the president and JCS such as the need to overcome the budgetary shortfalls and achieve greater efficiency. The QDR describes the need for greater capability and readiness by the DOD in order to meet the strategic focus, specifically looking at modernization and a rebalance of the force to decrease unneeded infrastructure (Secretary of Defense, 2014). A shift in IT strategy has the potential to decrease infrastructure, and increase the effectiveness and efficiency of the force in the future.

b. Department of Navy (DON) Areas of Focus

The previously discussed strategies from the DOD leadership are further digested and developed into a more Department of Navy-focused strategy, as laid out in the Cooperative Strategy for 21st Century Sea power (Secretary of the Navy, 2015). In this strategy, many of the main areas of focus from the higher echelon strategies are discussed with a greater focus on how the Navy, Marine Corps, and Coast Guard are expected to utilize their unique capabilities. One main point of this strategy is the need to maintain throughout the force a high level of readiness to deploy rapidly to respond to crisis. Additionally, this strategy prioritizes affordability and cost control in order to meet

budget shortfalls (Secretary of the Navy, 2015). In terms of adding capability, this strategy discusses the need to capitalize on the strategic and intellectual capital of the service members, which has the potential to benefit from the greater proliferation of and usage of mobile devices and specific applications within the DOD.

c. *Marine Corps Areas of Focus*

In terms of the strategic focus of the Marine Corps, the most recent plan is Expeditionary Force 21 (EF21) (Commandant of the Marine Corps, 2014). The Marine Corps prides itself on being expeditionary, amphibious and on the front lines of any conflict that arises. Maintaining high readiness levels, and being prepared to deploy to any point of friction quickly in order to achieve the designated objectives is the primary focus of the Marine Corps. EF21 specifically describes an intent to improve training and organization capability within the Marine Air Ground Task Force (MAGTF). It also specifically lays out the intent to enhance capability with regard to social media, information technology, and cyberspace capabilities (Commandant of the Marine Corps, 2014, p. 11). These areas of focus are, as discussed above, capable of achieving success through the implementation of CMD technology in the MAGTF.

2. *Plans and Policies*

In order to understand the many plans, policies, directives, and instructions that must be followed in the implementation of any Commercial Mobile Device (CMD) that may access DOD information and/or operate on a DOD network, this research begins with an examination of the Federal Chief Information Officer (CIO) level issuances and then proceeds down the levels of command to the Marine Corps CIO.

a. *Federal CIO*

In *Digital Government: Building A 21st Century Platform to Better Serve the American People* (Federal CIO, 2012), the Federal CIO along with the president recognize that technology, and more specifically mobile technology, is an opportunity and a challenge. The Federal CIO acknowledged that “early adopters” within the government were working toward innovation in mobile usage, but that no over-arching

policy or strategy was in place to ensure that innovations were able to apply across the disparate organizations of the federal government.

Digital Government (Federal CIO, 2012) established unifying strategy objectives for all of the federal government to enable the mobile workforce to access government information “anywhere, anytime, on any device.” It recognizes “customer-centricity” and “security and privacy” as two of the major principles of achieving the strategy objectives. The Federal CIO explains that the focus should be on mobility and not necessarily mobile technology in this way:

Mobility is not just about embracing the newest technology, but rather reflects a fundamental change in how, when, and where our citizens and employees work and interact. Mobile technology-the devices, infrastructure, and applications required to support a mobile citizenry and workforce-is a critical enabler of mobility, but is only part of the profound environmental shift that mobility represents. (Federal CIO, 2012, p. 14)

This focus on mobility rather than the specific technology is an important concept that will be discussed in greater detail in the development of the case studies for this research.

b. Department of Defense (DOD)

The Department of Defense, and more specifically the DOD Chief Information Officer (DOD CIO) has the overall responsibility for the coordination of information technology between the organizations that make up the DOD. The DOD CIO issues the plans and policies that describe the development of and use of information technology to meet the needs of the greater DOD. The policies and instructions developed by the DOD CIO are more generic in nature and are intended to address issues related to the interoperability of DOD IT systems as well as the confidentiality, integrity, and availability issues common to all subordinate agencies. Interoperability is recognized by the DOD CIO as imperative to the successful implementation of any IT system in the current joint, interagency, and/or multinational operating environment (DOD CIO, 2014a, p. 3). For the purposes of this research, any systems that “receive, process, store, display, or transmit DOD information” are considered DOD IT systems (DOD CIO, 2014b, p. 2).

(1) DOD Commercial Mobile Device Implementation Plan

The DOD Commercial Mobile Device (CMD) Implementation Plan (DOD CIO, 2103) discussed the need for a phased approach to implementing CMDs in the DOD. It specifically discussed the belief that greater mission effectiveness can be achieved through the development and proliferation of what it called “secure commercial mobile applications.” The plan goes on to describe the four priorities, in terms of unclassified access, which the DOD CIO plans to pursue (DOD CIO, 2103).

The first is priority dealt with providing infrastructure for wireless services. This is further described as acquiring contracts for carrier services, monitoring and managing the use of those services, and implementing a Mobile Device Management (MDM) system to ensure maintenance and security. Also described is the desire to consider infrastructure options that reduce costs “to the greatest extent possible.”

The second priority dealt with the need to determine what devices can meet the requirements threshold, in terms of capability and security, and then to approve those devices for acquisition and distribution to the forces.

The third priority discussed the need for a development and certification process of mobile applications that may access DOD information and networks, with the main focus of this priority being the interoperability of applications with various operating systems.

The fourth priority focused on the need to protect and secure the DOD information environment through security approval processes, continuous monitoring to ensure policy and configuration compliance, as well as classified CMD plans which goes beyond the scope of this research (DOD CIO, 2013).

The “Future Capability” section of this plan discussed the desire to possibly implement a Bring Your Own Device (BYOD) style program that is more like the ones in use in the commercial business sector. It went on to describe that this future desired capability, while possibly beneficial, is prevented by DOD policies and the potential security vulnerabilities. The plan also described that through the use of Virtual Desktop Infrastructure (VDI), or Trusted Platform Module (TPM) (either through software or

hardware) the DOD may be able to realize the benefits of BYOD in the future (DOD CIO, 2013). This research will go into more detail on these solutions and their possible use.

(2) DOD Mobile Device Strategy

In the DOD Mobile Device Strategy (2012, p. 1), the DOD CIO recognizes mobile nature of the DOD workforce. Mobile devices are recognized as improving the productivity, and situational awareness of individuals to include members of the DOD.

The increasing use of social media, smartphones, and tablet computers has made information sharing an expectation. Our challenge today is ensuring our networks can securely support the information demands of our users – users who require access to information anywhere and anytime across the DOD Information Enterprise, allowing them to make informed decisions in the execution of their missions. (DOD CIO, 2012, p. 2)

This statement by then DOD CIO, Teresa M. Takai, described the demand for mobility, interoperability as well as security in DOD IT systems.

The first goal described in this strategy discussed the need to further develop enterprise infrastructure to support mobile devices, which has a potential to decrease overall infrastructure costs in terms of government owned and furnished computers and mobile devices. Much like the previously discussed plan, this strategy recognized the inherent security issues with mobile devices and the need for Public Key Infrastructure (PKI) security to control access (DOD CIO, 2012, p. 3).

The second goal described in this strategy recognizes the need for formalized policies and standards governing the use of mobile devices on the network. Recognizing that most CMDs are not appropriately equipped (in terms of security controls, access protocols, etc.) for use on a DOD network, this strategy discussed the need for required standards in addition to a streamlining of the process to approve CMDs (DOD CIO, 2012, p. 3). Central to achieving this goal, the strategy recognized the need for appropriate workforce education and training in order to mitigate potentially hazardous employee behavior and practices.

The third goal described in this strategy is the need for mobile and web-enabled applications to provide increased functionality to the users (DOD CIO, 2012, p. 4). This topic will be discussed in greater detail in this research.

One of the main considerations of this implementation strategy is the need to identify the type of user using the device and the level of access that is required by that user. This research is focused on Unclassified Non-Sensitive information access for personal CMD. User categories, the level of access required, and the considerations the DOD CIO recognizes as needing to be addressed in the implementation of mobile devices are shown in Figure 3.



| User Category | | Implementation Considerations | | | |
|------------------|---------------------------|---|---|--------|------------|
| | | NON-SENSITIVE | CUI | SECRET | TOP SECRET |
| Enterprise-wide | Security |  |  | | |
| | Transport | | <ul style="list-style-type: none"> • Encryption • Federal Information Processing Standards | | |
| | Gateways | | <ul style="list-style-type: none"> • Broadband service • Quality of service | | |
| | Mission Critical Services | | <ul style="list-style-type: none"> • Interoperable access • Redundancy • Cross domain support | | |
| | Mobile Device Management | | <ul style="list-style-type: none"> • Low latency • High availability • Robust cellular roaming / persistent connectivity | | |
| | Application Management | | <ul style="list-style-type: none"> • Auditing • Data-at-rest / data-in-transit encryption • Remote wipe • Strong authentication • CMD peripheral control (Camera/GPS/Wi-Fi/etc.) | | |
| Executive | | <ul style="list-style-type: none"> • Approved commercial apps • Application control | <ul style="list-style-type: none"> • Validated apps • Application authorization • Centralized app store | | |
| Executive | | <ul style="list-style-type: none"> • Network control | <ul style="list-style-type: none"> • Priority access • Gateway(s) to C2 networks | | |
| Tactical Support | | <ul style="list-style-type: none"> • Network control | <ul style="list-style-type: none"> • Ruggedized device • Delay tolerant networking • Selective availability anti-spoofing • Transmission security • Anti-jam | | |
| Tactical Support | | | <ul style="list-style-type: none"> • Spectrum • Interoperability • Phase of conflict • Removal of fixed infrastructure vulnerability | | |

Figure 3. Implementation Considerations. Source: DOD CIO (2012, p. 6)

This research will address several of these Non-Sensitive Implementation Considerations at the Enterprise-wide User Category level, recognizing that the current state of mobile device technology and the budgetary constraints in the DOD will have an impact on the overall strategy.

c. Marine Corps

The Marine Corps Commercial Mobile Device Strategy (2013) is one of the main driving factors behind conducting this research. In this strategy, Headquarters Marine Corps (HQMC) established the current approach regarding research and development of technology and policies to determine the level of implementation that should be pursued regarding the use of personally procured mobile devices. It highlights several of the currently understood issues with implementation as well the anticipated benefits. The anticipated benefits are limited and based on an understanding of the benefits other organizations have seen. This strategy also establishes the USMC definition of a CMD as:

a handheld computing device with a display screen that allows for user input (e.g., touch screen, keyboard). When connected to a network, it enables the sharing of information in formats specially designed to maximize the use of information given device limitations (i.e., screen size, computing power). (Anderson, 2013, p. 4)

This strategy additionally looks at the “way forward” for the USMC as establishing a secure mobile framework (SMF). It goes on to specifically state developing BYOD as one of the ways the USMC will achieve SMF. This strategy sets a goal of establishing a mobile environment that allows personally owned CMDs to access “controlled unclassified information (CUI),” recognizing the potential benefit in terms of “cost efficiency and increased worker effectiveness.” Additionally, it recognizes that “legal ownership rights,” and the “security of the MCEN” are challenges that will need to be addressed in order for SMF to be realized in the USMC (Anderson, 2013, p. 10). Figure 4 graphically displays how, at a very high level, the USMC will develop policy, streamline procurement and testing, develop mobile applications and mobile infrastructure, all in order to optimize operations (Anderson, 2013, p. 6).

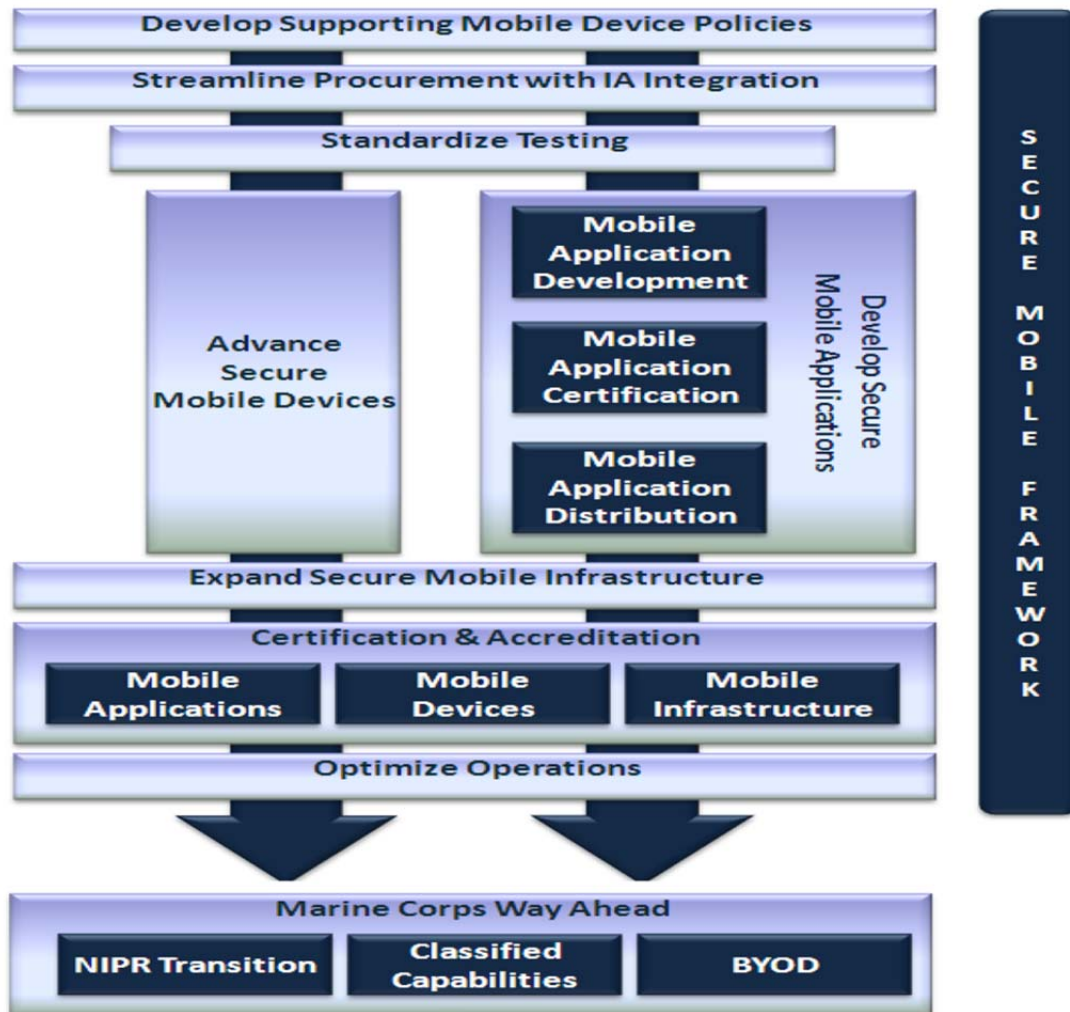


Figure 4. Secure Management Framework, Source: Anderson (2013, p. 6)

This research is specifically intended to look at the “Optimize Operations” portion of SMF with the assumption that mobile applications and infrastructure can be developed and appropriately secured.

E. SOCIOTECHNICAL SYSTEMS THEORY

In order to analyze the impact on the DOD and USMC workplace, the intersection of the workforce and the technology must be examined. One recognized method of conducting this analysis is to use the sociotechnical systems (STS) perspective, which enables analysis of the organization (in this case the DOD, USMC, smaller unit, etc.)

from a social and a technical standpoint (Bostrom & Heinen, 1977). STS theory starts with a premise that “Work organizations exist to do work” and that work involves people (inherently social creatures) and technology (computers, machines, tools, etc.) to complete the specified “work” (Trist, 1981, p. 10). STS theory recognizes that technological innovations are unlikely to be successfully integrated into an organization unless the organization changes and adapts to the new technology (Bostrom & Heinen, 1977, p. 17). Therefore, the worker and the technology cannot be examined separately, but must instead be analyzed at the intersection between the two in order to optimize their interaction.

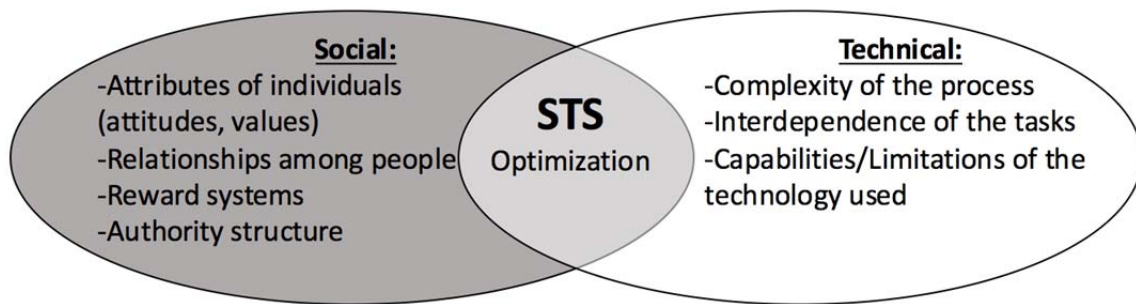


Figure 5. Sociotechnical Systems Theory. Adapted from Bostrom and Heinen, (1977, p. 17).

STS theory can also lead to an understanding of why the DOD CIO and leadership within the DOD desires to look into implementing policies that will allow CMD in the DOD workplace. In Geels (2004, p. 911), the researcher determined that as availability of a technology increased, and as workers saw their peers in other agencies and organizations using the technology, a greater desire for a similar capability in their own organization was present. Additionally, the more highly proliferated the technology was, the better the understanding of and familiarity with that technology within the workforce, and the more that technology was improved upon (Geels, 2004, p. 911).

Looking at a newly introduced technical innovation in the workplace from a social standpoint, it can be determined that the organization will be made up of at least

some people that do not want the new technology implemented and will either be overtly or covertly resistant to the implementation. These individuals are usually in positions within the organization that will realize some loss of status, budget, authority, etc., due to the change. Trist (1981, p. 46) recognized that in these situations, the optimization of STS must address this perceived or actual loss by these individuals with “sharing of power” in order to minimize their resistance. This research will use STS theory in order to analyze the CMD implementation case studies to determine the potential benefits and issues that are likely to arise from both a social and technical standpoint.

F. TECHNOLOGY ACCEPTANCE MODEL

In addition to looking at the optimization between the social and technical aspects of the organization, this research will look at how human behavior and individual perception can impact the successful implementation of a CMD policy in the USMC. To conduct this analysis, the Technology Acceptance Model will be used, which attempts to look at how external factors affect internal beliefs and attitudes thereby determining an individual’s intentions with regard to adopting a technology (Davis, Bagozzi, & Warshaw, 1989, p. 985). The two key factors that will be analyzed in this research are the “Perceived Usefulness” and the “Perceived Ease of Use,” and how those two factors will affect user acceptance of a CMD usage policy in the individual case studies.

The extent to which an employee believes a particular technology will aid in the performance of their duties is referred to as “Perceived Usefulness,” and this factor has direct influence on how willing that employee is to adopting and using that technology (Davis, 1989, p. 320). In addition to this factor, is that of “Perceived Ease of Use” which refers to the employee’s perception of how difficult the technology will be to learn to operate and integrate into their performance of duties (Davis, 1989, p. 320).

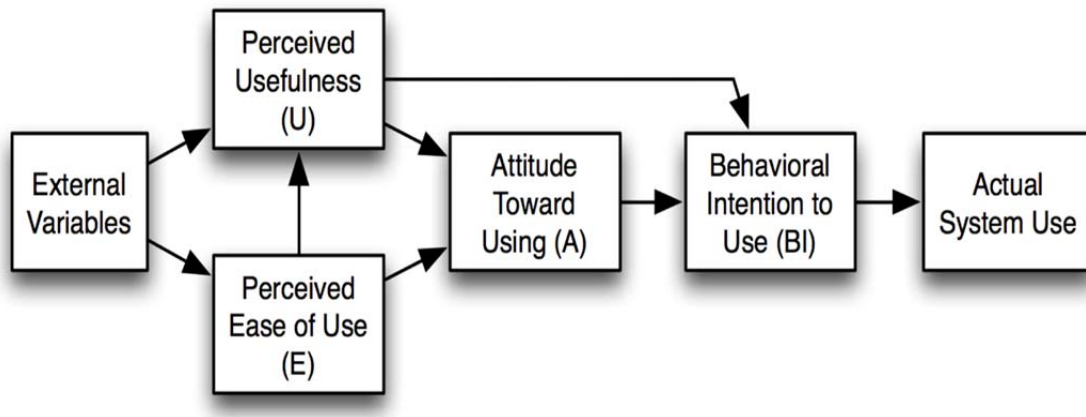


Figure 6. Technology Acceptance Model. Source: Davis et al. (1989, p. 985).

This figure displays that “Perceived Ease of Use” is compared by the individual to “Perceived Usefulness” and an internal “Cost Benefit Analysis” is conducted to determine the “Attitude Toward Using” that technology. This internal analysis by the individual all leads to the individual determining their “Behavioral Intention to Use” and that leads to “Actual System Use” by the individual of that technology. The intent of the Technology Acceptance Model is to look at all of these factors in order to make a reasonable estimate of how technology will be accepted or rejected by the users within an organization (Davis et al., 1989, p. 985). The research conducted by Davis et al. (1989, p. 997) determined that the most influential factor is “Perceived Usefulness” in predicting the individual’s intention to use a particular technology.

With this insight, the case studies developed in this research, and the policy implementation recommendations made will focus on the maximizing this factor as well as attempting to minimize the perceived difficulty of use in the eyes of the individual that is the target “end user” for each case. This research will look at both of these key factors from the perspective of the “end user” in the case studies as well as the perspective of the IT professionals at the unit and higher headquarters levels.

G. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA) TRIAD

The Federal Information Security Management Act (FISMA) of 2002, established the baseline definition of information security as “protecting information and information

systems from unauthorized access, use, disclosure, disruption, modification, or destruction.” From this definition, FISMA (2002) lays out the three tenets of information security, confidentiality, integrity, and availability, which are commonly referred to as the CIA Triad, displayed in Figure 7.



Figure 7. Confidentiality, Integrity, and Availability (CIA) Triad.
Adapted from (FISMA, 2002).

FISMA defines the three tenets of the CIA Triad as follows:

Tenet 1: Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. (FISMA, 2002)

Tenet 2: Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. (FISMA, 2002)

Tenet 3: Availability, which means ensuring timely and reliable access to and use of information. (FISMA, 2002)

These definitions provide the baseline for how information security will be analyzed with regard to the case studies developed in this research. The FISMA definition for information security and the sub tenets are fairly generic. Malcom Harkins,

Chief Information Security Officer of Intel Corporation in 2010, discussed the topic further in his six irrefutable and unwritten laws of information security as follows:

Users want to click; when connected to the Internet, people will click on things. Information wants to be free; people are prone to talk, post, and share. Code wants to be wrong; a software program can never be 100 per cent error-free. Services want to be on tap; some background processes will always have to be switched on. Security features are double-edged; they help and they also harm. People set and forget; the efficacy of a control deteriorates with time. In such a context, compromise is inevitable for CIO's. (Chandrasekhar, 2013, p. 2)

With the FISMA definitions and these “unwritten laws” a basis for analysis and evaluation of past, present and future IT policy implementations with regard to information security is present. The individual case studies in this research will look at specific CIA Triad issues and solutions regarding specific implementations of CMD on a government network. The following sub-paragraphs will serve as a brief discussion of the research on general CIA Triad issues of CMD implementation and the solutions that address those issues.

1. General Issues

In a DOD CIO Memorandum (2006), the issue of the security of unclassified sensitive DOD data on portable computing devices is recognized as a potential hazard to confidentiality. CMD are commercially available devices that are designed for mobility, which makes them vulnerable to theft or loss. In a DOD CMD implementation, the device is likely to connect to multiple wireless access-points, including those access-points that are not controlled and maintained by DOD IT professionals. These access-points could potentially provide opportunities for malicious actors to gain remote access to a CMD and then, in certain implementations, gain access to government networks and data. The employees that own and operate the CMD can be targeted for phishing, spam, whaling, downloading malware, and even intentionally disclosing sensitive government information. Employees have done these things on government networks using government equipment, and it can reasonably be expected that similar incidents are likely to occur if CMDs are given access to government networks. These issues are the same as

those experienced in the commercial sector in implementing CMD access policies. Using some commercially available technology solutions as well as well-developed user agreements and holding individuals accountable for their behavior has allowed government organizations and commercial organizations to realize the benefits of CMDs in the workplace while mitigating many of the risks. The key point that needs to be considered is that the risks cannot be eliminated and the solutions described in this research are capable only of managing and mitigating risk to an acceptable level.

2. General Solutions

The key to solving the CIA Triad issues of implementing CMD in the DOD is to look at the social and technical issues in order to develop an overall strategy that mitigates the risk of each. The technical solutions are numerous and vary based on the confidentiality required by law, and the level of integrity and availability that is required to achieve success.

One of the most common ways of addressing issues with CMD on an enterprise network is the use of virtualization technology to mitigate and compartmentalize risk to the enterprise. In Jaramillo, Katz, Bodin, Tworek, Smart, and Cook (2013) the researchers looked at developing separation between the user and the enterprise in order to provide protection to both. Their research looked at specific software applications that could be used to provide this protection, as well as what software and hardware combinations worked best to provide security to both user and enterprise. Virtualization technology has the ability to allow the workforce to remotely access a virtual desktop on the enterprise network and to carry out their duties from any location. Additionally, virtualization has the ability to prevent some of the ability for DOD data to be stored on a personal CMD. The Jaramillo et al. (2013) research is important in looking at how the DOD could appropriately compartmentalize access to its networks in order to more securely allow limited CMD access. In Lennon (2012), the researcher studied the implementation of BYOD at the Letterkenny Institute of Technology in Ireland. In this research, the author described how Cloud Computing was used with BYOD to create a Virtual Learning Environment. This research is important as a means to understanding

what technology is available to improve training and education systems availability to the workforce, which will be addressed in a follow-on case study of this research.

Another technology that has been used to maintain information security in an environment in which CMDs are able to access the organization network is trusted platform module (TPM). Under this system, the integrity of the device attempting to access the network is assessed and devices that do not conform to the established standards in terms of software installed and system settings applied are denied access to the network (Costantino, Martinelli, Saracino, & Sgandurra, 2013). Costantino et al. (2013) described the use of role-based access control systems in providing security. Their research looked at restricting system access based on the user, and administrator set permissions. Establishing the restrictions on the user will be essential in order to provide the needed security for the Marine Corps in any implementation of using personally procured mobile and computing devices. In Armando, Costa, and Merlo (2013), the specific issue of securely implementing BYOD with an Android device was addressed. Their research was limited to Android devices, which while popular in the DOD, do not represent the majority of devices that DOD personnel desire to connect to the network as shown by Mercado and Spain (2014). TPM along with other technology will likely be needed in order to appropriately secure access from CMD accessing a DOD network.

The DOD currently uses the Public Key Infrastructure (PKI) technology in order to authenticate users on government furnished IT systems. The Common Access Card (CAC) is a device that allows the workforce to access PKI enabled systems, websites, etc. The DOD CIO Memorandum (2006) described the use of PKI in order to secure the “Data at Rest” on personal CMD.

Application based access is another way that the commercial sector uses to compartmentalize IT systems from the threats CMD access presents to their networks. Intel Corp. determined that apps that made the appropriate data available to the users that needed that data achieved the greatest success for their company (Chandrasekhar, 2013, p. 4). For certain situations within the DOD, application-based access is likely all that is needed in order to allow secure access to a DOD network. In these cases, only the

information that is needed or allowed to be accessed is displayed in the application interface. The user has limited, if any, ability to make changes to the organization's data, and permissions can be tightly controlled when combined with other technological means. The case studies developed in this research will look at the potential for application-based access to optimize operations, while mitigating risk to the network.

Behavioral changes are necessary for the successful implementation of the use of CMD. In Barkhuus (2005), behavioral issues were observed when implementing BYOD for education. Primarily this research focused on the issue of student attention when using BYOD in an actual classroom. This research will be applied to developing the implementation plan for the proposed case studies. Additionally, Intel Corporation's IT professionals raised the concern that productivity would be negatively impacted due to employees making the personal decision to use their devices for non-work-related activities and accessing the applications on the device that provide no value added to the company during work hours (Chandrasekhar, 2013, p. 2). This is a social issue that will need to be addressed through training, and supervision by the DOD and the USMC in order to mitigate the risk that the worker presents to the network.

During its implementation of CMD policies, Intel's research determined that only 30% of its employees were accepting of the company accessing the information on their personal devices; however, employees were almost unanimously in favor of Intel managing security of their CMDs while also completing necessary training (Chandrasekhar, 2013, p. 3). Essentially, the IT professionals tasked with spearheading any CMD implementation plan will need to be aware of the inherent social/behavioral issues. Appropriate supervision and training, in addition to technological safeguards, will help to limit the CIA Triad issues of implementing a CMD policy.

H. PREVIOUS CASE STUDIES AND RESEARCH ON CMD IMPLEMENTATION POLICY

The issues of CMD implementation have not stopped or stalled the movement in the commercial sector, education, and even some government organizations. Each of

these examples shows how using various technology and behavior policies have been successful in increasing the mobility of their end-users.

1. CMD in Commercial Sector (Intel Corporation)

In 2010, Intel Corporation had nearly 80,000 employees worldwide, and nearly 10,000 of them were already using their personal CMDs to work. The Chief Information Security Officer, Malcom Harkins, was faced with the challenges of determining how to gain a competitive advantage from employees using these devices, how to ensure the security of corporate data, and how to deal with the ownership of Intel Corp. data present on privately owned devices (Chandrasekhar, 2013, p. 1). The DOD is wrestling with many of these same issues as Intel Corp. in terms of how CMDs may be used to improve efficiency, and reduce operating costs while also addressing the potential security issues.

Another issue Intel discovered was personal data stored on a personal CMD used at work and the legal issues in the event of loss, theft, or device security compromise. Intel recognized the legal issue regarding data encryption or implementing a remote-wipe capability on an employee's CMD (Chandrasekhar, 2013, p. 7). Remotely wiping an employee's device would ensure that sensitive company information was safe from exposure; however, this would also ensure that the employees' personal data on that device was removed. This Intel Corp. case study will be used in this research to display the struggles that are likely to occur in implementing a CMD access policy in the DOD and USMC.

2. CMD in Government

Implementing CMD access to government networks is not a new idea, but it has yet to be attempted on a large scale in the DOD. Several government organizations have developed policies for and allowed access to their networks to worker-owned CMDs.

a. Alcohol and Tobacco Tax and Trade Bureau (TTB)

In order to reduce costs in terms of acquisition and maintenance of workforce computing capability the TTB has embraced the use of Virtual Desktop Infrastructure (VDI) in order to allow CMD usage (White House, 2012). The TTB recognized that its

workforce was highly dispersed, with over 80% teleworking, at a nearly \$2 million cost to regularly replace and update their employees' desktop and laptop IT devices (three- to four-year replacement cycle). TTB's implementation of VDI saved the organization nearly \$1.2 million in these infrastructure costs, while also increasing the mobility of its workforce. As a result of its implementation policy, the TTB has seen the program expand to a point where 70% of its personnel are using CMD to conduct their daily duties. The main lessons learned from the TTB implementation are that VDI helps to mitigate the financial risks associated with the rapid pace of technological change in CMDs, as well as insulates the organization by not allowing organizational data to reside on the personal device (White House, 2012).

b. U.S. Equal Employment Opportunity Commission (EEOC)

Similar to the TTB, the EEOC was under budgetary constraints that necessitated a shift in their IT policy. Their implementation policy focused on the use of third-party software, in the form of mobile device management (MDM) software, which allowed the EEOC to enforce security settings and remotely wipe the devices in the event of theft or loss. This policy allowed their employees to bring their personal CMD and access the organization network as long as the user was in compliance with an acceptable use policy and the device was in compliance with the MDM.

The EEOC was able to cut its infrastructure costs and increase the mobility of its workforce through the implementation of a CMD access policy. The main lesson learned from the EEOC implementation were that legal counsel should be consulted early and often to protect the organization and ensure the legality of any user policy developed (White House, 2012). This will be important for any DOD or USMC implementation policy, as the DOD is subject to Freedom of Information Act (FOIA) requests, and other government records audit laws.

c. State of Delaware

In dealing with an aging portfolio of BlackBerry devices, the State of Delaware made the transition from organization furnished devices to a BYOD program for certain employees. Delaware recognized that "many employees carry personal devices in

addition to the state issued device” and that employee efficiency and cost savings could be realized through allowing employees to use their personal device for work.

The key challenges that Delaware faced included legal questions about taxability of the employee reimbursements (for wireless costs) as well as the FOIA request issues, similar to the TTB and EEOC cases. These issues were ultimately addressed to a satisfactory level, and the State of Delaware was able to reduce expenses related to devices by 45%. Delaware limited the reimbursement program to employees who are “out of the office on business 50 or more annual days,” whose “duties require them to be contacted anywhere/anytime,” and who have “24/7 response requirements” (White House, 2012). The employees in this program have similar job duty requirements to many DOD employees, and therefore may be a good target group for the DOD in a CMD implementation pilot program.

The State of Delaware case is particularly applicable to this research because the DOD and, more specifically, the USMC are currently looking at how to deal with the costs of an aging BlackBerry device portfolio. It is important to note that the State of Delaware made the BYOD policy open to all employees, but only reimbursed expenses to the employees who met the previously stated requirements.

3. Previous Research on CMD in DOD

Similar to the issues faced by the previously described government agencies, the USMC and the DOD in larger part will need to determine how best to deal with ownership of devices, reimbursement, FOIA requests, remote device wiping, and employee behavior. In the research done by Wedel and Michalowicz (2015), the researchers looked at some of the legal, technical, and security issues with BYOD in terms of developing a user policy that could be used by the Marine Corps. Their research was primarily focused policy issues, and looked at three implementations of BYOD in government and commercial business organizations. It was their determination that a carefully crafted user agreement could protect the organization and the individual while realizing the benefits of BYOD for the workforce (Wedel & Michalowicz, 2015, p. 91).

The issue of policy and policy development for incorporating secure smartphone technology in the USMC was researched by Epstein (2014). Epstein (2014, p. 76) was able to determine that significant benefits in terms of efficiency and effectiveness were possible through the use of a hypothetical secure smartphone in a tactical situation for the USMC. However, through analyzing current policy in the DOD, Epstein (2014, p. 76) determined that current policies are unable to list the vulnerabilities associated with the numerous hardware/software configurations. This results in a potentially unacceptable level of risk with regard to implementing these devices, based on the current technology and policies. In Adkison (2015), the topic of mobile application development for use on CMDs in a tactical USMC unit was looked at. Adkison (2015) looked at the utility of enterprise mobile applications for aviation, healthcare, document management, as well as more military specific applications for fires, reporting, and information sharing. The determination was that the USMC could benefit from the use of mobile applications, and that additional research was needed in terms of the security and connectivity of mobile devices in a tactical environment (Adkison, 2015, p. 72). The issue of smartphones in tactical situations is beyond the scope of this research.

The gap in the previous research is that implementing a CMD access policy is an information strategy, as described in The Information Systems Strategy Triangle framework developed by Pearson and Saunders (2013, p. 24). The research tends to focus on this one portion of the triangle; it does not look into how this information strategy will affect or be affected by the business and organizational strategies. The previous research seems to be based on the notion that the implementation of a CMD access policy in the Marine Corps is inevitable, and the business and organizational issues will need to adapt.

I. SUMMARY

The focus of this research is on better understanding the implications of using CMDs in the DOD in order to allow senior leaders within the DOD to better determine if these policies should be pursued, rather than viewing the change as inevitable. The business strategy, organizational strategy and the informational strategy of the Marine Corps will be analyzed in specific case studies to understand their alignment or disparity.

Using sociotechnical systems (STS) theory and the technology acceptance model (TAM) this research will look at these cases to understand the potential issues of implementing a new policy regarding CMD usage by the workforce as well as potential solutions to those issues.

III. METHODOLOGY

This research is a series of three qualitative case studies on the implications of creating a new information technology strategy within the United States Marine Corps (USMC) that allows the use of Commercial Mobile Devices (CMD) by the workforce to connect to and interact with organizational data systems. The case studies developed in this research are intended to address specific circumstances that would benefit the USMC in terms of efficiency and effectiveness of the workforce, while also providing potential opportunities for cost savings in infrastructure. Due to established information technology security policies, infrastructure limitations, and the current state of mobile device technology, it is not possible to study these cases directly. Consequently, in order to conduct this research, hypothetical case study methodology will be used.

The fundamental purpose of this research is to create a better understanding of the potential issues and benefits the Marine Corps could reasonably expect if a conceptual policy allowing the use of CMDs in the workplace was enacted. Therefore, the cases developed for this research are conceptual in nature and address specific instances of the conceptual policy and the implications at the individual, unit, and organizational levels.

A. RESEARCHER BIAS

The researcher is biased toward technology solutions that decrease redundancy (duplicating work in multiple systems), while simultaneously increasing information availability to those individuals that need it. Additionally, the researcher is biased against solutions that place additional workload on the end-users of the technology, preferring that burden to be on supporting elements (contractors, etc.). This bias comes from the researcher's experiences and the perception that technology solutions have been implemented that seemed to only increase redundancy and increase the workload of the end-user.

B. CMD IN MARINE CORPS EDUCATION AND TRAINING CASE STUDY (CASE 1)

Time to conduct training is one of the many resource limitations facing the USMC that leaders are required to contend with in order to prepare their units for deployment. The premise of this case study is that CMD technology has an ability to increase availability of education and training resources to the individual Marine. By increasing availability of education and training resources, this technology has the potential to allow leaders to more effectively and efficiently use this limited resource of time. If appropriately implemented and integrated with Marine Corps culture and training processes, this technology could positively impact overall training and readiness of the force.

The total number of active duty personnel in the United States Marine Corps varies slightly from month to month; however, the current end-strength goal is 182,000 (Marine Corps Concepts and Programs—End Strength, 2015, Description section, para 1). In order to maintain the total end-strength, Marine Corps Recruiting Command (MCRC) must recruit talented candidates (both enlisted and officer) to counter the outflow of personnel due to retirements, resignations, or completing their contractual obligation and returning to a civilian or reserve status. The Marine Corps Recruit Depots (MCRD) in San Diego and Parris Island, produce nearly 21,000 and 18,000 new Marines a year, respectively (Marines Operating Forces Presence Detail MCRD Parris Island & MCRD San Diego, n.d.). These new Marines generally serve a four-year contract, with roughly 23% of these first term Marines receiving an opportunity to re-enlist for a second term (Motley & Bird, 2016). The result of the high accession of new recruits and low retention opportunities are a high throughput of Marines every year.

1. Background and Organization

Training and education in the Marine Corps is overseen by Training and Education Command (TECOM), headquartered in Quantico, VA. TECOM's mission is as follows:

TECOM is charged by the Commandant of the Marine Corps with the development, coordination, resourcing, execution, and evaluation of training and education concepts, policies, plans, and programs to ensure Marines are prepared to meet the challenges of present and future operational environments. (Training and Education Command, n.d., Mission section)

TECOM is further divided into two separate commands, Training Command and Education Command (also referred to as the Marine Corps University [MCU]). Training Command conducts Military Occupational Specialty (MOS) “individual-skill training, analyzes, designs, develops, resources, implements, and evaluates standards-based individual training in order to provide combat-capable Marines and Sailors to the operating forces” (Training Command, n.d., para. 1). MCU’s mission is “to develop, deliver, and evaluate professional military education and training through resident and nonresident programs to prepare leaders to meet the challenges of the national security environment” (Marine Corps University Vision Statement, n.d., MCU Mission Statement section).

Within MCU is the College of Distance Education and Training (CDET) whose mission is to “design, develop, deliver, evaluate, manage, and resource distance learning products and programs across the Marine Corps training and education continuum in order to increase operational readiness” (United States Marine Corps College of Distance Education and Training, n.d.). CDET works with a network of regional centers (based on Marine Corps bases) to provide Professional Military Education (PME) to Marines on these bases. Additionally, CDET maintains the online repository of computer-based training for the Marine Corps, Marine Corps Distance Learning Network (MarineNet).

All Marines are required to complete mandatory annual training through MarineNet, which is an online system that provides access to computer based training modules. Fifteen courses are required to be completed by every Marine annually with topics ranging from Cyber Awareness, Operational Security, Anti-terrorism Awareness, to personal health and wellness training (MarineNet Annual Training Curriculums in Support of MCBul 1500, 2013). In addition to these annual training requirements, MarineNet offers courses (both mandatory and optional) that provide Military

Occupational Specialty (MOS) specific initial and follow-on training, as well as Professional Military Education (PME) courses that are required for advancement at various stages of a Marines career. In total, MarineNet offers over 4,500 computer-based training modules and numerous training resources that are available 24/7 to Marines provided they have access to a compatible computer system (MarineNet Tips, Tools & Practices, 2011).

According to the MarineNet Software Baseline Requirements (n.d.), “To ensure correct operation of audio, video, and interactive courseware components, you need specific computer hardware and software.” This resource goes on to list a number of Windows operating systems and applications that are required to complete the computer-based training modules. These baseline requirements do not mention compatibility with the current Windows operating system (Windows 10) or the previous operating system (Windows 8). Additionally, the requirements list only one web browser as compatible, Internet Explorer. This requirements list does not provide any information regarding compatibility with CMDs.

The Marine Corps has approximately 184,000 Active Duty Marines who require regular access to computer-based training, and approximately 39,000 Reserve Marines who require periodic access (Title IV—Military Personnel Authorizations, 2015). Increasing accessibility to this training has the potential to positively affect Marine Corps training and readiness. Additionally, increasing accessibility through devices that users already own and operate has the potential to reduce the infrastructure costs (in terms of desktop and laptop computers) of the Marine Corps. The focus of this case is on how allowing CMDs to access Marine Corps training and education resources could potentially provide benefits within an Infantry unit in a garrison training environment.

2. Researcher Experience

The researcher has previously served in the Regimental Operations Department of 3d Marine Regiment, stationed at Marine Corps Base Hawaii (MCBH) Kaneohe Bay, Hawaii. The researcher was assigned as the Assistant Regimental Air Officer. Due to manpower shortages, the researcher’s duties exceeded the bounds of an Air Officer,

which normally include training Joint Terminal Attack Controllers (JTAC) and serving as the Regimental Commanding Officers principal advisor on all matters involving the tactical employment of aircraft. The researcher also was involved in developing, scheduling, coordinating, and observing subordinate unit infantry tactics training to include field exercises, weapons training, as well as annual required training. The researcher has observed infantry units training for and deploying to combat operations as well as joint and multi-national exercises.

3. Case Explanation

The observation of the researcher is that Marine Corps infantry units train to a diverse set of missions and then deploy to accomplish some, all, or none of the missions for which they specifically trained. The Infantry Training & Readiness Manual (Department of the Navy: Headquarters United States Marine Corps, 2013) lists hundreds of training events, along with the performance standards, that infantry units are expected to complete in order to meet the demands of deployment. These training events range from individual skills, to squad/platoon/company/battalion level live-fire events.

This manual does not include additional training requirements such as annual marksmanship qualification training (generally two dedicated weeks of training), water-survival qualification, daily physical training, PME, the Marine Corps Martial Arts Program (MCMAP), Chemical Biological Radiological & Nuclear (CBRN) training, and annual administrative training. Additionally, the researcher has observed additional training mandated on these units from higher echelons of command that was in reaction to some incident or mandate outside of the Marine Corps (i.e., Marine is involved in an incident with local Police and an “All Hands” training is mandated, or Congressional leadership mandates training due to an increase in reported sexual assaults).

Wong (2002, p. 7) conducted a study in the U.S. Army to determine the time available to train for an infantry company in comparison to the training required to be conducted in a given year. In any given year, 109 of the 365 days are unavailable for training due weekends or federal holidays, resulting in only 256 available training days (Wong, 2002, p. 7). Examining the required training events and the time required to

complete each of these events, Wong (2002, p. 7) determined that approximately 297 days of training were required. Of these 297 days, it was determined that 254 days of training were dedicated to mission-related training (infantry skills training, etc.), while the other 43 days were dedicated to non-mission-related training (Wong, 2002, p. 7). This study only looked at Army units; however, the training requirements between the Army and Marine Corps are potentially similar in terms of the time to complete and the ratio of mission-related to non-mission-related training events. Additionally, the researcher observed instances where a Marine Corps infantry unit conducted its training on weekends or holidays. Every effort was made to avoid this, however, and to provide compensatory time during the work week to the affected personnel when possible. All of these education and training requirements, coupled with looming deadlines to prepare the Marines and their families for the rigors of deployment, add to the need for creative and innovative solutions in time management.

It is important to recognize that while the unit itself may have more training requirements than it has training days to complete them, a particular individual (especially the more junior Marines) is not likely to be actively engaged in training during the entire time the unit is conducting a particular training event. This allows the opportunity for potential white-space (free time, or time not actively engaged in an event) that could be used by a Marine to access MarineNet and complete PME, MOS training, language training, or other annual training requirements.

One particular example of this white-space opportunity is annual marksmanship training. The researcher has observed this training first hand numerous times. During this training, windows of time are present that a Marine has completed a live-fire event and is waiting for the remaining Marines to finish to move on to another stage of the training. This time can range from 15 minutes to an hour or more depending on the number of Marines training. The researcher observed that this time is generally spent by Marines conducting their “Smoke break” or socializing with their friends. This research is not advocating that Marines not be allowed their “Smoke-break” or socialization time, only that in an already crowded training schedule this time could potentially be used for the completion of training.

The researcher observed that a majority of these Marines own a CMD, usually a smartphone or tablet, which is with them in their backpack during this marksmanship training. These devices are not allowed on the firing line, and the researcher has observed them being confiscated by range personnel due to their unauthorized use. This research is not advocating that Marines who are engaged in conducting other training themselves, or are aiding other Marines in their training, be distracted from their task by using CMDs for professional purposes. Supervision, both by range personnel and the training units Staff Non-Commissioned Officers (SNCOs) and Non-Commissioned Officers (NCOs) is critical in order to ensure safety and quality training.

Another example of white-space in an infantry units' schedule is helicopter operations training. In this training, a helicopter squadron is tasked with providing a static aircraft for Marines to practice entering and exiting in a tactical manner. Additionally, the squadron provides a section (two aircraft) to fly in and out of a landing zone allowing the Marines to enter the aircraft, fly a pre-determined flight path, and either land in the same zone or a different zone and exit the aircraft. During this training, each helicopter is able to accommodate one squad or less per flight. According to Marine Corps Reference Publication (MCRP) 1-10.1 (2016), a Marine Infantry Rifle Company generally has 9 squads, with the potential for additional attachment squads as desired by the Battalion Commander.

The researcher has observed this training event, by a company-sized infantry element, takes anywhere from 3-6 hours to complete. During this period, an individual squad may go an hour or more without an aircraft to train with. This waiting period is extended in the event that one or more of the aircraft have mechanical or weather-related issues prior to or during the scheduled training time.

These situations are only two examples of periods of time that could be used for training and education of Marines. The issue is access to the resources, more specifically access to MarineNet. Looking at the current state of technology, several alternative solutions exist.

4. Potential Courses of Action

These solutions are limited to the specifics of this particular case, but the courses of action (COA) have the potential to be expanded for use by other units in the Marine Corps. These COAs will be discussed in terms of the potential CMD implementation strategy categories, and Confidentiality, Integrity, & Availability (CIA) Triad considerations.

a. HYOD with App-Based Access (Case 1, COA 1)

This COA recognizes that the Marine Corps may want to ensure 100% of Marines have access to the newly developed application. The Marine Corps does not currently mandate ownership of a CMD by Marines, and of those Marines that do own a CMD, the Marine Corps does not force the usage of a particular operating system on a personally owned CMD. A HYOD implementation strategy would allow the Marine Corps to select a single device (or group of similar devices) with only one common operating system and then control those devices in terms of configuration and usage. In this case, the Marine Corps is responsible for purchasing the devices, managing the devices, providing wireless access (possibly even cellular access), and developing and maintaining the application. The individual Marine is responsible for learning to operate the device, maintain accountability of the device, use the device in accordance with appropriate usage guidelines, and return the device to Information Technology (IT) staff when requested.

b. CYOD with App-Based Access (Case 1, COA 2)

The Marine Corps could potentially use a CYOD implementation strategy, which is a slight modification of the HYOD implementation strategy. In this COA, the Marine Corps could capitalize on the individual user familiarity in a particular operating system by offering a choice between (for an example) an iOS device or an Android device. The responsibilities of the Marine Corps and the individual are the same as Case 1, COA 1.

c. BYOD with App-Based Access (Case 1, COA 3)

This research assumes that the majority of Marines have a personally owned CMD, which is based on the Mercado and Spain (2014, p. 7) research that showed that

over 79% of Soldiers in the Army owned “at least one mobile device.” With this assumption, it is suggested that the Marine Corps develop a MarineNet application and make it available for download on personally owned CMD. This application would need to be compatible with at least the two most popular mobile operating systems (Android, and iOS), which would allow access to 70% or more of personally owned devices (Mercado, & Spain, 2014, p. 9).

This MarineNet application would need the ability to authenticate the user using at least two factors. It is suggested that a username and a password be used to authenticate each time the user accesses the application. It is also suggested that some process is established that allows the Marine to download the application initially, and having a confirmation email sent to their official email (@usmc.mil) account. This email would allow the Marine to authorize the CMDs media access control (MAC) address. This could help to prevent unauthorized users from access the application, helping to enforce confidentiality of the courseware.

In terms of availability, this research recognized that some of these training events occur in remote field-environment areas, and therefore wireless connectivity may not be available. For the purposes of this case study, the assumption is made that the zone is in a location that has cellular connectivity, which would allow the Marines waiting to conduct training the opportunity to connect to MarineNet and access the multitude of computer-based training modules available. The requirement for wireless connectivity could potentially be overcome, if subsequent application updates allowed Marines the ability to download courses from MarineNet on their CMD. This would also require the ability for the application to update the Marines’ training records the next time the application is able to connect to the Internet.

This COA allows the Marines to bring their personally owned (user preferred) devices and connect to the application, allowing access to training and education resources. This research recognizes that not all Marines own a CMD, and of those who do own a CMD, not all of them will be willing or able to use the application.

5. Case Summary

This case looked specifically at maximizing the availability of MarineNet training and education courseware to Marines during periods of down-time in their regular garrison training environment. The use of CMDs in conjunction with application based access could provide more efficient and timely completion of computer-based training by Marines. While this case looked only at an infantry unit in the Marine Corps, it is possible that other units (in the Marine Corps, and other services) could potentially benefit from the selection of any of the previously described COAs. The potential efficiency of application based access on a CMD are not limited to training and education. It is possible that numerous daily processes performed by Marine Corps units could benefit from the application of this technology.

C. CMD IN SQUADRON FLIGHT SCHEDULE DEVELOPMENT CASE STUDY (CASE 2)

Squadron flight schedule development and approval is a complex, time-consuming process requiring collaboration by several individuals. The premise of this case study is that CMD technology has an ability to increase collaboration of those individuals involved in flight schedule development. By increasing collaboration, this technology has the potential to allow for a more effective and efficient flight schedule development by Marine Corps squadrons. If appropriately implemented and integrated into the culture, and flight schedule development processes this technology could potentially positively impact aviation mishap investigations.

In the garrison training environment, the mission of the Marines in a USMC aviation squadron can be simply stated as “the safe execution of the daily flight schedule.” Each of the individual departments that make up the squadron (Operations, Maintenance, Logistics, Safety, etc.) has an impact on, and input into the development and execution of the daily flight schedule. The daily task of developing the flight schedule can be a complex, and time-consuming process. Through the use of CMD technology by the Marines involved in this process, potential positive impacts could be gained.

1. Background

For the purposes of this research, the terms Naval Aviation and Marine Corps Aviation are considered to be synonymous. Navy aircraft and Marine Corps aircraft are all subject to the rules and regulations of the Federal Aviation Administration (FAA), Office of the Chief of Naval Operations (OpNav), Naval Air Systems Command (NAVAIR), and Headquarters United States Marine Corps (HQMC). Marine Corps pilots are responsible for understanding FAA regulations, and by following the procedures described in the OpNav and HQMC sources, all flights are in compliance with the FAA scheduling regulations.

The Commanding Officer authorizes an aircrew to fly naval aircraft under his/her control through physically signing the daily flight schedule (OpNav, 2009). The signature of the Commanding Officer on the flight schedule marks the successful completion of a complex process that is usually carried out daily in a squadron. The process of developing the daily schedule can start months in advance of execution, when key stakeholders (Operations Officer, Maintenance Officer, and Commanding Officer) meet to develop long-term training plans. Prior to this meeting, the Operations Officer determines what aircrew training is needed by the squadron in order to prepare for the next deployment. The Maintenance Officer determines the state of the aircraft and attempts to forecast their availability, taking into account regularly scheduled maintenance periods. The Commanding Officer acts as the arbiter between the key stakeholders and the result of the meeting is a general schedule (usually a 30-day, 60-day, and 90-day plan) that both the Operations and Maintenance departments can prepare for. For the purposes of this research, this output will be referred to as the monthly flight schedule.

The researcher has observed this monthly flight schedule development from the perspective of the Operations department and the Maintenance department. The monthly flight schedule usually shows the number of aircraft that can be scheduled for flight operations/training on a given day, as well as the number of hours that those aircraft can be flown during that day. It is from this information that the Operations Officer (OpsO) and the Pilot Training Officer (PTO) develop the weekly flight schedule. The weekly

flight schedule is used to describe the expected takeoff and landing times of the aircraft, the training events that will occur, and the aircrew expected to fly those aircraft.

The weekly flight schedule is, in general, written at least one week in advance and must take into account many factors. The PTO must look at the training that is needed to prepare the aircrew of the squadron and then match those in need of training, with aircrew instructors that are authorized to conduct the training. This task is made more difficult by the individual schedules of the Marines in the squadron. The researcher has observed one method that PTOs use to accommodate individual needs, called the Snivel Log. The Snivel Log is the method by which an individual Marine can communicate to the PTO his/her availability to conduct aircrew training on a given day. The individual Marine is expected to put in periods of non-availability due to appointments, vacation, temporary active duty assignment, or family issues.

With the Snivel Log, the PTO populates the weekly flight schedule, and then that schedule is agreed to by the key stakeholders (the Safety department is added to the key stakeholders at this point). This provides the Maintenance department another opportunity to assess the state of the squadron's aircraft and determine if the previously agreed to monthly plan is still supportable. The Safety department assesses the weekly flight schedule to ensure it is in compliance with all OpNav and HQMC rules and regulations regarding aircrew selection and assignment. Finally, the Commanding Officer approves the weekly flight schedule and sends it back to the PTO, who directly oversees the squadron schedule writers.

The researcher has observed that the monthly and weekly flight schedules are generally developed in a spreadsheet program (usually Microsoft Excel). The successful completion of the weekly flight schedule results in the schedule writers inputting the information into the Marine-Sierra Hotel Aviation Readiness Program (M-SHARP). M-SHARP is an online-based training management system used for scheduling and logging flights (Department of the Navy: Headquarters United States Marine Corps, 2016). This program stores the individual qualifications (i.e., Night Vision Goggle qualified) and designations (i.e., Night Vision Systems Instructor) for squadron personnel.

The Marine Corps mandates the use of M-SHARP in order to “plan, schedule, log, track, and manage all training and readiness reporting requirements” (Department of the Navy: Headquarters United States Marine Corps, 2016, p. 2-17). M-SHARP offers the ability to operate connected to the Internet, as well as the ability to create a self-contained network (not requiring Internet connection) for use during deployed operations. This self-contained system is required to be connected to the Internet upon return from deployment to update the online system (Department of the Navy DON: Headquarters United States Marine Corps, 2016, p. 2-20).

The daily flight schedule is developed in M-SHARP by a qualified schedule writer, and then a paper copy of the schedule is printed for validation and concurrence by the various departments as directed by the Commanding Officer. The researcher observed that at a minimum the following key stakeholders validate and concur with the daily flight schedule prior to Commanding Officers approval: Operations Officer, Maintenance Officer, Aviation Safety Officer, and Executive Officer. The researcher has also observed that in special circumstances, the Commanding Officer signed the daily flight schedule without key stakeholder validation and concurrence.

Each of these key stakeholders has the ability to make changes to the schedule that the schedule writer is then required to fix in M-SHARP. The schedule writer then re-prints and re-circulates the altered flight schedule for each key stakeholder’s concurrence. The researcher has observed that this process of revision and re-work consumes hours of schedule writer time and effort. In a squadron with multiple schedule writers, the researcher has observed the assignment of one schedule writer to inputting the weekly flight schedule into M-SHARP and another to the daily routing of the next day’s flight schedule. In this scenario, the schedule writer begins the work-day with a schedule that is already prepared for routing, and then that schedule writer could take an entire eight- to 10-hour day attempting to get the concurrence of all the key stakeholders in order to allow the Commanding Officer to sign the flight schedule.

The researcher has observed many causes for the duration of this task. Some of these causes are due to aircraft maintenance issues, or time-critical personnel issues that are unlikely to be avoided. Other causes are due to nature of naval aviation training and

various safety policies that affect the key stakeholder's ability to physically arrive for duty before a certain time. For example, if one of the key stakeholders are assigned to night flight training. OpNav "crew rest" regulations require that, at a minimum, aircrew be given 8 hours of "uninterrupted sleep time for every 24-hour period" and should not be "scheduled for continuous alert and/or flight duty in excess of 18 hours" (Department of the Navy Office of the Chief of Naval Operations, 2009, p. 8-15).

In order to comply with these regulations, the researcher has observed Commanding Officers to use their squadron Standard Operating Procedures (SOP) to enforce more stringent "crew rest" planning factors. In these planning factors, the researcher has observed the Commanding Officer restrict aircrew from reporting to work earlier than 10 hours prior to that aircrew's expected land time. In the case of night flying training operations that include flying until midnight, the aircrew would not be allowed to report to work earlier than 1400 that day. If a member of that aircrew is a key stakeholder in the schedule development and approval, the schedule would wait until he/she reported to work for the day. This case will look at how, with additional functionality added to M-SHARP, the Marine Corps could potentially complete this process in a timelier and more efficient manner.

2. Researcher Experience

The researcher has four years of experience in a Marine Corps CH-53D "Sea Stallion" squadron, stationed on Marine Corps Base Hawaii, Kaneohe Bay, HI. The researcher served as a squadron pilot with multiple instructor designations and assignments as a squadron schedule writer, assistant to the Operations Officer, Aviation Safety Officer (ASO), Director of Safety and Standardization (DoSS), and Assistant Aircraft Maintenance Officer (AAMO) with the squadron. Due to this experience, the researcher has been involved with the flight scheduling process from every key stakeholder position with the exception of the Commanding Officer.

3. Case Explanation

The development and eventual Commanding Officer approval of the daily flight schedule is a process that involves collaboration by numerous individuals. The process is

complex—not because it is complicated—but because numerous factors affecting it are constantly changing. For example, the previous day’s flying operations could leave the maintenance department with fewer flyable aircraft than previously agreed to. This situation could cause an entire schedule to be cancelled, or some reduced number of events flown. Additionally, aircraft readiness or weather-related cancellations of a high-priority event could cause a ripple effect that forces changes to several subsequent flight schedules. In the researcher’s experience, these issues are very common, to the point of being routine.

Often the consequences of making changes to the schedule due to these issues leads to 2nd- and 3rd-order effects that extend the time for the schedule to reach completion. For example, in the case of weather affecting a high-priority event, the researcher has observed the PTO may re-schedule the event and push the previously scheduled event back a day or more. This change seems benign; however, the consequence is the schedule is re-routed through all the key stakeholders again. During this process, the researcher has observed that aircrew are scheduled for events that they are unable to fly due to previously scheduled engagements, as detailed in the Snivel Log. The schedule is then returned to the PTO and the schedule writer for further re-work, and re-routing. This process takes time, and as each individual key stakeholder returns the schedule for re-work, the schedule must be re-routed to all the key stakeholders for their concurrence. Additionally, this time consuming and inefficient process is further delayed if any individual is prevented from reporting to work due to crew rest considerations.

CMDs are, by their nature highly portable, instantly accessible and able to connect to the Internet (Tucker, 2010, p. 1). The connectivity and portability of CMDs could allow the Marine Corps to overcome issues related to crew rest. This would likely require the Commanding Officer to officially grant the key stakeholders an exemption (in the squadron Standard Operating Procedures) regarding crew rest policy allowing them to telecommute (under circumstances where it is warranted) during their crew rest period.

These devices are not currently given access to the M-SHARP system. M-SHARP requires a common access card (CAC) and a CAC reader in order to access the system. Additionally, Internet Explorer 11 is the only web browser that is stated to be compatible

with M-SHARP, and the user manual clearly states “attempting to use other versions of Internet Explorer or other web browsers may result in the program not displaying or functioning as intended” (Marines Sierra Hotel Aviation Readiness Program: Software User Manual, 2016, p. xxxv). Navy Marine Corps (NAVMC) 3500.14D (2016), mandates the use of M-SHARP by all aviation units. In order to allow a CMD to access M-SHARP, this research has developed several COAs.

4. Potential Courses of Action

These solutions are limited to the specifics of this particular case. These COAs will be discussed in terms of the potential CMD implementation strategy categories, and CIA Triad considerations.

This research assumes that the majority of Marines have a personally owned CMD, but do not have a CAC capability on their devices. In this COA, the Marine Corps would be required to contract the development of an application that had access to a limited number of functions within the M-SHARP program by either the developer of M-SHARP or a third-party contractor. M-SHARP, in addition to the scheduling utility, has numerous functions that while not subject to classification requirements are likely sensitive information. The researcher has observed information regarding aircrew training and readiness levels, and personally identifiable information (PII) has been stored on the M-SHARP system. The application developed would only need access to specific information (based on the individual key stakeholder’s position) and access to the schedule.

The researcher has observed that M-SHARP only allows one user (usually the schedule writer) to view/edit the schedule. This limits collaboration by the key stakeholders and would not take advantage of the connectivity, and collaborative capability that CMDs allow. It is suggested that the application incorporate a document editor function that would allow the schedule writer to share the schedule with all the key stakeholders for their review and edits simultaneously. The application should have the ability for the key stakeholders to make changes, add notes, as well as a text-based chat function. With an application like this, the key stakeholders would have the ability to see

each other's changes in near real time, and make comments to each other and the schedule writer. The potential benefit of this application is that collaboration would be possible between the key stakeholders until a satisfactory product is produced and ready for the Commanding Officer's signature.

a. HYOD with App-Based Access (Case 2, COA 1)

In a HYOD implementation strategy, the Marine Corps would be responsible for developing the application, providing a CMD to each key stakeholder, and procuring wireless contracts for the devices. The individual would be required to maintain physical security of the device, and provide it to the IT staff when requested for updates and configuration checks. The squadron would maintain the devices, as new people rotated in and out of the key stakeholder positions. The devices would likely be of one configuration (operating system, security functions, etc.). Additionally, the newly developed application would only need to allow access to the government furnished devices.

b. CYOD with App-Based Access (Case 2, COA 2)

In a CYOD implementation, the Marine Corps and the individual would have the same responsibilities as Case 2, COA 1. The fundamental difference would be that the Marine Corps would offer a choice in device to either the squadron or the key stakeholder. The intended benefit of CYOD over HYOD would be observed when the user is allowed to use a device he/she is more familiar with (Grajcar et al., 2013, p. 63). The researcher has observed that individuals can transition in and out of these key stakeholder positions frequently, and it may be more timely and cost efficient to allow the squadron Commanding Officer or IT staff to decide on a mix of various approved devices that are distributed. For example, a squadron may be allotted six CMDs, and choose to have four running iOS, and two running Android. In this scenario, the potential exists that some of the key stakeholders would not be issued their preferred device. The researcher has observed that the majority of these key stakeholders are officers of the rank O-3 or O-4 (with four to 20 years of commissioned service), and would likely adapt quickly to the device with minimal adversity.

c. BYOD with App-Based Access (Case 2, COA 3)

In a BYOD implementation, the Marine Corps could capitalize on the CMD already owned by the individual Marine. The researcher has observed that individuals in these key stakeholder positions usually owned their own CMD and were familiar with the operation of their device. The Marine Corps would still be responsible for developing the application, and could possibly provide a stipend to offset the users wireless contract costs. The Marine Corps would need to develop a system of granting and revoking access to the application as individuals were transferred in and out of the key stakeholder billets.

5. Case Summary

This case looked at the possibility of using CMDs to improve efficiency and collaboration in the development of a Marine Corps aviation squadron conducting training in a garrison environment. Through application-based access to M-SHARP by the key stakeholders working on a CMD, the case was made that the process could potentially be improved. This daily process is common to all Marine Corps aviation squadrons. The potential exists, that a similar application and CMD access could benefit the daily flight scheduling process of other services (Army, Navy, Air Force, & Coast Guard).

D. CMD IN AVIATION MISHAP INVESTIGATION CASE STUDY (CASE 3)

Conducting an aviation mishap investigation is a lengthy, time-consuming process that involves extensive collaboration by several individuals. The premise of this case study is that CMD technology has an ability to increase collaboration and mobility of those individuals involved in the investigation. By increasing collaboration and mobility, this technology has the potential to allow for a more effective and efficient investigative capability in the Navy and Marine Corps. If appropriately implemented and integrated into the culture, training, and investigative processes this technology could potentially positively impact aviation mishap investigations.

In a USMC aviation squadron, aviation mishaps can and do occur at any time of the day or night and require immediate investigation by a several appointed experts in

order to determine the cause of the incident. Each of the individual departments that make up the squadron (Operations, Maintenance, Safety, etc.) has either a direct or an indirect role in completing the investigation. Aviation mishap investigations are a complex and, in some cases, a time-consuming process for numerous individuals. The use of CMD technology by the Marines involved in the early and on-going stages of the investigation could have significant impact on the ability to conduct a thorough investigation in a timely and efficient manner.

1. Background

The stated purpose of both a Navy and a Marine Corps aviation squadron's aviation safety program is to "preserve human lives and material resources, thereby, to enhance readiness" (Department of the Navy Office of the Chief of Naval Operations, 2014). Aviation mishap investigations are intended to determine "the hazard(s) which precipitated the mishap and to recommend remedies to prevent recurrence" (Senior Member Guide, 2010). In the event of an aviation mishap, including a naval aircraft of unmanned aerial vehicle (UAV), the squadron will execute the Pre-Mishap Plan as developed by the Aviation Safety Officer and in accordance with Office of the Chief of Naval Operations Instruction (OPNAVINST) 3750.6S (Naval Aviation Safety Management System).

For purposes of this research, a naval aviation mishap is defined as:

an unplanned event or series of events, directly involving a defined naval aircraft or UAV, that results in damage to DOD property; occupational illness to DOD personnel; injury to on or off-duty DOD military personnel; injury to on-duty DOD civilian personnel; or damage to public or private property, or injury or illness to non-DOD personnel, caused by DOD activities. (OpNav, 2014, p. 3-5)

Naval aviation mishaps are classified based on the severity of material damage and personnel injury, as shown in Table 2.

Table 2. Naval Aviation Mishap Severity Classifications.
Adapted from OpNav (2014, pp. 3-14 – 3-15).

| Mishap Severity | Damage to Naval Aircraft Or Property | | Personnel Injury | |
|-----------------|--------------------------------------|--|---------------------|--|
| | Max | Min | Max | Min |
| Class A | None | \$2,000,000 (or aircraft destroyed/missing) | None | Fatality, or permanent total disability |
| Class B | < \$2,000,000 | > or = \$500,000 | < Class A threshold | Permanent partial disability, or 3 or more personnel hospitalized |
| Class C | < \$500,000 | > or = \$50,000 | < Class B threshold | Nonfatal injury or illness (that results in 1 or more lost work day, not including day of injury) |
| Class D | < \$50,000 | > or = \$20,000 | < Class C threshold | Any injury (greater than first aid) |

Naval aviation mishaps are further classified into subcategories relating to the state of the aircraft and the aircrew at the time of the mishap. The first category is a flight mishap (FM) which is defined as a mishap where “there is intent for flight and damage to a DOD aircraft of UAV or the loss of a DOD manned aircraft” which includes any mishaps that occur in flight, or during take-off and landing periods. The second category is a flight related mishap (FRM), which is defined as a mishap where “there is intent for flight and no reportable damage to the aircraft or UAV itself, but the mishap involves a fatality, reportable injury, or reportable property damage.” The third category is an aviation ground mishap (AGM) which is defined as a mishap where “there is no intent for flight that results in reportable damage to an aircraft or UAV or death or injury involving an aircraft or UAV” (Department of the Navy Office of the Chief of Naval Operations, 2014, pp. 3-15–3-16). The category and classification do not have an impact on the conduct of the investigation but are provided in this research to show the wide range of incidents that require the convening of an aviation mishap investigation.

Prior to a mishap occurring, the Aviation Safety Officer is expected to have developed a Pre-Mishap Plan, and given training regarding the plan to the standing members of the Aviation Mishap Board (AMB), if not to the entire compliment of aviators in the squadron (Department of the Navy Office of the Chief of Naval Operations, 2014, p. 2-8). For all Class A, B, and C which involve more than minor

injuries, mishaps the AMB is comprised of “at a minimum, an ASO, a flight surgeon, an officer well-qualified in aircraft maintenance, and an officer well-qualified in aircraft operations” (Department of the Navy Office of the Chief of Naval Operations, 2014, p. 2-8). The AMB is headed by a senior member (usually the squadron Executive Officer) appointed by the Commanding Officer, with the exception of Class A mishaps (in this case the senior member is assigned from an outside command). This is the minimum staff on an AMB, and the researcher has observed AMBs that had numerous specialists depending on the nature of the incident.

The standing members of the AMB are, with the exception of the flight surgeon all pilots or flight officers who may potentially be involved in the mishap (piloting aircraft, eye witness, etc.), which leads to the need for alternates who are also trained and ready to conduct the investigation. Additionally, in the event of a mishap, the AMB members may be off-duty and may not be able to immediately begin to conduct the investigation. The researcher has observed that when a mishap occurs, the initial period can be chaotic with numerous tasks from the Pre-Mishap Plan being executed simultaneously. In these circumstances, the ASO has been observed to not proceed to the investigation site until the initial tasks are completed (reporting and notifications of higher headquarters units, etc.). The need for the members of the AMB to work autonomously and collaboratively, without the guidance of the ASO is imperative to collecting the necessary evidence for the investigation.

Following the initial evidence collection in a mishap investigation, it is likely that further evidence collection will be required. Witnesses are likely to be interviewed and re-interviewed. Numerous external agencies such as weather, air traffic control, and local law enforcement are likely to coordinate with and provide information to the AMB. The result of the many disparate tasks in an investigation is that large period of time can pass between AMB members meeting face to face. In the Senior Member Guide (2010), the senior member is advised to establish meeting times, to have each member report on their status, and then set goals for (and the time and date of) the next meeting.

The researcher has observed the completion of the AMB process in weeks for more minor investigations, and in months for more major investigations.

Interchangeability of AMB members is necessary in circumstances where an individual must execute a permanent change of station (PCS) move, deploy, or conduct a temporary assigned duty (TAD). With an appropriately designed application installed on a CMD, it is possible that the aviation mishap investigation process could be improved.

2. Researcher Experience

The researcher attended the Naval School of Aviation Safety in Pensacola, Florida in 2010, receiving certification as a qualified Aviation Safety Officer (ASO). Following completion of ASO certification, the researcher held the billet of Squadron Aviation Safety Officer and Director of Safety and Standardization. The researcher has experience as a AMB member on multiple mishap investigations that span each of the severity classifications (Class A, B, C, etc.) and each subcategory (FM, FRM, & AGM). Additionally, the researcher has acted as ASO for a mishap involving a different squadron than the researcher was assigned to, due to the involvement of that squadron's ASO in the mishap. The researcher has experienced first-hand the need for interchangeability of AMB members, and collaboration among those members in order to complete the investigation in a timely manner.

3. Case Explanation

Aviation mishaps are an uncommon occurrence, and in the case of many squadrons in the Navy and Marine Corps, an ASO has the potential to complete a two- to three-year tour and not experience a single mishap. The latest statistics from the Naval Safety Center (2016) show that in the last 12 months (July 2015 to July 2016) the Navy had seven Class A (FM) mishaps and 12 Class B (FM) mishaps, while the Marine Corps had six Class A (FM) mishaps and three Class B (FM) mishaps. This equates to a Class A (FM) mishap rate for the Navy of .82 mishaps per 100,000 flying hours, and a Class A (FM) mishap rate for the Marine Corps of 2.48 mishaps per 100,000 flying hours (Naval Safety Center, 2016). This research is not intended to suggest that CMD technology would lower these mishap rates, only that the technology could improve the ability to conduct an investigation when necessary.

In the event of a mishap, the first person notified is the Marine assigned to Operations Duty Officer (ODO) in the squadron ready room. This Marine is generally, although not necessarily, a more junior aviator in the squadron, and is notified through a radio transmission or a phone call from some external agency such as air traffic control, Federal Aviation Administration (FAA), local police, etc. The ODO is often responsible for initiating the Pre-Mishap Plan, and locating the Mishap Kit, which holds the investigation-specific items needed by the initial responders and the AMB. Often, the members of the standing AMB are not present for duty at the time of the incident or are involved in the mishap themselves. In these situations, the ASO or other command representative directs initial responders to the investigation site to begin evidence collection (pictures, materials, etc.).

The researcher has observed that in the event of a mishap, the initial responders collect the pictures and videos on their personal CMD or personal digital camera and provide the materials to the AMB. These photos can be of a sensitive nature, and need at least some level of control exercised over them. It is important to note, that OPNAVINST 3750.6S (2014) does not consider these pictures and video “privileged information” unless they are “staged by the AMB (i.e., photographs that are preplanned or posed to illustrate a specific condition or situation.” The order also includes photographs that have captions or markings on them “indicative of the AMB’s deliberative process” as privileged information. Privileged information is required to be safeguarded against disclosure through “public release and non-safety uses” (Department of the Navy Office of the Chief of Naval Operations, 2014, p. 1-28).

The Naval Safety Center (NAVSAFECEN) is responsible to the Chief of Naval Operations (CNO), for managing all safety matters in the Navy and Marine Corps including the Naval Aviation Safety Management System (Department of the Navy Office of the Chief of Naval Operations, 2014, p. 1-1). The NAVSAFECEN uses the online system Web-Enabled Safety System (WESS) for the electronic development and submission of Safety Investigation Reports (SIREP) by Navy and Marine Corps units. The aviation mishap specific portion of this system is called WESS Aviation Mishaps & Hazards Reporting System (WAMHRS).

WAMHRS allows each the AMB to store evidence, points of contact, general information, and weather data for reference throughout the investigation. The system is also used for each AMB member to write their respective portion of the SIREP. Access to WESS and WAMHRS is controlled by the Commanding Officer through the ASO, and access to the SIREP in the system is further controlled by the ASO and the AMB senior member. A CAC with public key infrastructure (PKI) is required to access the system, and the system is only stated to be compatible with the Internet Explorer web browser (Department of the Navy Office of the Chief of Naval Operations, 2014, p. 4-1).

It is possible that WESS and WAMHRS could be updated to allow access to a wider range of operating systems and web browsers. However, it may be more beneficial to develop a mobile application that could allow AMB members to upload investigation materials to the WESS and WAMHRS. Compartmentalizing and limiting access to the system through the application could potentially improve the confidentiality and integrity of the system while improving accessibility. In order to allow a CMD to access WESS and WAMHRS, this research has developed several COAs.

4. Potential Courses of Action

These solutions are limited to the specifics of this particular case. These COAs will be discussed in terms of the potential CMD implementation strategy categories, and CIA Triad considerations.

This research assumes that the majority of the Marines that are assigned to (or could be expected to be assigned to) the AMB have a personally owned CMD that they are familiar with operating. Additionally, it is assumed that WESS and WAMHRS can be made compatible with additional operating systems and web browsers. With these assumptions, the following COAs were developed to potentially address the availability issue described in this case.

a. HYOD with App-Based Access (Case 3, COA 1)

In a HYOD implementation strategy, NAVSAFECEN would be responsible for contracting the development of a mobile application that was compatible with WESS and

WAMHRS. The Navy and Marine Corps would be responsible for procuring the CMDs, maintaining the CMDs and contracts for wireless access. This COA would allow NAVSAFECEN the ability to restrict access to WESS and WAMHRS on the mobile application to only those specific devices that the government procured.

The Marine Corps has a limited CMD HYOD implementation program that allows “privileged users” to obtain a government furnished device if the user is identified as “being mission critical or mission essential” (Anderson, 2013, p. 11). The researcher has observed that in a Marine Corps aviation squadron the Commanding Officer, Executive Officer and Sergeant Major are often deemed “privileged users” under this program. This COA could essentially be an expansion of this program to include the standing members of the AMB. This research suggests that the unit ASO be responsible for these additional devices, and maintain them in the units Mishap Kit rather than distribute them to the standing AMB members. The ASO would then have control over the devices, and be responsible for training the standing AMB members and alternates on the devices use in the event of a mishap.

It is likely that in an HYOD implementation, only one type of CMD would be selected thereby reducing the necessity to make WESS and WAMHRS compatible with multiple operating systems or web browsers.

b. CYOD with App-Based Access (Case 3, COA 2)

In a CYOD implementation, the NAVSAFECEN would have the same responsibilities as the previous COA with the additional responsibility of making the application compatible with multiple CMD configurations. The Navy and Marine Corps responsibility would remain the same with the additional responsibility of providing multiple CMD configurations that the individual or unit could choose from.

Similar to Case 2, COA 2, the researcher has observed that standing AMB member assignment can change frequently, and it may be more timely and cost efficient to allow the squadron Commanding Officer or IT staff to decide on a mix of various approved devices that are distributed. In this scenario, the potential exists that some of the AMB members would be issued a device that they are less familiar with. The majority of

the AMB members are officers of the ranks O-3 through O-6 (with four to 30 years of commissioned service), however, and would likely adapt quickly to the device with minimal adversity.

c. BYOD with App-Based Access (Case 3, COA 3)

In a BYOD implementation, the NAVSAFECEN would have the same responsibilities as COA 2. The Navy and Marine Corps would be responsible for making the application available to individuals on their own device, as well as limited technical support. The individual units would likely be responsible for controlling which individuals have access to their units WESS and WAMHRS information. This COA would potentially allow the greatest number of people to collaborate on an investigation, while limiting the cost to the government to developing a mobile application.

It would likely be the responsibility of the ASO to manage WESS and WAMHRS and only allow access to individuals that are authorized. Additionally, the ASO would likely need the ability to revoke access of an individual at the completion of an investigation.

5. Case Summary

This case looked at the possibility of using CMDs to improve collaboration, information availability and accessibility in order to more efficiently and effectively investigate an aviation mishap. This case is applicable to all Navy and Marine Corps aviation units conducting an aviation mishap investigation in a garrison environment where wireless mobile access is available. Additionally, an appropriately developed application with access to WESS and WAMHRS could potentially benefit non-aviation units in the Navy and Marine Corps conducting other safety investigations (non-aviation mishaps). This is outside the scope of this research and would need to be examined in follow on research to determine applicability to those processes.

E. SUMMARY

This research has developed three independent case studies involving the implementation of CMD technology with mobile application based access that have the

potential to improve information availability and accessibility of the end user. Each case has been presented with multiple course of action for implementation, each with varying risks and benefits from the perspective of the end-user, and the organization. The cases and their purposed courses of action will be analyzed based on risk and benefits to the individual and the organization. In analyzing the risks and benefits, this research will seek to understand how the individual and the technology are likely to interact (socio-technical systems theory) and how likely the individual is to accept the new technological capability (using the technology acceptance model).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS

The three case studies developed in this research examine scenarios in which the United States Marine Corps (USMC) could potentially implement commercial mobile device (CMD) technology into business processes. Commercial sector businesses like Intel Corporation have utilized CMD technology to revolutionize the way their employees work, learn, socialize, organize, and entertain themselves. It is possible that this technology could similarly revolutionize the USMC.

In research done by Mercado and Spain (2014, p. 7), mobile device ownership was 79% in the U.S. Army, with the youngest age group (20 years old and under) at 94% ownership, and it is possible that the USMC has similar levels of ownership. This younger demographic of Marines are the future Non-Commissioned Officers (NCO), Staff Non-Commissioned Officers (SNCO), and junior and mid-grade commissioned officers that are at the forefront of day to day operations and training in Marine Corps units. These younger Marines are considered “digital natives” in that they were raised with the Internet, computers, mobile phones and digital technologies (Prensky, 2001). These “digital natives” come to the USMC pre-programmed and trained to operate on CMDs. The challenge for leaders within the USMC is to determine how to garner the benefits of using CMDs while limiting the detrimental security impacts these devices can have on the network.

The analysis presented in this research is both general and specific. General risks and benefits will be analyzed and applied to the USMC. Additionally, each individual case will be analyzed independently with a focus on Socio-technical Systems Theory, and the Technology Acceptance Model. Within the analysis of each individual case the independent courses of action (COA) will be analyzed based on the Confidentiality, Integrity, and Availability (CIA) Triad risks and benefits.

A. GENERAL ANALYSIS OF CMD IMPLEMENTATION IN THE USMC

Metcalf's Law described the value of the network, as seen by those users on the network, as increasing "as the square of the number of users: $V \sim N^2$ " (Metcalf, 2013, p.26). Value as it is seen here is not necessarily in monetary terms, but more in utility of the network to serve its intended purpose. The researcher observed this law in the introduction of the Blue Force Tracker (BFT) to the battlefield in Afghanistan during Operation ENDURING FREEDOM. The value of the BFT to the researcher, as a pilot operating in Afghanistan, was minimal in the early stages of the introduction, because a relatively small number of users were on the network and even fewer had enough familiarity with the system to operate it. As the BFT gained popularity as a communications and situational awareness tool, the value of the BFT increased exponentially.

It is possible that the greatest single benefit related to CMD usage in the USMC would be the increase in the number of people that would have access to the network. This could allow these individuals to help create value to the Marine Corps by increasing their work efficiency and effectiveness. Conversely, this potential greatest benefit could also be one of the greatest sources of risk associated with CMD use. This is due to the risk associated with increasing the number of potential access points to the network, which increases the attack surface area for individuals and organizations intending to cause harm.

Many of the advantages regarding CMD usage are closely tied to a disadvantage of that usage. The benefits of CMD usage at work are broadly thought of as falling into three categories: reduction of IT procurement cost, increasing employee productivity, and gaining an organizational competitive advantage (Chandrasekhar, 2013, p. 6). These three categories are used in this research in order to provide a framework of general analysis for implementing CMD technology.

1. Cost Related Risks and Benefits

In the CMD implementation cases of the Alcohol and Tobacco Tax and Trade Bureau (TTB), the U.S. Equal Employment Opportunity Commission (EEOC), and the State of Delaware each organization cited cost related factors as a major reason for pursuing their new technology policies (White House, 2012). The researcher has observed that cost savings is a major factor in an organization deciding to pursue CMD technology. In many cases, infrastructure and equipment costs are reduced, while costs in technical support have been observed to increase.

a. Infrastructure and Equipment Related Savings

CMD technology has the potential to decrease the necessity of a desktop or laptop computer in business processes. The TTB was spending nearly \$2 million every three to four years to replace outdated desktop and laptop computers. By implementing CMD technology into their business processes, they were able to save \$1.2 million of that \$2 million in infrastructure and equipment costs (White House, 2012). The State of Delaware's CMD implementation resulted in a 45% reduction in infrastructure expenses, and a 15% reduction in wireless costs (White House, 2012). The EEOC had already implemented CMD technology with their workforce and shifted from organizationally owned and provided devices to employee owned devices. By providing a subsidy to their employees for wireless service costs, they were able to decrease their monthly costs related to wireless service by 20–30% (White House, 2012). These are only three examples of an organization achieving infrastructure savings by implementing CMD technology.

Intel Corp. recognized that costs were reduced in terms of procurement of devices, however they also determined that costs increased elsewhere due to the necessity of evaluating devices, ensuring proper configuration, and continuing to support these devices (Chandrasekhar, 2013, p. 2). The decrease in procurement costs is tied to the particular device implementation strategy that is selected. For instance, the here's your own device (HYOD) system has significantly higher procurement costs but potentially lower configuration and support costs when compared to the more open bring your own

device (BYOD) system which can allow for almost no procurement cost on the organization.

Loss or damage to desktop and laptop computers is another significant infrastructure cost. Mobile computing devices are recognized as being more susceptible to be loss, theft, and exploitation than laptop and desktop computing devices located in an office space (Department of Defense Chief Information Officer, 2006). Allowing employees to bring their own devices could reduce hardware loss. Intel lost one percent of its laptop computers each year due to employee carelessness and theft (Chandrasekhar, 2013, p. 3). A BYOD implementation would reduce the monetary cost to the USMC in the event of a lost or stolen device, however the cost associated with the potential damage caused by that stolen/lost device being used for nefarious purposes could quickly offset the savings.

b. Technical Support Increases

The infrastructure savings associated with CMD implementation have been observed to cause increased technical support costs. Organizations have been observed to see their costs grow dramatically due to the need to “support mobile device access to organizational resources and to help reduce risks when, not if, these devices are lost, stolen, or damaged” (Harvard Business Review Analytic Services, 2014, p. 1). The IT professionals that addressed the implementation of CMDs in Intel Corp. were concerned with the additional workload related to providing support for an increasing number of different devices each with differing configurations, operating systems, and levels of security or encryption (Chandrasekhar, 2013).

Any CMD implementation in the USMC could potentially increase the cost related to technical support. The USMC may need to hire civilian technical support staff or train more uniformed technical support staff.

c. Wireless Contracts

Wireless contracts can be expensive, and the costs related to the USMC funding of wireless contracts for all employees could have detrimental effects on the overall budget. The necessity of the Marine Corps to provide some sort of subsidy to offset the wireless contract costs to the individual is likely to be related to the type of implementation used and the degree to which the implementation mandates use. If the implementation allows employees the option to use their own device, the need to subsidize the wireless contract cost could be minimized. However, mandating the use of CMDs in a process could potentially lead to a situation where the USMC would be required to provide full funding for an employee's wireless contract.

In the cases of TTB, EEOC, and State of Delaware each organization was faced with a decision regarding the organization paying for employee wireless contracts. If an organization desires to subsidize the employees wireless contract costs they have several options ranging from paying the entire employee costs to providing a regular fixed stipend. In the case of the State of Delaware, the organization categorized users based on the mobile necessity of their job and then determines that employee's eligibility for wireless cost reimbursement. A determination by the organization not to compensate the employee for wireless costs did not preclude that employee from using their personal CMD (White House, 2012). This research recommends a similar policy in the USMC, allowing the maximum number of employees to benefit while only requiring subsidies for employees that require mobility in the completion of their duties.

2. Productivity Related Risks and Benefits

The business of defending United States in an increasingly globalized and interconnected world is complex and seems to become more difficult over time. This complexity results in DOD employees being required to "do more with less," which results in a desire to increase productivity and efficiency. Extensive research has been done by psychologists and companies to determine if the proliferation of digital communications devices is having a positive or negative effect on human productivity. Microsoft Canada (2015, p. 6), conducted a study on 2000 Canadians of various age, sex,

and technology use demographics and determined that overall, the human attention span has decreased from around 12 seconds in the year 2000 to eight seconds, which is slightly less than the nine-second attention span of the average goldfish. The popularity of smartphones, tablets, and the constant connectivity these technologies provide is unlikely to decrease, therefore it is beneficial to understand how these devices can be used to increase productivity and how they can be used to distract.

a. Increasing Employee Productivity

CMD implementation has the potential to allow employees to connect, collaborate, and be productive at anytime from anywhere that has connectivity. The DOD, and more specifically the Marine Corps operate around the globe and around the clock. Marines are indoctrinated into the mindset that they are “Marines 24/7.” This mindset is intended to instill the idea that the standards of conduct and values of a Marine are expected to be adhered to at all times, but in the digital age it has carried over into the way many Marines work. Marines are not explicitly required to have a personal mobile phone, but the researcher has observed that using a mobile phones email/text/voice capability is a primary means of conducting communications in a garrison environment. This is more common among the “key billet holders” (Commanding Officer, Executive Officer, etc.) who are required to be continuously on-call to make a decision or authorize action upon notification through their device.

The Marine Corps has recognized the value of CMDs in increasing command and control when connected to the Marine Corps Enterprise Network (MCEN), but currently limits the program to only government furnished equipment (GFE) and “privileged users” (Anderson, 2013, p. 11). “Privileged users” are limited based on the size of and budgetary authority of a unit, usually consisting of the more senior “key billet holders” of the unit. This leaves the remaining members of the unit to connect through their personal CMD, with no connectivity to the MCEN, limiting their ability to be productive outside of the confines of their workspace. Armano (2012) said, “it’s not about mobile as much as it is about understanding mobility.” The intent of any policy addressing CMD implementation needs to address the idea of mobility, not necessary mobile. “Mobility means

information, convenience, and social all served up on the go, across a variety of screen sizes and devices” (Armano, 2012).

Currently, the Department of Defense (DOD) and USMC are heavily dependent on desktop computers, or laptop computers that must remain plugged into a specific Ethernet port, which limits the mobility of the device and ultimately the productive capability of the employee tethered to that device. The researcher has observed that the mobile phone decreased the necessity of a land-line telephone, and in much the same way, CMDs are decreasing the necessity of stationary desktop/laptop in the office.

Harvard Business Review Analytic Services (2014, p. 2) research found that 85% of employees regularly used their mobile phone for work related activities, 65% of employees said BYOD made them more efficient at work, 51% said customer service improved, and 47% reported enhanced employee satisfaction. Following their BYOD implementation, Intel Corp. determined that their employees averaged a 57-minute daily increase in time spent on company-related work (Chandrasekhar, 2013, p. 6). The researcher has observed CMD proliferation and usage by Marines in USMC aviation squadrons and infantry units to be similar to the 85% employee usage statistic in the previously mentioned study. The researcher has observed these employees use their devices to conduct their daily work, in a limited capacity because of the restrictions on connecting their device to the MCEN. Allowing these employees to access the MCEN with CMDs could allow the USMC to see similar productivity and employee satisfaction gains to the previously mentioned study.

Marines own CMDs and in some circumstances have their device with them in the workplace. Employers must understand that their employees will “Interact with their mobile device” an average of 150 times per day (Panepinto, 2014). These mobile devices have become a primary interaction tool that affects how employees get their news and entertainment, how they learn, and how they fill at least some of their “white space” time during the day (Panepinto, 2014). Designing enterprise specific applications has helped companies and organizations achieve enhanced productivity (Panepinto, 2014). The Marine Corps could potentially design and develop Marine Corps specific applications and enhance employee productivity.

In practice, personally owned CMDs have an ability to provide access to an incredibly large amount of information that is well above that which is necessarily needed to complete daily tasks and/or be processed in the time available to complete those tasks. Rosen & Samuel (2015) discussed the need to better streamline the information individuals expose themselves to in a given day to only that which is necessary to complete the task assigned. This could be difficult to accomplish in the DOD, where constant situational awareness on a wide variety of tasks is often considered necessary in order to maintain good command and control. The researcher has observed one particular example of this issue in the use of the carbon copy (CC) and blind carbon copy (BCC) Email capability. The use of this capability has been observed to fill an individual's Email Inbox with messages that could potentially have little value to that individuals assigned tasks and provide an overload of information, negatively affecting productivity.

b. Devices of Digital Distraction

Allowing CMD use in the workplace has the potential to result in decreased productivity through some employees experiencing a level of distraction due to their devices. "The constant availability of information and entertainment takes advantage of our easily distracted minds" (Evans, 2015). In a study done by Ricoh Americas Corporation (2014), over three-quarters of employees used their device to check personal emails, two-thirds sent personal texts, and over one-third checked social media accounts or played games while at work. No company or organization that observes the results of this study is likely to be pleased with the amount of time that is spent on non-work activities. This same study described how the younger workers (18–34) were twice as likely as the next-closest age demographic to access social media or games on their device during work hours (RicoH Americas Corporation, 2014). The uniformed portion of the USMC is largely represented by this younger worker demographic (18–34), and it could expect that allowing greater usage of CMD in the workplace may lead to some workers succumbing to the distracting capability of their devices.

Multi-tasking is one way in which employees attempt to achieve greater efficiency in their work day. The evidence is not entirely supportive of this belief, in that the ability to effectively do two things at the same time is only possible when one task is “automatic” (Rosen & Samuel, 2015). Therefore, employees who believe they can effectively pay attention in a meeting and check their email at the same time are potentially neglecting one task or the other, or both. In the USMC, this issue could lead to important information being missed during a meeting, and lost efficiency due to mistakes and re-work.

CMDs have the ability to cause a digital distraction even when the user does not actually interact with the device (Stothart, Mitchum, & Yehnert, 2015, pp. 893–897). Current public service announcement campaigns on television, radio, etc., are concerned with the increased rate of vehicular accidents caused by drivers who are distracted and interacting with their devices. Large numbers of videos posted on websites like You Tube show distracted device users walking into fountains in public places or other embarrassing and dangerous situations. Stothart et al. (2015, pp. 893–897) conducted a study on students at Florida State University to determine the effect of various device notification stimuli on the participant’s ability to perform a task that required sustained attention. In their experiment, they attempted to distract the test subject with either a text message or a phone call and compared the results to a control group. The result of their study was that the decrease in performance of their test subjects who received calls or texts was similar in magnitude to the decrease in performance of distracted drivers, even when the subjects did not actively interact with their device (Stothart et al., 2015, p. 896).

These findings are applicable to the potential distractive capability of these devices in a USMC workplace. The USMC could possibly anticipate that a mechanic working on a difficult vehicular maintenance procedure, with his/her CMD nearby, receives a phone call that goes unanswered, but for a brief distracted second makes an error that is potentially costly or catastrophic. Or, perhaps a helicopter pilot is flying a training mission and is momentarily distracted by the subtle vibration of an incoming text to the CMD in his/her flight suit pocket. These devices have an undeniable ability to draw attention away, both long-term and short-term, from essential tasks.

It is possible that CMD technology in the workplace is both a cause of digital distraction and if appropriately utilized a productivity tool. It should be the goal of a CMD implementation policy to recognize the distraction capability and address it with appropriate expectations of employee behavior. The policy should also recognize the finite nature of the human attention span and use the technology to increase the productivity of the workforce. Evans (2015) recommendation for overcoming digital distraction was to ensure that emphasizing the use of productivity enhancing applications, encouraging employees to take a break from their devices during their work day, and disabling the notifications on their device to decrease the distracting capabilities.

The research done by Microsoft Canada (2015) has interesting insights that show how digital devices can act as both a productivity tool and a distraction device. For instance, if the DOD or USMC desires to increase the effectiveness of annual training, it would be beneficial to understand that a prolonged training period on the dangers of drinking and driving may not be as effective as putting a short message and a picture on an Internet access “splash page” before employees are able to access the Internet on their devices. Microsoft Canada (2015, p. 7) research also showed that 77% of 18- to 24-year-olds reach for their smartphone “When nothing is occupying my attention.” By understanding this reality and tailoring training to be conducted anywhere at any time on any device and for any duration, we may be able to see the increased effectiveness.

3. Gaining Organizational Competitive Advantage

The USMC does not necessarily have a business competitor in the way commercial organizations compete against each other for market share. The USMC does compete with other organizations (commercial sector and government) for quality employees both uniformed and civilian. This research addresses the competitive advantage that the USMC could gain in terms of recruiting and retaining a high quality workforce by pursuing a CMD implementation strategy.

Any implementation of CMD technology that enables the workforce to achieve mobility and the ability to conduct business process from non-standard locations could be seen as similar to the DOD Telework Policy. This policy recognizes that telework

policies “can serve as an effective recruitment and retention strategy” and “enhance DOD efforts to employ and accommodate people with disabilities” (Department of Defense, 2012, p. 2).

Gaining an organizational competitive advantage must be analyzed over a long time period. It is also the most difficult of the benefits to monetize, due to the fact that the use of CMDs is seen as an enabler to the human talent of the organization. As employees have the ability to network more easily, and access their work from anywhere at any time the company the potential of those employees to benefit the organization is likely to increase (Chandrasekhar, 2013). One way the USMC could gain a competitive advantage is by developing a positive perception among potential recruits that the Marine Corps is a forward leaning organization in the area of IT.

Today’s recruits—your new employees—live on their mobile devices. They’re going to judge you by how well your company allows them to live on them as well. With competition for tech talent at an all-time high and mobile tech savviness a common characteristic of new employees, demonstrating that your org “gets” the new IT landscape is incredibly important. (Panepinto, 2014)

The Marine Corps could benefit from recognizing the nature of their future employees and their concerns and desires with regard to their future employer. Implementing CMD technology into Marine Corps business processes, and increasing the mobility of the workforce could make the organization a more attractive place for high quality employees to work, which would potentially lead to a long term competitive advantage.

4. General Analysis Summary

Any implementation of CMD technology in the USMC is likely to have risks and benefits from the standpoint of the organization and the individual. Assessing the cost, productivity, and competitive advantage related risks and benefits is a good starting point for analyzing CMD implementation. The key to successful implementation of this technology is in analyzing the specific technology, how it is intended to be incorporated

into the business processes, and mitigating the risks in order to better understand specific risks and benefits.

B. CASE 1 ANALYSIS

In the background and explanation of case study 1, the use of CMD technology was presented as a potential means of addressing resource limitations and improving the efficiency of training and education in Marine Corps. This case focused on the capability to fill potential “white space” in a unit’s schedule by increasing the availability of computer based training modules. The use of CMDs in an educational environment is more commonly referred to as “mobile learning” and is defined as “the exploitation of ubiquitous handheld technologies, together with wireless and mobile phone networks to facilitate, support and enhance and extend the reach of teaching and learning” (Brown, 2010).

1. Sociotechnical Systems Theory Analysis

The key to determining the degree in which the benefits will be realized in any implementation requires analysis of the intersection of the new technology and the workforce. In order to accomplish this analysis, this research uses Sociotechnical Systems (STS) theory. A key part of this theory recognizes that a technology change in the organization is unlikely to succeed without a corresponding change in that organizations workforce.

In terms of the social impact on the organization of implementing this technology, it is unlikely that the authority structure, and the relationships among people would change (Bostrom & Heinen, 1977). Using an application to access training and education resources from a CMD does not require the Marine Corps to restructure its hierarchal organization. In the limited implementation of this case, interpersonal relationships would change only in that collaboration in certain training situations could be accomplished electronically rather than face to face. The “reward system” in terms of rewarding the Marines for completing their training already exists. Assuming that all Marines desire to be promoted to the next higher rank, the system already rewards Marines with points

towards promotion (junior enlisted Marines), and promotion boards give consideration to those Marines that actively pursue education.

Possibly the greatest social impact of implementing this technology in Case 1 is the minor changes in the attitudes and values that would be necessary. Marines would be required to demonstrate the maturity to use the devices for training and education during working hours, and not use them to look at social media or play games. This could result in greater reliance on SNCOs and NCOs to supervise their Marines use of these devices. Requiring these Marines to focus on supervision rather than their own training and education will then result in those SNCOs and NCOs being required to spend time outside of their normal working hours to complete their own training and education. This is not significantly different from what the researcher has observed currently takes place in the Marine Corps.

In terms of technical impact on the organization, this case assumes that the Marine Corps has the ability to develop a user friendly mobile application that provides access to computer based training and resources. Potential difficulties with regard to limiting access to only those individual authorized could create a situation in which the application is too difficult to access. Additionally, the issue of updating an individual Marine's training record could add complexity to the system. MarineNet currently allows Marines to take courses online and then automatically updates their individual training record. In an environment where the application has access to the Internet, this is less of an issue. However, if the application has the ability to download training and resources to the CMD and complete the training in an offline mode then the application will need some means of updating MarineNet during a subsequent application to server connection.

This case and the corresponding courses of action will have limited socio-technical implications due to the similarity between the current state of the process and the process following the implementation of CMDs in order to increase training and education availability. A larger issue for this case will be the acceptance of the technology at the end user level.

2. Technology Acceptance Model Considerations

Case 1 involves increasing the availability of the computer based training modules that the Marines already complete through desktop or laptop computers. This research makes the assumption that these Marines desire to complete their required training, and become more proficient in their particular specialty within the Marine Corps. The two key factors in assessing the acceptance of the technology by the end user are “Perceived Usefulness” and “Perceived Ease of Use” (Davis et al., 1989).

In terms of perceived usefulness, the end user must make a personal decision regarding how useful he/she believes the new technology to be. If the assumption is made that the individual Marine desires to become more proficient in their specialty and desires to be promoted, then usefulness of this technology should be relatively high. Case 1 proposes increasing availability of training and education resources to allow the individual the ability to more easily complete their required training. The issue in terms of acceptance of the technology will be whether or not the individual believes the usefulness outweighs any negative factors in terms of the ease of use of the technology.

The perceived ease of use, will be impacted by the quality of the application itself and the course of action (COA) implemented. This research assumes that the application will have the ability to provide computer based education and training resources to the CMD in a format that does not distort the digital media and operates without significant degradation in the quality of the training in comparison to the current state. Therefore, if the training itself is of the same quality, the ease of use will be entirely dependent on the user’s ability to easily navigate the applications interface, find the training he/she desires, complete that training, and then update their personal training record. This ease of use could also depend on the user’s familiarity with the CMD that the application is running on.

In COA 3 of this case the BYOD implementation strategy was proposed. A BYOD implementation would mean that the individual was able to access the training on a device of his/her choosing and therefore possibly more familiar with. The main ease of use issue regarding this COA is that some Marines may potentially not own a CMD. In

this case, those Marines would be required to borrow another individual's CMD, which may be unfamiliar to him/her, which would decrease that individual's perceived ease of use.

The solution to this issue is COA 2, which requires the Marine Corps to furnish a CMD to each Marine or each unit. The choose your own device (CYOD) implementation strategy allows the individual to operate on a CMD that they are familiar with, and ensures that all Marines have access to a CMD to complete their training. This COA has the potential to result in a higher cost to the organization due to the fact that it requires the government to develop an application that can run on multiple platforms, and to furnish the CMDs to the individuals.

COA 1, uses a here's your own device (HYOD) implementation strategy, which could address the cost of developing an application that works across platforms, due to the government choosing to provide only one platform with compatibility. The government could also save money, in comparison to COA 2, by purchasing only one type CMD and therefore buying the devices in bulk. This COA however has the potential to lower the perceived ease of use of some individuals that may not be familiar with the provided CMD platform. Each of these COAs provides a give and take in terms of the degree to which they will be perceived as easy to use and useful to the individual.

Using the Technology Acceptance Model, the end users should choose to use the new technology if the perceived usefulness is high in comparison to the negative aspects of the perceived ease of use. Therefore, if the application and the technology work well together and the individual believes they are useful in terms of their career development the technology should be accepted and used. If the application is difficult to operate, and the device is unfamiliar to the individual, the perceived ease of use is likely to be more of a negative factor and could potentially outweigh the positive useful aspect to the individual.

3. Confidentiality, Integrity, and Availability Analysis

Mobile learning through a CMD has the potential to increase productivity and collaboration in an educational environment. The IT policies at Naval Postgraduate School (NPS) recognize that their students' success depends on "the availability, flexibility, reliability, and capacity of the NPS academic technology infrastructure" (Naval Postgraduate School, 2009, p. 10). However, the benefits of implementing this technology do come with some risks. These risks can be mitigated to some degree with an appropriate implementation strategy and the use of technologies like virtual desktop infrastructure (VDI), trusted platform module (TPM), mobile device management (MDM), and application access controls. These technologies can improve confidentiality and integrity; however, they are often associated with some decrease in availability from the end users prospective.

Each COA presented in this case has varying levels of risk related to confidentiality, integrity, and availability (CIA) from the perspective of the organization. The training and education resources that the application provides access to are, for the purposes of this research, not classified and confidentiality is a minor concern to the organization. Assuming that the application is developed with multi-factor authentication the Marine Corps could be reasonably assured that only those individuals that have a reason to access the resources are able to access the resources. The application should be set up in a manner that does not allow an individual to use the application to alter the training or resources in any way, which leaves only the issue of training record update integrity. The application should only be able to access and update the training record of the authenticated user using the device.

One integrity issue that this technology would be vulnerable to fraudulent training completion. In this hypothetical scenario, a Marine gains access to the application and then allows another individual to complete the training for him/her. This issue is not likely to be prevented with any technology that the researcher is aware of. This researcher has not personally observed this occur, however it is an issue of the current MarineNet system.

With respect to the proposed COAs in this case study, COA 3 has the highest potential for risk in terms of CIA. Allowing individual Marines to access and store the organizational information from MarineNet on their personal devices is potentially riskier than a government furnished device. This would be due in part to the individual security settings of the personally owned device and the other applications installed on the device. COA 1 and COA 2 are essentially variations on a program that requires the government to furnish a device to the individual. Because the government furnishes the device, the government could potentially have greater oversight on the device and more tightly control the settings and applications, thereby potentially lowering the confidentiality and integrity risks.

4. Analysis Summary

Allowing CMD access to training and education courses and resources currently available on MarineNet in any of the COAs developed for this case study presents risk to the organization. The new technology has a risk of not being accepted by the individuals expected to utilize it, making the implementation unsuccessful. Additionally, risks exist in terms of confidentiality and integrity of the organizations data. The degree to which these risks are outweighed by the potential benefits should be considered before pursuing any of these COAs.

C. CASE 2 ANALYSIS

In the background and explanation of case study 2, the use of CMD technology was presented as a potential means of increasing collaboration and improving the efficiency of squadron flight schedule development in the Marine Corps. This case focused on the capability of key stakeholders to collaborate in the development and approval process of a squadron flight schedule. The daily flight schedule development and approval process was described in detail to show that a properly developed mobile application running on a CMD could provide make the process more efficient.

1. Sociotechnical Systems Theory Analysis

The squadron daily flight schedule development and approval process is a very social process. In its current state, the process involves the technology only in the development, and after the approval. Through the use of an application running on CMDs in the hands of the key stakeholders, the technology is involved throughout the process. From a STS perspective, the implementation of this technology could have implications on the social and technical sides of the process.

In terms of social impact, the implementation of this technology could alter the relationships among the key stakeholders. In this implementation, the application would have the ability to allow real time collaboration between all of the key stakeholders, and potentially the Commanding Officer during all stages of flight schedule development. This change in relationships among the key stakeholders is one of the major potential benefits of implementing CMD technology into this process. Rather than the current system of developing the schedule and allowing each individual key stakeholder to make his/her changes with no visibility of those change to the others, this technology is proposed to allow real time visibility of those changes. The benefit of altering the relationships and increasing collaboration would be to decrease the work and re-work time of the schedule.

In terms of the technical impact, this technology should decrease the complexity of the process. Decreasing complexity and increasing the efficiency in terms of time is the major benefit of the technology in this case. If the application and the implementation of the technology increases complexity of the process, then the implementation would likely fail.

2. Technology Acceptance Model Considerations

Case 2 involves the development of an application allowing collaborative capability in squadron flight schedule development. The main technology factor in this case is the application and its ability to run on a CMD. The collaborative capability and the mobility of the key stakeholder are the two biggest benefits gained by implementing this technology. Using the Technology Acceptance Model to analyze this case, each COA

is likely to have varying degrees of perceived usefulness and perceived ease of use from the perspective of the end user (key stakeholder).

Perceived usefulness is the major factor in this case in determining how the technology will be accepted by the end user. The degree to which the key stakeholders believe the application increases collaboration, decreases the amount of time they spend on development and approval, and the additional freedom they have to complete the task away from their traditional workspace will all factor into the perceived usefulness of the technology. This research assumes that the application is developed to address these factors affecting perceived usefulness. Assuming that the application is developed for a specific CMD platform (as is the case in COA 1), or multiple platforms (as is the case in COA 2, and 3) there should be no difference in perceived usefulness between the respective COAs.

The perceived ease of use of this technology is affected by the COA selected. In COA 1, a HYOD implementation plan was proposed. This COA has the potential for slightly lower perceived ease of use. This is due to the potential for a particular CMD platform being selected, and the individual key stakeholder lacking familiarity with that platform. COA 2 and COA 3 both decrease the likelihood of this outcome by increasing the number of platforms that are supported. Additionally, regardless of COA selected, if the application is developed without significant input from the individuals that are experts in the process, the potential exists that the application has low usefulness and low ease of use. In this scenario, the implementation is likely to fail to improve the process.

3. Confidentiality, Integrity, and Availability Analysis

Similar to Case 1, CMD technology implementation in this case has the potential to benefit the process in terms of information availability. This benefit comes at a cost of potential threats to confidentiality and integrity of the data. Squadron daily flight schedules are not classified, but they are protected from disclosure for operational security reasons. The M-SHARP system contains personally identifiable information (PII) and unit readiness statistics that require protection from threats to confidentiality

and integrity. With access to the system, and bad intentions, an individual could potentially cause erroneous information to be inserted causing a lack of data integrity.

Assuming that the application is developed with multi-factor authentication the Marine Corps could be reasonable assured that only those individuals that have a reason to access the resources are able to access the resources. This could prevent issues with regard to confidentiality. Additionally, the application could be set up in a manner that does not allow an individual to use the application to alter the readiness information in any way. In this configuration the application would be able to “read only” the readiness and qualification information in the system, and would be able to “write” only to the daily flight schedule. This would limit the potential for issues with integrity.

Each individual COA would have slightly different risk levels with regard to CIA. COA 1 implementation, has the potential for the least risk. In this COA, the government owns all the devices that are able to use the application, and is responsible for maintaining the configuration and security of the CMDs. COA 2 has a potential has similar risk to COA 1. In this implementation, the government owns a selection of CMD platforms that the individual is able to use. The CIA risk is slightly higher here, due to the requirement of the government to manage multiple platforms settings and security. Each of these COAs has the potential to limit availability, due to the limited number of CMDs allotted to the unit. COA 3 increases availability due to the development of the application to run on multiple CMD platforms. Additionally, in this COA the number of devices with access to the system is limited by the number of authorized users the organization chooses to allow (assuming that all the key stakeholders and their alternates own a CMD). This COA has the potential for the highest risk in terms of confidentiality and integrity, in that it would require the organization to manage access.

4. Analysis Summary

Implementing CMD technology into the squadron daily flight scheduling process in any of the COAs developed for this case study presents risk to the organization. Risks exist in terms of confidentiality and integrity of the organizations data. Through an appropriately developed application, and diligent access management by the organization

these risks could potentially be mitigated to an acceptable level. The degree to which the resultant risk is outweighed by the potential benefits should be considered before pursuing any of these COAs.

D. CASE 3 ANALYSIS

In the background and explanation of Case 3, the use of CMD technology was presented as a potential means of increasing collaboration, interoperability, and improving the efficiency of the member assigned to conduct an aviation mishap investigation. This case focused on the issues of training the members of the board, changing out members of the board, and collaborating on the investigation. The aviation mishap investigation process was described to show the complexity of the process and that a properly developed mobile application running on a CMD could provide make the process more efficient.

1. Sociotechnical Systems Theory Analysis

The process of conducting an aviation mishap investigation is by its very nature a social process. In its current state, the process involves several individuals conducting investigative tasks within their area of expertise independently and then periodically collaborating to develop the investigation report. In this process, the individuals use personal CMDs to conduct portions of the investigation, but must use a laptop or desktop computer to input the evidence and findings into the online investigation report system. From a STS perspective, the implementation of this technology could have implications on the social and technical sides of the process.

In terms of social impact, the implementation of this technology could alter the relationships among the mishap board members. In this implementation, the application would have the ability to allow members to collaborate during the investigation and development of the investigation report. The additional benefit of implementing this technology is the interchangeability of the members on the board. The application could allow new members to be assigned and removed from the board as desired by the Commanding Officer or investigative authority. The availability of the application on CMDs has the potential to allow any member of the squadron with the application to

collect digital evidence and provide it to the mishap board. If the application were developed with various roles, every member of the command with a CMD could be given the ability to take pictures or give statements to the board through the application, without having access to the entire body of evidence and findings.

In terms of the technical impact, this technology is likely to increase the complexity of the process to a certain degree. Allowing a potentially larger group of individuals to collect evidence and provide that evidence to the board has the potential to cause redundant information to be provided. Additionally, this application could increase the amount of irrelevant information causing the investigation to potentially take more time to complete than necessary.

The second technical impact is that the application is unlikely to replace the desktop or laptop in the development of the investigation report. CMDs are recognized as having a keyboard capability (either touchscreen or peripheral device), however the researcher has observed these devices to be cumbersome when doing a significant amount of writing in a text editor program. These technical issues and the social impact of this technology could impact the acceptance of this technology in the process.

2. Technology Acceptance Model Considerations

Case 3 involves the development of an application allowing data collection and a collaborative capability in investigating an aviation mishap. The main technology factor in this case is the application and its ability to run on a CMD. The mobility of the individuals conducting the investigation is the biggest benefit gained by implementing this technology. Using the Technology Acceptance Model to analyze this case, each COA is likely to have varying degrees of perceived usefulness and perceived ease of use from the perspective of the end user.

Perceived usefulness is the major factor in this case in determining how the technology will be accepted by the end user. It is possible that the use of this technology is only perceived to be useful from the viewpoint of the Aviation Safety Officer and the members of the mishap board. These individuals could benefit, in terms of efficiency, through the ability to collect evidence and collaborate with other members of the board.

The degree to which these individuals believe these benefits will be realized through using CMD technology will directly impact their perception of usefulness. Assuming that the application is developed for a specific CMD platform (as is the case in COA 1), or multiple platforms (as is the case in COA 2, and 3) there should be no difference in perceived usefulness between the respective COAs.

Similar to Case 2's analysis, the perceived ease of use of this technology is affected by the COA selected. In COA 1, a HYOD implementation plan was proposed. This COA has the potential for slightly lower perceived ease of use, due to the potential for an individual lacking familiarity with the particular CMD platform selected. COA 2 and COA 3 both decrease the likelihood of this outcome by increasing the number of platforms that are supported. Similar to Case 2's analysis, if the application is developed without significant input from the experts in the process, the potential exists that the application has low usefulness and low ease of use. From the user's perspective, if the application is well developed and runs on a CMD platform that he/she is familiar with, the technology should be perceived as having a high ease of use. If the user's perception is that the positive benefits in terms of usefulness of the technology are higher than the negative aspects of ease of use, the technology could be accepted.

3. Confidentiality, Integrity, and Availability Analysis

CMD technology implementation in this case has the potential to benefit the process in terms of mobility and collaboration. To gain these benefits, the CMD and the application increase the availability of data. This benefit comes at a cost of potential threats to confidentiality and integrity of that data. The system currently used in aviation safety investigation contains PII, and privileged information that require protection from threats to confidentiality and integrity.

Similar to Case 2's analysis, an individual with bad intentions could potentially cause erroneous information to be inserted causing a lack of data integrity. Beyond that, the compromise of privileged information could have criminal implications and cause embarrassment to the Department of Navy (DON). Additionally, the entire aviation safety mishap investigation process could experience a reluctance to provide information

by witnesses due to a fear that privileged information will be compromised on the new system. The need for confidentiality could supersede the desire for increased availability in this case. This research recognizes that if the CMD and application are unable to provide acceptable confidentiality of the data, then the implementation could fail.

In this case, multi-factor authentication may not provide the DON enough assurance that only those individuals that have a reason to access the resources are able to access the resources. It may be necessary to create different roles in the application, that allow certain individuals the ability to put information into the system with no information retrieval capability, while allowing the investigation board members full access. In this scenario, any member of a squadron could have the application on their personal CMD and take pictures, record audio/video, and scan documents for upload into the system. Those individuals would have no ability to access anything in the system to include other data or board deliberations. This could prevent the disclosure of privileged information to an acceptable level and address potential integrity and confidentiality issues.

Each individual COA would have slightly different risk levels with regard to CIA. COA 1 implementation has the potential for the least risk. In this COA, the government owns all the devices that are able to use the application, and is responsible for maintaining the configuration and security of the CMDs. This would provide the lowest risk to confidentiality and integrity, but would minimize the positive aspects of availability to only individuals with government furnished CMDs. COA 2 has a potential for similar risk to COA 1. In this implementation, the government owns a selection of CMD platforms that the individual is able to use. The CIA risk is slightly higher here, due to the requirement of the government to manage multiple platforms settings and security. COA 3 increases availability due to the development of the application to run on multiple CMD platforms. The number of devices with access to the system in this COA is limited by the number of authorized users the organization chooses to allow (assuming that all the key stakeholders and their alternates own a CMD). This COA has the potential for the highest risk in terms of confidentiality and integrity, in that it would require the organization to manage the roles of individuals using the application.

4. Analysis Summary

Implementing CMD technology into the investigation process of an aviation mishap presents risk to the organization. In terms of confidentiality, disclosure of privileged information could be highly detrimental to the process. In terms of integrity, unauthorized or unwanted alteration of the data could lead to erroneous investigation findings leading to similar mishaps occurring. Through an appropriately developed application, and diligent role based access management by the organization these risks could potentially be mitigated to an acceptable level. The degree to which the resultant risk is outweighed by the potential benefits should be considered before pursuing any of these COAs.

E. SUMMARY

Each of the cases and their individual COAs vary in terms of risks and benefits to the organization. These cases represent three very different processes that could potentially benefit from allowing CMD technology in the USMC. This research analyzed each potential case and COA in terms of STS theory, the Technology Acceptance Model, and the CIA risks versus benefits. The specific analyses of each of these cases display that a single “best” implementation strategy for all processes is available. Each case should be looked at individually, and an individual solution selected in order to minimize the risks and maximize the benefits.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The cases developed in this research, and the corresponding analysis has shown that the implementation of commercial mobile devices (CMD) into business processes in the United States Marine Corps (USMC) is a complex balance between increasing information availability and information security. Each of the individual cases shows the complexity of the integration of the technology with the users in terms of sociotechnical systems (STS) theory. The cases show that, in terms of the technology acceptance model (TAM), that “perceived usefulness” is relatively constant between the courses of action (COA). However, “perceived ease of use” varies with the implementation strategy selected, which directly affects the user acceptance of the technology. Finally, the cases and analysis show that increasing availability of information has a corresponding elevated risk associated with the confidentiality and integrity of the information.

B. FINDINGS AND RECOMMENDATIONS

The findings and recommendations of this research make the assumption that the USMC desires to pursue implementing CMD technology in the individual case’s process. Within each individual case, a specific COA is recommended as the best choice from the perspective of the organization. It is assumed that the organization desires to minimize cost and risks, while maximizing user satisfaction and benefits. In some of these cases, an additional modified hybrid COA is recommended which would need to be researched in greater detail by follow-on studies to determine feasibility.

1. Case 1 Findings

Case 1 involved the use of CMD technology to address resource limitations and improve training and education efficiency in the USMC. The findings of the analysis of the individual implementation COAs are displayed in Table 3.

Table 3. Case 1 Findings

| CASE 1 FINDINGS | | |
|-------------------------|--|---|
| | Strengths | Weaknesses |
| COA 1 (HYOD) | <ul style="list-style-type: none"> • Lowest potential cost to the government in terms of technical support • Lowest cost in application compatibility • Lowest risk to the organization in terms of confidentiality and integrity • Lowest risk to the organization in terms of confidentiality and integrity | <ul style="list-style-type: none"> • Requires government to furnish a specific device configuration • Potential for high cost to government in terms of purchasing a specific device configuration • Lowest potential for user familiarity • Lower “perceived ease of use” if individual is unfamiliar with provided device |
| COA 2 (CYOD) | <ul style="list-style-type: none"> • Moderate potential for user familiarity • Moderate potential cost to the government in terms of technical support • Moderate cost in application compatibility • Lower risk to the organization in terms of confidentiality and integrity | <ul style="list-style-type: none"> • Requires government to furnish a collection of device configurations • Potential for highest cost to government in terms of purchasing multiple device configurations • Lower “perceived ease of use” if individual is unfamiliar with provided device |
| COA 3 (BYOD) | <ul style="list-style-type: none"> • Highest user familiarity • Potential for highest “perceived ease of use” • Lowest potential cost to government in terms of purchasing devices • Highest potential for increasing availability of access • Highest potential for widespread use in the organization | <ul style="list-style-type: none"> • Assumes all users own a CMD • Lower “perceived ease of use” if user does not own a CMD • Highest potential cost in terms of technical support • Highest cost to the individual user in terms of purchasing device • Highest cost in application compatibility • Highest risk to the organization in terms of confidentiality and integrity |

The implementation of this technology has the potential to apply to all Marines in the USMC, both active duty and reservists. The number of potential users in this case could make the pursuit of COA 1 and COA 2 cost prohibitive, due to the requirement for the USMC to purchase devices for all. Due to this main factor, it is the recommendation of this research that COA 1 is pursued by the USMC. This COA minimizes the cost to the government in terms of purchasing CMDs and takes advantage of the devices that users already own. This COA also takes advantage of the user's familiarity with their device, which could lead to a higher acceptance of the technology into the process.

COA 3 could result in higher costs in terms of application compatibility and technical support. These potential costs are minimal in comparison to the cost of acquiring and maintaining the number of devices required in COA 1 and COA 2. The main weakness of selecting COA 3 is the expectation that potential users may not own a CMD. Because of this expectation, some users would potentially not have the ability to access the information and realize the benefits. It is therefore suggested that a hybrid COA may be the most beneficial.

The possible hybrid COA involves selecting COA 3, and a limited COA 1 implementation. In this COA, the application could be developed to run on user owned CMDs, providing access to those individuals. The USMC could then purchase a limited number of government furnished CMDs to the individual units for temporary loan to individuals that do not own their own CMD. This would present an additional cost to the government, but would maximize utilization of the technology.

2. Case 2 Findings

Case 2 involved the use of CMD technology to improve collaboration and efficiency in the squadron daily flight schedule development process. The findings of the analysis of the individual implementation COAs are shown in Table 4.

Table 4. Case 2 Findings

| CASE 2 FINDINGS | | |
|-------------------------|--|---|
| | Strengths | Weaknesses |
| COA 1 (HYOD) | <ul style="list-style-type: none"> • Lowest potential cost to the government in terms of technical support • Lowest cost in application compatibility • Lowest risk to the organization in terms of confidentiality of PII • Lowest risk to the organization in terms of integrity of readiness data | <ul style="list-style-type: none"> • Requires government to furnish a specific device configuration • Potential for high cost to government in terms of purchasing a specific device configuration • Lowest potential for user familiarity • Lower “perceived ease of use” if individual is unfamiliar with provided device |
| COA 2 (CYOD) | <ul style="list-style-type: none"> • Moderate potential for user familiarity • Moderate potential cost to the government in terms of technical support • Moderate cost in application compatibility • Lower risk to the organization in terms of confidentiality and integrity | <ul style="list-style-type: none"> • Requires government to furnish a collection of device configurations • Potential for highest cost to government in terms of purchasing multiple device configurations • Lower “perceived ease of use” if individual is unfamiliar with provided device |
| COA 3 (BYOD) | <ul style="list-style-type: none"> • Highest user familiarity • Potential for highest “perceived ease of use” • Lowest potential cost to government in terms of purchasing devices • Highest potential for increasing availability of access • Highest potential for larger pool of users collaborating | <ul style="list-style-type: none"> • Assumes all users own a CMD • Lower “perceived ease of use” if user does not own a CMD • Highest potential cost in terms of technical support • Highest cost to the individual user in terms of purchasing device • Highest cost in application compatibility • Highest risk to the organization in terms of confidentiality and integrity |

The implementation of this technology would affect a much smaller group of users than Case 1. This case only addressed USMC aviation squadron scheduling, and focused primarily on the interactions between key stakeholders in the process. The analysis of this case addressed the elevated need for confidentiality of personally identifiable information (PII) and maintaining the integrity of the squadron readiness data. Due to the relatively small number of potential CMDs requiring access, and the elevated risks, it is the recommendation of this research that either COA 1 or COA 2 be pursued by the USMC.

COA 2 would result in the highest cost to the organization in terms of acquiring devices and providing them to the key stakeholders. The cost associated with COA 1 could be slightly lower than COA 2, however COA 2 has the advantage of higher user familiarity and therefore higher “perceived ease of use” over COA 1. To maximize user familiarity and “perceived ease of use” in a COA 1 implementation, the USMC could do additional research on the key stakeholders to determine the most prevalent CMD among that group.

The possibility of a hybrid implementation of CMD technology exists in this case where COA 1 or COA 2 is selected for the key stakeholders, while developing the application for use on user owned CMDs in a limited capacity. In this hybrid COA, the key stakeholders would use their government furnished CMD to collaborate on the development of the daily flight schedule. The remaining members of the squadron could access the application for information purposes, and providing their availability in the “snivel log.” Each authorized user in the squadron with a CMD could be allowed to see the daily/weekly/monthly flight schedules. Additionally, individual aircrew personnel could provide the Pilot Training Officer their availability to be scheduled based on their personal schedules.

3. Case 3 Findings

Case 3 involved the use of CMD technology to improve collaboration and efficiency in the investigation of aviation mishap. The findings of the analysis of the individual implementation COAs are given in Table 5.

Table 5. Case 3 Findings

| CASE 3 FINDINGS | | |
|-------------------------|--|--|
| | Strengths | Weaknesses |
| COA 1 (HYOD) | <ul style="list-style-type: none"> • Lowest potential cost to the government in terms of technical support • Lowest cost in application compatibility • Lowest risk to the organization in terms of inappropriate disclosure of privileged information • Lowest risk to the organization in terms of integrity of investigation data | <ul style="list-style-type: none"> • Requires government to furnish a specific device configuration • Potential for high cost to government in terms of purchasing a specific device configuration • Lowest potential for user familiarity • Lower “perceived ease of use” if individual is unfamiliar with provided device |
| COA 2 (CYOD) | <ul style="list-style-type: none"> • Moderate potential for user familiarity • Moderate potential cost to the government in terms of technical support • Moderate cost in application compatibility • Lower risk to the organization in terms of confidentiality and integrity | <ul style="list-style-type: none"> • Requires government to furnish a collection of device configurations • Potential for highest cost to government in terms of purchasing multiple device configurations • Lower “perceived ease of use” if individual is unfamiliar with provided device |
| COA 3 (BYOD) | <ul style="list-style-type: none"> • Highest user familiarity • Potential for highest “perceived ease of use” • Lowest potential cost to government in terms of purchasing devices • Highest potential for increasing availability of access • Highest potential for larger pool of users collaborating | <ul style="list-style-type: none"> • Assumes all users own a CMD • Lower “perceived ease of use” if user does not own a CMD • Highest potential cost in terms of technical support • Highest cost to the individual user in terms of purchasing device • Highest cost in application compatibility • Highest risk to the organization in terms of inappropriate disclosure of privileged information • Highest risk to the organization in terms of integrity of investigation data |

The implementation of this technology would affect a smaller group of users than Case 1 or Case 2. Additionally, the frequency of use of the technology is much less frequent than Case 1 or Case 2. The analysis of this case addressed the elevated need for confidentiality of privileged information and maintaining the integrity of the investigation data and findings. Due to the relatively small number of potential CMDs requiring access, the infrequent need for access, and the elevated risks, it is the recommendation of this research that COA 1 be pursued by the USMC.

COA 1 has the lowest risk to the organization in terms of inappropriate disclosure of privileged information. This is important because, disclosure of this information could have catastrophic effects on trust and confidence in the mishap investigation process by potential witnesses. COA 1 has the lowest risk to the organization in terms of integrity of investigation data. This is important because, accurate investigation data and findings can directly impact the ability of the aviation community to prevent similar mishaps from occurring. Erroneous findings along with not accurately determining the cause of the mishap could lead to loss of life and equipment. Because of these issues, confidentiality and integrity are prioritized above availability in this case.

It is recommended that in implementing COA 1, the USMC acquire CMDs and assign them directly to the squadron Aviation Safety Officer (ASO). The ASO could then maintain accountability of the devices and issue them on an “as needed” basis to the members of the aviation mishap board. It would be the responsibility of the ASO to maintain these CMDs and provide training on their appropriate use to the aviation mishap board members.

4. Findings Summary

Three different cases were developed in this research, and each case has been found to minimize risk and maximize benefit through a different implementation strategy. This is due to the differing requirements between the cases in terms of confidentiality, integrity and availability of information. This research shows that a single “best” implementation strategy of CMD technology for all cases does not exist.

C. RECOMMENDATIONS FOR FUTURE RESEARCH

This research focused on the risks and benefits associated with implementing CMD technology. The risks and benefits were discussed both in general and with a more case specific focus. The confidentiality and integrity risks could change as CMD technology and application security improve. Therefore, future research should consider the state of technology at the time of implementation as well as the likely future state of technology in these areas.

To maximize technology acceptance, it is recommended that future research survey the potential pool of users in any implementation case to determine the anticipated perception among those users regarding usefulness of the technology. This survey research could also determine the expected perceived ease of use by determining the personal CMD ownership among the users.

LIST OF REFERENCES

- Adkison, J. D. (2015). *Data supporting mobile application development for use within the Marine Air-Ground Task Force* (Master's thesis). Retrieved from Calhoun: <http://hdl.handle.net/10945/47220>
- Anderson, R. L. (2013). *Marine Corps commercial mobile device strategy*. Washington, DC: Headquarters U.S. Marine Corps. Retrieved from: [http://www.hqmc.marines.mil/Portals/156/Newsfeeds/SV%20Documents/20130411 Marine Corps Commercial mobile device strategy Final.pdf](http://www.hqmc.marines.mil/Portals/156/Newsfeeds/SV%20Documents/20130411_Marine_Corps_Commercial_mobile_device_strategy_Final.pdf)
- Armando, A., Costa, G., & Merlo, A. (2013). Bring your own device, securely. *Proceedings of the 28th Annual ACM Symposium on Applied Computing—SAC '13*. doi:10.1145/2480362.2480707
- Armano, D. (2012, July 18). The future isn't about mobile; It's about mobility. *Harvard Business Review*. Retrieved on 25 May, 2016. Retrieved from <https://hbr.org/2012/07/the-future-isnt-about-mobile-its>
- Barkhuus, L. (2005). "Bring your own laptop unless you want to follow the lecture." *Proceedings of the 2005 International ACM SIGGROUP Conference on Supporting Group Work—GROUP '05*. doi:10.1145/1099203.1099230
- Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Part I: The causes. *MIS Quarterly*, 1(3), 17. doi:10.2307/248710
- Brown, J. (2010). Can you hear me now? *T + D*, 64(2), 28–30. Retrieved from <http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/227021446?accountid=12702>
- Cebrowski, A. K., & Garstka, J. J. (1998). Network-centric warfare: Its origin and future. *US Naval Institute Proceedings*, 124(1), 28–35. Retrieved from http://www.kinecton.com/ncoic/new_origin_future.pdf
- Chairman Joint Chiefs of Staff. (2015). *The national military strategy of the United States of America 2015*. Washington, DC: Office of the Chairman of the Joint Chiefs of Staff. Retrieved from [http://www.jcs.mil/Portals/36/Documents/Publications/2015 National Military Strategy.pdf](http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf)
- Chandrasekhar, R. (2013). Intel Corp.—Bring your own device. *Richard Ivey School of Business, The University of Western Ontario*. Retrieved from <https://hbr.org/download/292882214/W13035-PDF-ENG/W13035-PDF-ENG>

- Commandant of the Marine Corps. (2014). *Expeditionary Force 21—Forward and ready: Now and in the future*. Washington, DC: Department of the Navy, Headquarters United States Marine Corps. Retrieved from http://www.mccdc.marines.mil/Portals/172/Docs/MCCDC/EF21/EF21_USMC_Capstone_Concept.pdf
- Costantino, G., Martinelli, F., Saracino, A., & Sgandurra, D. (2013). Towards enforcing on-the-fly policies in BYOD environments. *2013 9th International Conference on Information Assurance and Security (IAS)*. doi:10.1109/isias.2013.6947734
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319. doi:10.2307/249008
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8), 982–1003. doi:10.1287/mnsc.35.8.982
- Department of Defense. (2012, Apr. 14). Telework policy (DODI 1035.01). Washington, DC: Under Secretary of Defense for Personnel and Readiness, Jo Ann Rooney. Retrieved from <http://www.dtic.mil/whs/directives/corres/pdf/103501p.pdf>
- Department of Defense Chief Information Officer (DOD CIO). (2006, Apr. 18). Protection of sensitive Department of Defense (DOD) data at rest on portable computing devices [Memorandum]. Washington, DC: John G. Grimes. Retrieved from <http://www.doncio.navy.mil/Download.aspx?AttachID=785>
- Department of Defense Chief Information Officer (DOD CIO). (2016, Mar. 17). *Management of the Department of Defense information enterprise* (DODD 8000.01). Washington, DC: Robert O. Work. Retrieved from <http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf>
- Department of Defense Chief Information Officer (DOD CIO). (2012, Jun. 8). *Department of Defense mobile device strategy*. Washington, DC: Teresa M. Takai. Retrieved from <http://archive.defense.gov/news/DODmobilitystrategy.pdf>
- Department of Defense Chief Information Officer (DOD CIO). (2013, Feb. 15). *Department of Defense commercial mobile device implementation plan*. Washington, DC: Teresa M. Takai. Retrieved from <http://archive.defense.gov/news/DODCMDImplementationPlan.pdf>
- Department of Defense Chief Information Officer (DOD CIO). (2014a, May 21). *Interoperability of information technology (IT), including national security systems (NSS)* (DODI 8330.01). Washington, DC: David L. De Vries. Retrieved from <http://www.dtic.mil/whs/directives/corres/pdf/833001p.pdf>

- Department of Defense Chief Information Officer (DOD CIO). (2014b, Mar. 12). *Risk management framework (RMF) for DOD information technology (IT)* (DODI 8510.01). Washington, DC: Teresa M. Takai. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf
- Department of the Navy: Headquarters United States Marine Corps. (2013, Aug. 30). *Infantry training and readiness manual* (NAVMC 3500.44B). Washington, DC: T. M. Murray. Retrieved from <http://www.marines.mil/Portals/59/Publications/NAVMC%203500.44B.pdf>
- Department of the Navy: Headquarters United States Marine Corps. (2016, Feb. 05). *Aviation training and readiness program manual* (NAVMC 3500.14D). Washington, DC: J. W. Lukeman. Retrieved from <http://marineit.freshdesk.com/helpdesk/attachments/11002755668>
- Department of the Navy Office of the Chief of Naval Operations. (2009, Nov. 23). *Naval air training and operating procedures standardization general flight and operating instructions* (OPNAVINST 3710.7U). Washington, DC: D. L. Philman. Retrieved from http://www.med.navy.mil/sites/nmotc/nami/arwg/Documents/WaiverGuide/OPNAVINST_3710_7U_General_NATOPS.pdf
- Department of the Navy Office of the Chief of Naval Operations (OpNav) (2014, 13 May). *Naval aviation safety management system* (OPNAVINST 3750.6S). Washington, DC: K. J. Norton. Retrieved from <https://doni.daps.dla.mil/Directives/03000%20Naval%20Operations%20and%20Readiness/03-700%20Flight%20and%20Air%20Space%20Support%20Services/3750.6S.pdf>
- Epstein, R. J. (2014). *Policy and policy formulation considerations for incorporation of secure mobile devices in USMC ground combat units* (Master's thesis). Retrieved from Calhoun <http://hdl.handle.net/10945/43908>
- Evans, L. (2015, July 1). How the device you can't live without is also destroying your productivity. *Fast Company*. Retrieved from <http://www.fastcompany.com/3047705/the-future-of-work/how-the-device-you-cant-live-without-is-also-destroying-your-productivity>
- Federal CIO. (2012, May 23). *Digital government: Building a 21st century platform to better serve the American people*. Washington, DC: Executive Office of the President. Steven VanRoekel. Retrieved from <http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf>
- Federal Information Security Management Act (FISMA) of 2002, H.R. 2458–48. SEC. 301, §3541 (2002). Retrieved from: <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>

- Gajar, P. K., Ghosh, A., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, 4(4), 62–70. Retrieved from <http://www.rroij.com/open-access/bring-your-own-device-byod-security-risks-and-mitigating-strategies-62-70.php?aid=38224>
- Geels, F. W. (2004). From sectoral systems of innovation to socio-technical systems. *Research Policy*, 33(6-7), 897–920. doi:10.1016/j.respol.2004.01.015
- Harvard Business Review Analytic Services (2014, November 1). Making BYOD work: Balancing productivity and security. *Harvard Business Review*. Retrieved on 25 May, 2012. Retrieved from <https://hbr.org/sponsored/2014/11/making-byod-work-balancing-productivity-and-security>
- Jaramillo, D., Katz, N., Bodin, B., Tworek, W., Smart, R., & Cook, T. (2013). Cooperative solutions for bring your own device (BYOD). *IBM J. Res. & Dev.*, 57(6), 5:1–5:11. doi:10.1147/jrd.2013.2279600
- Lennon, R. G. (2012). Bring your own device (BYOD) with Cloud 4 education. *Proceedings of the 3rd Annual Conference on Systems, Programming, and Applications: Software for Humanity—SPLASH '12*. ACM, USA, 171-180 doi:10.1145/2384716.2384771
- Marine Corps concepts and programs—End strength. (2015). Retrieved July 13, 2016, from <https://marinecorpsconceptsandprograms.com/programs/manpower/end-strength>
- Marine Corps University vision statement. (n.d.). Retrieved July 13, 2016, from <https://www.mcu.usmc.mil/SitePages/aboutus/Vision%20Statement.aspx>
- MarineNet annual training curriculums in support of MCBul 1500. (2013). Retrieved July 13, 2016, from https://www.mcu.usmc.mil/cdet/docs/marinenet/ttps/Annual_1Nov13.pdf?mobile=0
- MarineNet software baseline requirements. (n.d.). Retrieved July 13, 2016, from <https://www.marinenet.usmc.mil/MarineNet/portal/PageView.aspx?pg=ComputerRequirements.aspx>
- MarineNet tips, tools & practices. (2011). Retrieved July 13, 2016, from https://www.mcu.usmc.mil/cdet/docs/marinenet/ttps/MNET-TTP_MarineNet_101.pdf?mobile=0
- Marines operating forces presence detail MCRD Parris Island. (n.d.). Retrieved July 13, 2016, from http://www.marines.com/operating-forces/presence-detail/-/presence/detail/PRES_LOC_PARRISISLAND

- Marines operating forces presence detail MCRD San Diego. (n.d.). Retrieved July 13, 2016, from http://www.marines.com/operating-forces/presence-detail/-/presence/detail/PRES_LOC_SANDIEGO
- Marines Sierra Hotel Aviation Readiness Program (M-SHARP): Software user manual (Release 1.0.64.1). (2016). Retrieved July, 22, 2016, from <https://s3.amazonaws.com/cdn.freshdesk.com/data/helpdesk/attachments/production/11002328158/original/M-SHARP%20Software%20User%20Manual%20%28SUM%29.pdf?AWSAccessKeyId=AKIAJ2JSYZ7O3I4JO6DA&Expires=1469213515&Signature=RNzIUizUo4g6Qk%2BLUhbJXm6sjDg%3D&response-content-type=application%2Fpdf>
- Mercado, J. E., & Spain, R. D. (2014). Evaluating mobile device ownership and usage in the U.S. Army: Implications for Army training. United States Army Research Institute for the Behavioral and Social Sciences. Retrieved from <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA603886>
- Metcalfe, B. (2013). "Metcalfe's Law after 40 years of Ethernet." *Computer*, 46(12), 26–31. .doi: 10.1109/MC.2013.374
- Microsoft Canada. (2015). Microsoft attention spans. Retrieved July 13, 2016, from <https://advertising.microsoft.com/en/WWDocs/User/display/cl/researchreport/31966/en/microsoft-attention-spans-research-report.pdf>
- Motley, M. M., & Bird, D. G. (2016). FY17 enlisted retention goals [MARADMIN 347/16]. Washington, DC: United States Marine Corps Manpower & Reserve Affairs, Manpower Management Division. Retrieved July 13, 2016, from <http://www.marines.mil/News/Messages/Messages-Display/Article/177038/fy17-enlisted-retention-goals/>
- Nally, K. J., (2013). Foreword: Marine Corps commercial mobile device strategy. Washington, DC: Headquarters, U.S. Marine Corps. Retrieved from: http://www.hqmc.marines.mil/Portals/156/Newsfeeds/SV%20Documents/20130411_Marine_Corps_Commercial_mobile_device_strategy_Final.pdf
- Naval Postgraduate School. (2009, June). *IT strategic plan 2009: Imagining the future of education and research*. Monterey, CA: Information Technology and Communications Services. Retrieved from http://www.nps.edu/Technology/Documents/NPS%20IT_Strategic_Plan%20June%202009.pdf
- Naval Safety Center. (2016). *Manned aviation rates and statistics: Class A/B (FM) mishaps: 10/01/2015 through 07/26/2016 (run date: Tuesday, July 26, 2016 07:50*. Retrieved July 27, 2016, from <http://www.public.navy.mil/navsafecen/Documents/statistics/ADS.pdf>

- Panepinto, J. (2014, November 13). The productivity payoff of mobile apps at work. *Harvard Business Review*. Retrieved from <https://hbr.org/2014/11/the-productivity-payoff-of-mobile-apps-at-work>.
- Pearlson, K. E., & Saunders, C. S. (2013). *Managing & using information systems: A strategic approach* (5th ed.). Hoboken, NJ: John Wiley & Sons.
- Prensky, M. (2001). Digital natives, digital immigrants: Part 1. *On the Horizon*, 9(5), 1–6. doi:10.1108/10748120110424816
- Ricoh Americas Corporation. (2014). Ricoh survey: The technology that empowers us may also sap our productivity. *Ricoh News Release*. Retrieved from https://www.ricoh-usa.com/about/docs/pdf/2014/09/Smartphones%20Sapping%20Worker%20Productivity_FINAL.pdf
- Rosen, L., & Samuel, A. (2015, June). Conquering digital distraction. *Harvard Business Review*. Retrieved from <https://hbr.org/2015/06/conquering-digital-distraction>
- Secretary of Defense. (2014). *Quadrennial Defense Review 2014*. Washington, DC: Office of the Secretary of Defense, Chuck Hagel. Retrieved from http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf
- Secretary of the Navy. (2015). *A Cooperative Strategy for 21st Century Seapower*. Washington, DC: Office of the Secretary of the Navy, Ray Mabus. Retrieved from https://www.uscg.mil/seniorleadership/DOCS/CS21R_Final.pdf
- Shives, T. R., & Pelz, L. M. (2012). *Analyzing the U.S. Marine Corps enterprise information technology framework for IT acquisition and portfolio governance* (Master's thesis). Retrieved from Calhoun: <http://hdl.handle.net/10945/17460>
- Stothart, C., Mitchum, A., & Yehnert, C. (2015). The attentional cost of receiving a cell phone notification. *Journal of Experimental Psychology: Human Perception and Performance*, 41(4), 893–897. doi:10.1037/xhp0000100
- Title IV – Military personnel authorizations. (2015). Retrieved July 18, 2016, from http://www.dtic.mil/congressional_budget/pdfs/FY2016_pdfs/MILPER_CRPT-114hrpt102.pdf
- Training and Education Command. (n.d.). Retrieved July 13, 2016, from <http://www.tecom.marines.mil/About/>
- Training Command. (n.d.). Retrieved July 13, 2016, from <http://www.trngcmd.marines.mil/About/>
- Trist, E. L. (1981). The evolution of socio-technical system: A conceptual framework and an action research program. Retrieved from <http://www.lmmiller.com/blog/wp-content/uploads/2013/06/The-Evolution-of-Socio-Technical-Systems-Trist.pdf>

- Tucker, J. S. (2010). Mobile learning approaches for U.S. Army training. *U.S. Army Research Institute for the Behavioral and Social Sciences*. Retrieved from <http://www.dtic.mil/get-tr-doc/pdf?AD=ADA528742>
- United States Marine Corps. (2016). *Organization of the United States Marine Corps* (MCRP 1–10.1). Washington, DC: Headquarters U.S. Marine Corps. Retrieved from <http://www.marines.mil/LinkClick.aspx?fileticket=MJ0g-cOyUyY%3D&portalid=59>
- United States Marine Corps College of Distance Education and Training. (n.d.). Retrieved July 13, 2016, from <https://www.mcu.usmc.mil/cdet/SitePages/home.aspx>
- Wedel, C. R., & Michalowicz, A. T. (2015). *Recommendations and privacy requirements for a bring-your-own-device user policy and agreement* (Master's thesis). Retrieved from Calhoun: <http://hdl.handle.net/10945/45270>
- White House. (2012, Aug. 23). A toolkit to support federal agencies implementing bring your own device (BYOD) programs [Memorandum]. Washington, DC. Retrieved from <https://www.whitehouse.gov/digitalgov/bring-your-own-device#ttb>
- White House. (2015, February). National security strategy. Retrieved from https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf
- Wong, L. (2002). Stifled innovation? Developing tomorrow's leaders today. *U.S. Army War College: Strategic Studies Institute*. Retrieved from <http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=279>

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California