NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

MBA PROFESSIONAL REPORT

ANALYSIS OF DEPARTMENT OF DEFENSE SOCIAL MEDIA POLICY AND ITS IMPACT ON OPERATIONAL SECURITY

by

Eric V. Leonhardi
Mark Murphy
Hannah Kim

June 2015

Thesis Advisor: Mie-Sophia Augier
Second Reader: Douglas Brinkley

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2015	**3. REPORT TYPE AND DATES COVERED** MBA Professional Report

4. TITLE AND SUBTITLE
ANALYSIS OF DEPARTMENT OF DEFENSE SOCIAL MEDIA POLICY AND ITS IMPACT ON OPERATIONAL SECURITY

5. FUNDING NUMBERS

6. AUTHOR(S) Eric V. Leonhardi, Mark Murphy, Hannah Kim

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

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

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

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

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

The emergence and rapid adoption of social media by society has forced the Department of Defense (DOD) to adapt, and ultimately develop and incorporate, social media policy into its cybersecurity strategy. While social media has influenced DOD strategy, it has also had a direct impact on the organization's operational security (OPSEC). DOD personnel using social media represent a potential OPSEC risk through the various ways and means in which they utilize social-networking platforms. In 2009, the DOD responded to this risk, in part, with a policy to regulate the use of social media. This project analyzes current DOD social media policy to determine how it can be changed to improve OPSEC. To address this issue, DOD social media policies from Army Cyber Command, Air Force Cyber Command, Fleet Cyber Command, and Marine Force Cyber Command were analyzed by performing an in-depth review and strengths, weaknesses, opportunities, and threats analysis.

14. SUBJECT TERMS
Social media, social networking, policy, cyber, security, cybersecurity, risk, threat, military, DOD, SWOT, strategy, operational security

15. NUMBER OF PAGES
73

16. PRICE CODE

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

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ANALYSIS OF DEPARTMENT OF DEFENSE SOCIAL MEDIA POLICY AND ITS IMPACT ON OPERATIONAL SECURITY

Eric V. Leonhardi, Lieutenant Commander, United States Navy

Mark Murphy, Lieutenant, United States Navy

Hannah Kim, Lieutenant, United States Navy

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
June 2015

Authors: Eric V. Leonhardi
Mark Murphy
Hannah Kim

Approved by: Mie-Sophia Augier
Thesis Advisor

Douglas Brinkley
Second Reader

William R. Gates
Dean, Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The emergence and rapid adoption of social media by society has forced the Department of Defense (DOD) to adapt, and ultimately develop and incorporate, social media policy into its cybersecurity strategy. While social media has influenced DOD strategy, it has also had a direct impact on the organization's operational security (OPSEC). DOD personnel using social media represent a potential OPSEC risk through the various ways and means in which they utilize social-networking platforms. In 2009, the DOD responded to this risk, in part, with a policy to regulate the use of social media. This project analyzes current DOD social media policy to determine how it can be changed to improve OPSEC. To address this issue, DOD social media policies from Army Cyber Command, Air Force Cyber Command, Fleet Cyber Command, and Marine Force Cyber Command were analyzed by performing an in-depth review and strengths, weaknesses, opportunities, and threats analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AFCYBER	24th Air Force Cyber Command
ARCYBER	Army Cyber Command
COCOMS	Combatant Commanders
CS/IA	Cyber Security/Information Assurance
DHS	Department of Homeland Security
DIACAP	DOD Information Assurance Certification and Accreditation Process
DIB	Defense Industrial Base
DOD	Department of Defense
DODI	Department of Defense Instruction
DoDIN	Department of Defense Information Network
DON	Department of the Navy
DTIC	Defense Technical Information Center
DTM	Direct Type Memorandum
EOP	Emergency Operating Procedures
FBI	Federal Bureau of Investigation
FLTCYBERCOM	Fleet Cyber Command
FOC	Full Operational Capability
FRG	Family Readiness Group
FRSA	Family Readiness Support Assistance
IA	Information Assurance
IbC	Internet-based Capabilities
IS	Information System
ISP	Internet Service Provider
IT	Information Technology
MARFORCYBER	Marine Corps Forces Cyber Command
MWR	Morale, Welfare, and Recreation
NIPRNET	Non-secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency

NSS	National Security Strategy
OPSEC	Operational Security
OSD	Office of the Secretary of Defense
SECDEF	Secretary of Defense
SECNAV	Secretary of the Navy
SBIR	Small Business Innovation Research
SWOT	Strengths, Weaknesses, Opportunities, and Threats
UCMJ	Uniform Code of Military Justice
USCYBERCOM	United States Cyber Command
USMC	United States Marine Corps
USSTRATCOM	United States Strategic Command
VRIO	Value, Rarity, Imitability, and Organization

ACKNOWLEDGMENTS

We would like to acknowledge and thank our advisors, Dr. Mie Augier and Dr. Douglas Brinkley, for their advice and guidance throughout this study. Furthermore, we would like to extend our gratitude to the faculty at the Naval Postgraduate School. This talented faculty has shaped and refined our critical thinking, providing us with life-long skills.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. SOCIAL MEDIA AS A STRATEGIC RESOURCE

The last decade has witnessed a tremendous increase in communication via social media platforms. While this phenomenon has had a significant impact on daily communication between individuals, social media platforms have become pervasive within organizations (Langer, 2014). The vast majority of public and private organizations and agencies have been forced to adapt to this rapidly expanding technology. The question is no longer if social media should be embraced; rather, it is how best to implement and manage it.

In 2009, the Department of Defense (DOD) implemented its first version of social media policy. The significance of this was two-fold. First, the DOD has a long-standing reputation as a laggard in acknowledging and accepting new societal trends and influences. Second, while supporting and funding various technological efforts through its acquisitions programs, the numerous bureaucratic layers of the agency have had a tendency to delay many innovative technologies from getting to the frontlines in a timely manner (Weisgerber, n.d.). Not only did the DOD accept this new technology, it has now fully implemented it into its network infrastructure to be used as both a strategic and operational resource.[1] In keeping with that theme, the DOD has utilized social media as a way of providing the public, as well as its service members, with a more transparent view of its overall mission and strategy. For the DOD to maintain a competitive advantage from social media use, however, it must effectively manage and control the incorporation and use of social media.[2]

[1] It is important to note that a resource becomes a *strategic* resource when it creates a sustainable competitive advantage for an entity (Jeyarathmm, 2008). Over the last decade, social media has become a strategic resource in that it can potentially contribute to the outperformance of one entity over another, with the metric of performance being profit or competitive potential (Coate, 2007).

[2] A competitive advantage is enjoyed by an organization when it can outperform competitors. The attributes that lead to a competitive advantage are varied and may include superior efficiency, superior quality, and/or superior innovation. The metric of performance for a business might consist of return on investment or return on assets. To adjust this to a nonbusiness entity, the metric of measurement should be adjusted to align with the organization (Jeyarathmm, 2008).

While the adoption of social media provides many benefits, there remain a number of inherent risks and vulnerabilities. Considering the increasing use of and reliance on it as a network resource, social media poses a tremendous risk to the DOD's operational security (OPSEC). Its mismanagement, intentional or not, can have immediate and long-lasting, negative impacts, ranging from the operational to strategic levels of the DOD. The DOD's approach allowing each of the military services to develop and implement their own independent social media policy creates a significant security liability. The risk of cyber exploitation is elevated due to gaps in oversight, standardization, procedures, guidelines, education, training, and control measures. Therefore, this project analyzes existing DOD social media policy by performing an in-depth review and strengths, weaknesses, opportunities, and threats (SWOT) analysis to determine how DOD policy can be changed to improve OPSEC. The next section of this chapter provides background information, as it discusses the growth of Internet and social media usage. Further sections in this chapter discuss the purpose of this project, as well as its associated research questions, methodology, and organization.

B. BACKGROUND

The Doctrine for the Armed Forces of the United States states the following with regard to the importance of information at all levels of government:

> Information remains an important instrument of national power and a strategic resource critical to national security. Previously considered in the context of traditional nation-states, the concept of information as an instrument of national power extends to non-state actors, such as terrorists and transnational criminal groups that are using information to further their causes and undermine those of the United States government and our allies. (Joint Chiefs of Staff, 2013, p. I-12)

The digital divide between individuals, organizations, and nation-states has rapidly decreased over the last 15 years. With that, advances in information and communication technology, reduced cost and ease of accessibility, and growing necessity to incorporate these technologies into society has ushered in a new age, commonly known as the "Information Age" (Brinkley, 2014). Many cybersecurity analysts and experts, such as Paul Saffo, Dave Burstein, and Danah Boyd, believe that access and

control of information is the characteristic that defines the current era of human civilization (Andersen & Rainie, 2014). Figure 1 provides a snapshot of increasing Internet usage between 2000 and 2010.

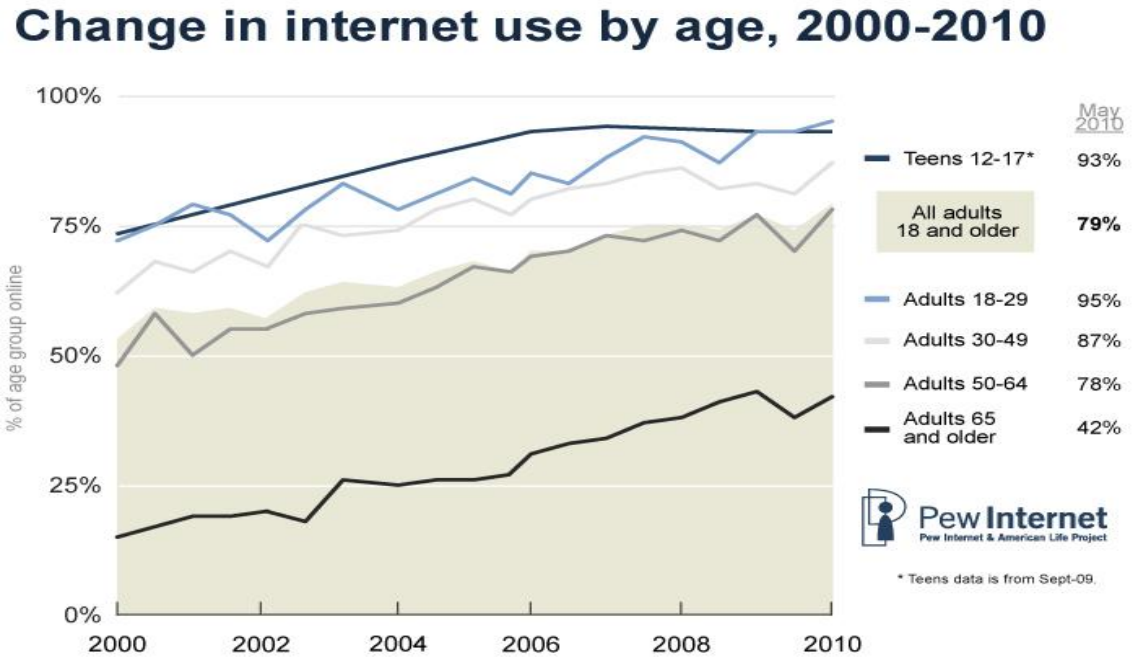

Figure 1. Internet growth rates by age, 2000–2010 (from Pew Research Center, 2010).

Social media allows connected individuals, organizations, communities, and businesses to interact and collaborate with each other (Kaplan, 2010). In recent years, open Application Program Interface and the technological advances of Web 2.0 have resulted in an additional boost to the global use of social media (Hughes, 2015). It promotes communication and connects people despite their physical proximity. It also permits the dissemination and sharing of information at a much faster rate and to wider audiences. The DOD is forced to operate in this dynamic environment, where new technologies translate into new-found opportunities, threats, and risks. Lynn (2010) notes, "As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare" (p. 97). Hence, the DOD has been forced to adapt to social media. It is now considered an important instrument for gathering and disseminating information

in the warfare environment (Joint Chiefs of Staff, 2011). This information provides the capability "to influence, disrupt, corrupt, or usurp an adversary's ability to make and share decisions" (Joint Chiefs of Staff, 2013, p. I-1).

As shown in Figure 2, multiple social media platforms exist that allow user access to various forms of real-time information, data, and services (Solis, 2013). Supporting a wide range of interests and practices, social media platforms have evolved, allowing people to connect through blogs, networks, and/or information sharing such as pictures and videos (Solis, 2013). Social media websites allow construction of a public or semi-public profile within a bounded system, can articulate a list of other users with whom they share a connection, and users can view and traverse their list of connections and those made by others within the system (Boyd & Ellison, 2007).

Figure 2. Conversation Prism (from Solis, 2013).

A recent study conducted by Pew Research Center, as shown in Figure 3, found that, as of January 2014, 74% of Internet users are using social networking sites. This number is predicted to grow in the coming years, primarily through Generation Z, which is comprised of those people born after 2000.[3] Social media and networking is quickly becoming the norm throughout much of society. This has now forced organizations to address its potential impact and risk on their operations. In doing so, they must develop policies and guidelines for effective management of social media, and must consider both its internal users as well as external users.

Who uses social networking sites

% of internet users within each group who use social networking sites

	All internet users	*74%*
a	Men	72
b	Women	76
a	18-29	89[cd]
b	30-49	82[cd]
c	50-64	65[d]
d	65+	49
a	High school grad or less	72
b	Some college	78
c	College+	73
a	Less than $30,000/yr	79
b	$30,000-$49,999	73
c	$50,000-$74,999	70
d	$75,000+	78

Pew Research Center's Internet Project January Omnibus Survey, January 23-26, 2014.
Note: Percentages marked with a superscript letter (e.g., [a]) indicate a statistically significant difference between that row and the row designated by that superscript letter, among categories of each demographic characteristic (e.g., age).

PEW RESEARCH CENTER

Figure 3. Social networking sites demographics (from Pew Research Center, n.d.).

[3] Generation X was born between 1966 and 1976, Generation Y was born between 1977 and 1994, and Generation Z was born after 1995 (Schroer, n.d.).

With over 1.3 billion users, Facebook remains the most popular social media site in the world (Edwards, 2014); however, as shown in Figure 4, the Pew Research Center found that there was no growth in Facebook users for 2013 and 2014 (Duggan, Ellison, Lampe, Lenhart, & Madden, 2015b). While Facebook growth has recently abated, other social media platforms, such as Twitter, Instagram, LinkedIn, and Pinterest, have shown significant user growth over the last six years (Duggan et al., 2015b). Another Pew Research Center survey, reflected in Figure 5, found that multiplatform use was on the rise, with 52% of users stating that they use two social networking sites simultaneously (Duggan et al., 2015a). In fact, a smaller, but growing, percentage of users employ five or more social networking sites.

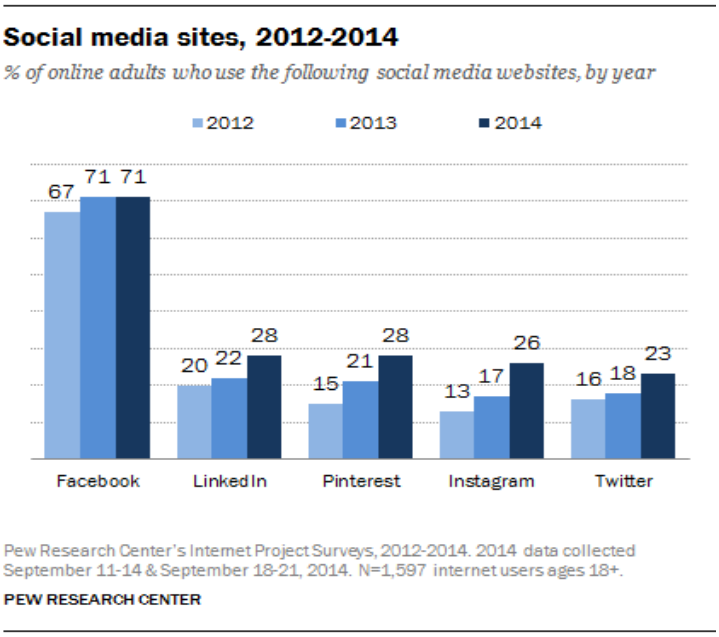

Figure 4. Social media site percent usage by adults, 2012–2014 (from Duggan et al., 2015b).

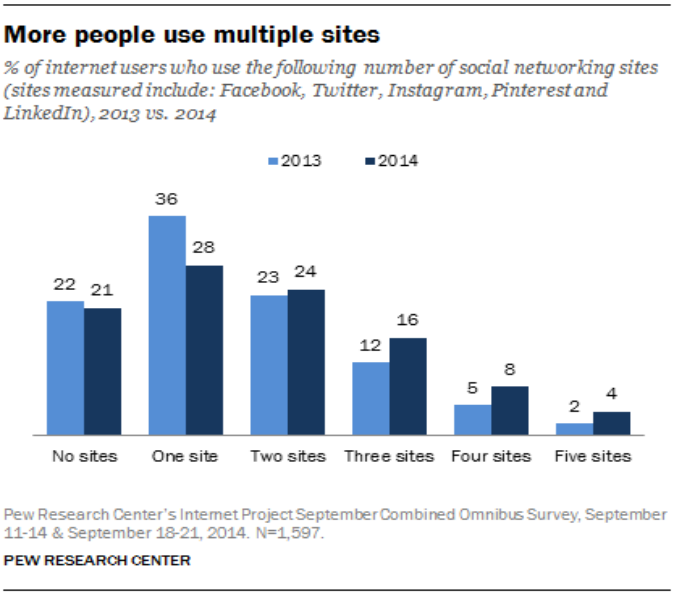

Figure 5. Number of social media sites used, 2013 vs. 2014 (from Duggan et al., 2015a).

Many businesses, corporations, and organizations have adopted social media platforms and technology to promote global communication, products, services, sales, and programs (Kaplan, 2012). A study conducted by Burson-Marstellar in 2010 found that 79% of the largest 100 companies in the Fortune 500 use Facebook, Twitter, or some other social media platform to assist in the execution of their strategy and daily operations. Not only did this trend impact the private sector, it permeated to the public domain as well. In February 2010, the DOD released its first policy memorandum on the responsible and effective use of Internet-based capabilities, to include social networking sites and other Web 2.0 applications (Budzyna, 2009).

C. PURPOSE

The widespread use of social media creates both strategic opportunities and threats. Joint Chiefs of Staff (2014) focuses on information operations and states the following with regard to the importance of information sharing:

> The ability to share information in near real time, anonymously and/or securely, is a capability that is both an asset and a potential vulnerability to us, our allies, and our adversaries. (p. I-1)

Social media presents an individual or organization with the ability to acquire and manipulate information. The information posted by rivals can be collected and exploited; for this reason, social media content must be regulated. Careless and unregulated usage can lead to the release of sensitive or classified information, but even unclassified information poses a threat, as it can be collected from a wide variety of open sources and compiled to produce information that is useful. Some collection efforts on open-source materials can reveal classified knowledge to an adversary. OPSEC deals with the regulation of unclassified information to prevent an adversary from gaining valuable intelligence by piecing together open-source information. Therefore, leveraging social media to the best strategic effect requires a social media policy that promotes OPSEC.

D. RESEARCH QUESTIONS

This project analyzes DOD social media policy and its impact on OPSEC. Specifically, the following items will be addressed:

- What are the strengths and vulnerabilities of the DOD's social media policy in regards to OPSEC?
- What opportunities exist to strengthen OPSEC through social media policy?
- How can an adversary threaten OPSEC through social media?
- What modifications to U.S. policy can be made to decrease the strategic liabilities of social media?

E. SCOPE AND METHODOLOGY

This project is focused solely on the relation between U.S. DOD OPSEC and social media. A SWOT analysis was used to analyze current DOD social media policy. SWOT analysis aids in analyzing the DOD's social media policies by identifying the internal factors (strengths and weaknesses) and external factors (opportunities and threats) that are favorable and unfavorable in regards to OPSEC. The factors are then examined to identify competitive advantages, weaknesses that can be improved, and threats that can be mitigated. Recommendations are provided to assist in developing competitive advantages, while improving upon weaknesses and mitigating threats.

F. ORGANIZATION OF THE STUDY

Chapter II reviews cybersecurity initiatives of the National Institute of Standards and Technology (NIST), the National Security Strategy (NSS), the DOD strategy for cyber security, and the social media policies of each branch of the uniformed services. Chapter III focuses on a SWOT analysis of the DOD's social media policy and how it relates to OPSEC. The SWOT analysis findings, along with policy change recommendations and further research, are concluded in Chapter IV.

THIS PAGE INTENTIONALLY LEFT BLANK

II. STRATEGIES AND POLICIES

To better understand how social media policy has been developed and implemented into the DOD's organizational structure, it is important to address its roots within the larger cyber security issue faced by both the U.S. government and private industry. Over the last 15 years, individual, organizational, and nation-state reliance on telecommunication and computer network infrastructure has increased dramatically. Increased use of computers, phones, and various forms of wireless media for rapid sharing and dissemination of information has become embedded within modern culture (Langer, 2014). While tremendous benefits are derived from modern information technology (IT), the global network infrastructure remains a vast and unregulated arena that is easily exploited by criminal hackers, organized crime syndicates, terrorist networks, and advanced nation-states. Utilizing a top-down approach to address this, the Obama administration directed both the DOD and Department of Homeland Security (DHS) to develop and implement an appropriate framework and policy that effectively addresses cyber security across both U.S. public and private domains.

A. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

President Obama's 2013 issuance of Executive Order 13636, Improving Critical Infrastructure Cyber security, confirmed the acceptance of cyber security as a top priority for the national security of the United States (National Institute of Standards and Technology [NIST], 2013). The release of this order was significant in that it addressed the importance of a unified front to counter the rapid expansion of the global cybersecurity threat landscape. It also emphasized that only through collaboration between public and private industry can governments and organizations effectively protect the critical infrastructure they so heavily depend on (NIST, 2013).

The NIST, an agency of the U.S. Department of Commerce, was subsequently chosen to develop a cybersecurity framework that would promote and foster cross-industry dialogue between agencies and organizations (NIST, 2014). The reason for this was two-fold. First, the agency has remained a leading authority and promoter of

innovation across a large number of industries and sectors (NIST, 2014). Second, NIST has developed a tremendous reputation over the years of promoting collaborative efforts between the public and private sectors (NIST, 2014).

In early 2014, NIST issued its first version of the new cybersecurity framework (Huergo, 2014). In keeping with the priorities of Executive Order 13636, the DOD promptly conducted an organizational shift from the DOD Information Assurance Certification and Accreditation Process (DIACAP) that it had been using since 2007, to the newly developed NIST framework. In doing so, the DOD's cybersecurity standards and practices would be matched with those of its civilian counterparts, as well as other government agencies. The DOD's quick shift from the legacy DIACAP process to the newer framework further emphasizes the willingness of organizations to establish commonality in the policies and procedures they develop and implement (Huergo, 2014).

The intent of the NIST cybersecurity framework is not to provide a rigid set of guidelines for policy development. Rather, it provides a baseline framework that is not industry specific and can be applied by agencies and organizations of varying types and size (NIST, 2014). This approach fosters top-level commonality, while also allowing organizations to tailor the framework to meet their specific needs (NIST, 2014). Through effective application, the NIST cybersecurity framework provides:

- Increased dialogue between industries and organizations.
- Alignment of cybersecurity policy, procedures, and guidelines.
- Increased protection of privacy and intellectual property.
- Reduces response time, through increased information sharing practices, to potential cyberattacks and incidences.
- Increased national security and protection of critical infrastructure. (NIST, 2014, p. 3)

B. NATIONAL SECURITY STRATEGY

Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges facing the United States today (White House, 2010). The technologies that allow people and organizations to lead and create also empower those wishing to disrupt and destroy (White House, 2010). While they support and enable U.S. military superiority, the government's unclassified networks are continuously scanned

and probed (White House, 2010). In many instances, and at times unknowingly, these networks are compromised (White House, 2010). While the safety and security of U.S. citizens depends on critical infrastructure, such as power and electric grids, cyber criminals continue to expose vulnerabilities to disrupt them on a massive scale (White House, 2010). Their actions result in organizations and consumers losing vast quantities of money and valuable intellectual property (White House, 2010).

National threats are broad in scope and can consist of individual hackers, organized criminal groups, terrorist networks, and advanced nation-states (White House, 2010). These threats to U.S. security and personal privacy require networks and infrastructure that are secure, dependable, and responsive (White House, 2010). With that comes the inherent responsibility of government agencies and private organizations to formulate and execute effective cybersecurity policies and guidelines. The country's network infrastructure is a strategic national asset and therefore makes it a national security priority (White House, 2010).

Facing a rapidly growing threat environment, the United States has determined that all agencies and organizations should focus their efforts on investing in human capital and technology, while simultaneously strengthening partnerships (White House, 2010). By doing so, organizations and agencies will be able to effectively deter, prevent, detect, defend against, and recover from cyber intrusions and attacks (White House, 2010). This growing threat environment has prompted the U.S. government to expand its efforts to work hand-in-hand with the private sector (White House, 2010). By sharing information and strategies, both public and private entities can effectively address a multitude of issues to include cybersecurity policies, guidelines, laws, privacy, and network defense and response procedures (White House, 2010). While U.S. military services and agencies have operated independently with regard to network practices and security, the threat landscape of the last decade has forced a change in policy, processes, and tactics. This culminated in early 2014, when the DOD adopted the NIST cybersecurity framework as a basis for developing an effective and actionable way forward in cyberspace (NIST, 2014).

C. DEPARTMENT OF DEFENSE STRATEGY

The DOD, along with the rest of the U.S. government, depends on cyberspace to execute its daily mission. Effective security and operation of critical infrastructure relies on cyberspace, industrial control systems, and information technology that may be vulnerable to exploitation and disruption techniques (DOD, 2011). Considering that the DOD operates over 15,000 networks and seven million computing devices around the world, it is easy to see the importance that cyberspace has within the organization (DOD, 2011). The DOD heavily leverages cyberspace to support military and commercial operations, which entails the movement of personnel and materiel, as well as the command and control of a wide range of military operations (DOD, 2011).

Ironically, the DOD's effective use of cyberspace has been counterbalanced by the shortcomings of its cybersecurity policies, guidelines, and procedures (DOD, 2011). The continued expansion of networked systems and platforms resulted in cyberspace being incorporated into capabilities, which the DOD relies on to execute both its strategy and day-to-day operations. Today's threat environment has proven that criminal hackers, organized criminal groups, terrorist networks, and advanced nation-states continue to apply exploitation techniques to the department's networks (DOD, 2011). In fact, some foreign intelligence organizations have already acquired the capacity to disrupt critical areas of the department's information infrastructure (DOD, 2011). Further increasing the DOD's problems, non-state actors progressively threaten disruption and penetration of the DOD infrastructure. Based on these factors, the DOD has stated that there may be malicious activities on the organization's network infrastructure that has yet to be detected (DOD, 2011).

Working with a number of interagency and international partners, the DOD has dedicated a tremendous amount of resources to reducing the risks posed to both U.S. and allied cyberspace capabilities (DOD, 2011). Critical to its strategy, the DOD has focused on a number of serious factors, to include external threat actors, insider threats, supply chain vulnerabilities, and threats to the organization's operational ability (DOD, 2011). In order for its strategy to work, the DOD must properly and effectively identify its

vulnerabilities, while mitigating concerted efforts of both state and non-state actors to gain unauthorized access to its network infrastructure (DOD, 2011).

In recent years, foreign cyberspace operations against U.S. public and private sector systems increased in both quantity and sophistication (DOD, 2011). Open-source intelligence reports identified that DOD networks are probed countless times on a daily basis (DOD, 2011). Unfortunately, not all such attempts can be prevented and successful penetrations have resulted in the loss of thousands of files from U.S. networks, U.S. allies and industry partners (DOD, 2011). Additional evidence has identified an evolution of threats, as adversaries focus on the development of increasingly sophisticated and capable cyber techniques and strategies (DOD, 2011).

A growing and persistent threat emanates from small and independent groups, which have an asymmetric impact in cyberspace. Asymmetric methods have successfully exposed numerous network vulnerabilities, resulting in a realistic incentive and motivation for malicious activity (DOD, 2011). One common asymmetric method is controlling botnets with millions of infected hosts (DOD, 2011). The tools, techniques, and methods developed and applied by cyber criminals are dynamic and continue to become more sophisticated. To further exacerbate the problem, many of these can be purchased cheaply on the Internet (DOD, 2011). Regardless of whether the goal is access to intellectual property, finances, or to disrupt the DOD's network, evolving cyber threats present a significant and complex challenge for both national and economic security (DOD, 2011).

The human element, commonly referred to as "insiders," poses a grave risk, as they commonly exploit their accessibility at the command of foreign governments, terrorist groups, criminal elements, or on their own initiative (DOD, 2011). Consequences can be devastating for an agency, regardless of activity, whether it is conducting espionage, voicing a political statement, or articulating personal disdain (DOD, 2011). The insider threat could potentially have an even broader impact on U.S. national security (DOD, 2011).

An additional challenge for the DOD resides with network software and hardware. In the case of foreign-produced software and hardware, a risk of malicious tampering exists before integration or installation of the hardware and/or software into systems. This can have a direct and detrimental impact on system security (DOD, 2011). The DOD's continued dependence on foreign manufacturing of network components creates significant challenges in managing risk in areas of production, assembly, service, delivery, and disposal (DOD, 2011).

The DOD recognizes that cyberspace poses a threat to national security, which extends beyond military targets and can have a range of impacts on many aspects of society (DOD, 2011). Cyber criminals and organizations have become increasingly more capable of launching sophisticated intrusions into the networks and systems that control critical civilian infrastructure such as electrical, telecommunication, transportation, and financial services (DOD, 2011). Considering the integration of cyberspace, the exploitation of power grids, telecommunication, transportation, or financial networks or systems could result in significant damage and economic disruption (DOD, 2011). Since the DOD utilizes this infrastructure to conduct its operations, both at home and abroad, every effort must be made to reduce risk, address network vulnerabilities, and identify cyber threats (DOD, 2011).

Lastly, the DOD has emphasized the most pervasive, yet less visible, form of cyber threat, is that of intellectual property theft (DOD, 2011). The U.S. government recently stated that, on an annual basis, the amount of intellectual property stolen from U.S. networks is greater than the amount of information contained in the Library of Congress (DOD, 2011). The effectiveness of the DOD is directly related to U.S. economic strength. With such staggering losses of intellectual property, both U.S. military capability and economic strength is significantly impacted (DOD, 2011).

In order to best execute its strategy, the DOD has focused its efforts on five strategic initiatives:

1. Strategic Initiative I

Under Initiative I, the DOD has declared cyberspace as an operational domain. This requires organizing, training, and equipping personnel so that the agency can take full advantage of cyberspace's potential, while minimizing risks (DOD, 2011). Considering that most DOD networks are privately managed and operated, treating cyberspace as a domain is a critical concept for the DOD's national strategy (DOD, 2011). This approach allows the agency to effectively organize and train personnel for operations within cyberspace, in order to support the interests of U.S. national security (DOD, 2011). The DOD has also expressed concern that every effort must be made to support essential operations within a degraded cyber environment (DOD, 2011).

By direction of the NSS, the DOD has emphasized the importance of having the necessary capabilities to operate effectively in all warfare domains to include air, land, maritime, space, and cyberspace (DOD, 2011). To best achieve this goal, the Secretary of Defense (SECDEF) assigned cyberspace mission responsibilities to U.S. Strategic Command (USSTRATCOM), the other Combatant Commanders (COCOMS), and each of the military services (DOD, 2011). The DOD established U.S. Cyber Command (USCYBERCOM) as a subordinate unified command of USSTRATCOM in response to its need to operate effectively in cyberspace and adequately organize its resources (DOD, 2011). The establishment of USCYBERCOM serves three primary needs of the DOD:

- Manage cyberspace risk by incorporating increased training requirements, boosting information assurance qualifications, promoting greater situational awareness, and creating more secure DOD networks.
- Promote integrity and availability by establishing solid partnerships, building cross-domain defense mechanisms, and establishing and maintaining a common operating picture that is shared by all major players.
- Promote and develop integrated capabilities by working closely with Combatant Commands, services, departments, agencies, and the acquisition community to deliver and deploy state-of-the-art capabilities where they are most needed. (DOD, 2011, p. 5)

USSTRATCOM delegated the responsibility for managing and coordinating service components within each branch of the military, to include the Army Cyber Command (ARCYBER), Fleet Cyber Command (FLTCYBERCOM), the 24th Air Force Cyber Command (AFCYBER), and Marine Forces Cyber Command (MARFORCYBER) to USCYBERCOM (DOD, 2011). A key organizational concept behind the stand-up of USCYBERCOM is its colocation with the National Security Agency (NSA), as the NSA director also serves as the Commander of USCYBERCOM (DOD, 2011). Colocation and dual-hatting of these separate and distinct organizations allows the DOD and the U.S. government to better leverage its respective authorities and manage its resources, both of which are critical to achieving the DOD's cybersecurity strategy (DOD, 2011).

Degraded cyberspace operations for extended periods are an assumed reality, therefore the DOD has designed and integrated a wide range of cyberspace scenarios into training and exercises to better prepare military commands for a wide variety of contingencies (DOD, 2011). A critical facet of this activity is the implementation of cyber "red teams" throughout these exercises and war games (DOD, 2011). Conducting training in environments where there is an assumed breach, forces military commands to perform and execute at a level that is outside the norm (DOD, 2011). Events such as these promote the DOD's efforts of mission assurance and the preservation of critical operating capabilities (DOD, 2011).

Finally, in order for Initiative I to be effective, every effort must be made to ensure the development and establishment of a resilient DOD network infrastructure. In the event that there is a failure or a significant compromise to the network, the DOD must be able to remain operationally effective. In order to do this, military commands must effectively isolate and neutralize threats by using redundant capacity or be able to shift operations from one support system to another (DOD, 2011). One way of effectively addressing this is by creating multiple networks, which adds diversity, overlap, resiliency, and further promotes mission assurance within cyberspace (DOD, 2011). Currently, the DOD is researching options for shifting operations to more secure networks at scale, which effectively complements the wide range of missions that the DOD supports (DOD, 2011).

2. Strategic Initiative II

The primary goal of Initiative II is assurance that the DOD properly and effectively employs new operating concepts that provide a functional, defense-in-depth capability to both its internal and external network structure (DOD, 2011). The DOD has identified a four-step process to achieve this goal.

- First, the DOD will overhaul and enhance its current cyber practices to improve overall network security.
- Second, to prevent insider threats, the agency is strengthening the communication practices of its workforce, increasing accountability measures, boosting internal monitoring procedures and practices, and increasing overall information management capabilities.
- The third step has the DOD employing active cyber defense capabilities to prevent DOD network intrusions.
- The final step has the DOD developing and implementing new defensive operating concepts and architectures (DOD, 2011, p. 6).

By incorporating these four steps, the DOD can form a network infrastructure that is both adaptive and dynamic, both of which are required, considering the current cyber threat landscape (DOD, 2011).

The DOD recognizes that a large percentage of cyber threats and malicious acts can be mitigated by sound cyber policy (DOD, 2011). In doing so, due diligence must be practiced at all times by military service members, DOD employees, and supporting private industry personnel (DOD, 2011). Protection is a two-fold process that entails individual protection, as well as ensuring that the security software and operating systems used on a daily basis are up to date and fully operational (DOD, 2011). Effective policy must address the maintenance of information security, promote sound cybersecurity practices for users and administrators, ensure that network design is secure, and employ an effective network configuration (DOD, 2011). The DOD has hardened the organization's network infrastructure by adopting the private sector's continuous renewal method (DOD, 2011). This approach will provide protection, monitoring, maintenance, design, and recovery for the agency's network infrastructure (DOD, 2011).

Personnel are the first line of defense in ensuring cyber policy effectiveness. They also play a critical role in identifying and reducing the number of potential insider threats

(DOD, 2011). To best mitigate the insider threat and prevent the release of classified information, the DOD started strengthening its current information assurance model (DOD, 2011). The agency has also commenced exploring a number of new operating concepts to reduce network vulnerabilities (DOD, 2011). The agency continues to focus a large percentage of its efforts on personnel training, cross-domain communication, new technologies, and streamlined processes (DOD, 2011). By promoting information assurance, the DOD believes it can better position the workforce to ensure individual responsibility (DOD, 2011). To promote these efforts, the DOD has determined that "culture" must be addressed within its new policy structure and training programs (DOD, 2011).

The DOD is implementing a more robust and active cyber defense methodology to prevent intrusions and thwart malicious activities on its network (DOD, 2011). The DOD defines its active cyber defense approach as a real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities (DOD, 2011). This approach builds on the more traditional approaches that the agency has used in defending its networks by supplementing best practices with newer and more realistic operational guidelines and procedures (DOD, 2011). The DOD has also accepted that intrusions may not always be stopped at the network boundary; therefore, the organization must prioritize the continued improvement of its advanced sensors to detect, discover, plot, and mitigate malicious activity on its network infrastructure (DOD, 2011). By embracing both evolutionary and rapid change, the DOD will be able to stay ahead of potential threats and reduce its exposure to risks.

3. Strategic Initiative III

The DOD has stated that Initiative III will prioritize partnering with other U.S. government departments and agencies, as well as the private sector, to facilitate and enable a more extensive cybersecurity strategy (DOD, 2011). Considering the threat landscape, the challenges of cyberspace cross multiple industries and extend across national boundaries, while impacting multiple facets of the global economy (DOD, 2011). A significant issue is that the DOD's functionality and operational capabilities rely on commercial assets to include Internet service providers (ISP) and global supply

entities (DOD, 2011). Ironically, many of the areas over which the DOD operates provide no ability or authority for the agency to mitigate its risk exposure (DOD, 2011). This has prompted the DOD to work directly with the DHS, selected interagency partners, and the private sector to share concepts and techniques (DOD, 2011). By doing so, the DOD can develop more advanced capabilities, while supporting collective efforts to meet the cross-domain challenges of cyberspace (DOD, 2011).

In pursuit of working more closely with interagency partners, the DOD has stated that it will take a broader governmental approach to addressing cybersecurity policy. A major step towards this initiative was the 2010 signing of a memorandum of agreement between the Secretary of Homeland Security and the Secretary of Defense to better align and promote collaboration for cybersecurity operations (DOD, 2011). The primary reason for strengthening the partnership between the DHS and the DOD was to enhance cyber security at the national level in three distinct ways:

- The first reason was because a more official structure reaffirms the limits that current policy and law set on the collaborative effort between the DOD and the DHS.
- The second reason was that a joint relationship in the programming and planning phases would boost both department's overall mission effectiveness. Not only would this improve the general understanding of cybersecurity needs between the organizations, but it would enhance protection in important areas such as privacy and civil liberties.
- Lastly, by sharing resources and energies to enhance cybersecurity efforts, each military service could potentially experience a reduction in budget expenditures. (DOD, 2011, p. 8)

The DOD has strengthened ties with the Defense Industrial Base (DIB) to increase the protection of sensitive information (DOD, 2011). The DIB, comprised of both public and private agencies and organizations, supports the DOD through the delivery of advanced technologies, weapons systems, support mechanisms, and personnel (DOD, 2011). To increase protection of both internal and external DIB networks, the DOD launched the DIB Cyber Security and Information Assurance (CS/IA) program in 2007 (DOD, 2011). Using this program as a foundation, the DOD established a public and private sector partnership to demonstrate the benefits of increased information sharing against cyber threats and to mitigate risk factors (DOD, 2011).

The DOD continues to emphasize the importance of building its relationship with the DHS to identify and mitigate cyber vulnerabilities within the nation's critical infrastructure (DOD, 2011). To be successful, both agencies must continue to support additional pilot programs, business methodologies, and policy frameworks to promote a stronger bond between the public and private sectors (DOD, 2011). To be effective, these relationships and partnerships must effectively promote innovation, trust, and information sharing (DOD, 2011). The DOD's efforts must also extend beyond large corporations to both small- and medium-sized businesses to ensure participation, as well as identify potential innovation (DOD, 2011).

Lastly, the DOD has taken the initiative of promoting a unified governmental approach for managing cyber risks at both the national and international levels (DOD, 2011). This is because many domestic technology firms outsource software production, hardware production, and services to overseas organizations (DOD, 2011). Another driver is that counterfeit components and products require procedures to reduce risk and increase quality control procedures (DOD, 2011). The DOD is currently reducing its dependence on technology from untrusted sources, which can have a detrimental effect on the information assurance it promotes (DOD, 2011). Interagency cooperation is critical to mitigating risks associated with the worldwide technology supply chain (DOD, 2011).

4. Strategic Initiative IV

The DOD identified the importance of relationship building with allies and international partners (DOD, 2011). To support the international strategy for cyberspace, the agency has prioritized the building and strengthening of international relationships to combat cyberspace threats (DOD, 2011). This has been achieved through the development of shared situational awareness and warning capabilities (DOD, 2011). Through a unified and collaborative effort, both the DOD and its international partners have been able to drastically increase the cyber defense of their respective networks (DOD, 2011).

The expanse of the cyber domain prevents a single entity, agency, organization, or government from maintaining a fail-safe network defense on its own. With that, the DOD has stated that international engagement is imperative to successfully execute its international strategy for cyberspace (DOD, 2011). To do this, the agency has ramped up its efforts to develop and promote international cyberspace procedures, guidelines, and norms that promote overall interoperability, security, and reliability (DOD, 2011). The agency has also taken a leadership role in encouraging responsible behavior and combating entities that threaten critical national and international infrastructure (DOD, 2011).

As international cyberspace cooperation continues to develop, the DOD has integrated more with its allies and international partners to develop shared warning capabilities, engage in capacity building, and conduct joint training exercises (DOD, 2011). By endorsing proactive engagement, the intent is to generate opportunities to initiate dialogues for sharing of best cyber practices in areas such as forensics, capability development, and exercise participation (DOD, 2011). An additional benefit is that burden-sharing arrangements can play to each nation's core strengths and capabilities (DOD, 2011). This further strengthens critical areas where allies are less proficient, while strengthening collective cybersecurity standards (DOD, 2011).

Lastly, the DOD has recently expanded its cyber cooperation to a wider pool of allied and partner militaries to develop more holistic cybersecurity practices and principles (DOD, 2011). Through these shared practices and principles, members can maximize scarce cyber capabilities, mitigate risk, and create coalitions to deter malicious activities in cyberspace (DOD, 2011). A more collaborative effort will serve to augment the DOD's formal alliances, while also increasing the effectiveness of cybersecurity practices and applied methodologies (DOD, 2011).

5. Strategic Initiative V

U.S. national security has a direct relationship with many facets of U.S. society. In recent years, the DOD has strived to utilize more academic, scientific, and economic resources to create a more talented and diverse base of military and civilian personnel to execute its cybersecurity strategy and objectives (DOD, 2011). The DOD has stressed the importance of fostering innovation through the acquisition processes to increase its overall cyberspace capabilities (DOD, 2011). To sustain this approach, the agency must continue to invest in people, research and development, and technology (DOD, 2011).

To meet strategic goals, the DOD has stated that identification, development, and retention of a capable workforce are essential to success (DOD, 2011). In order to accomplish this objective, the agency will continue to assess its cyber workforce, requirements, and capabilities on a periodic basis to maintain relevancy (DOD, 2011). A major recruiting concern is establishing the DOD as a competitive employer in comparison to private industry (DOD, 2011). To achieve this, the agency has focused on the establishment of dynamic programs to attract talent as early as possible (DOD, 2011). The agency also participates in human resources development areas associated with the 2010 Presidential Initiative to further improve recruitment and hiring processes of the federal government (DOD, 2011). The DOD is working directly with the Executive Branch to explore strategies designed to streamline hiring practices for its cyber workforce and exchange programs to allow for cross-flow of cyber professionals between both public and private sectors to identify, retain, and foster a more innovative cyber workforce (DOD, 2011).

In recent years, the DOD has fostered the adoption of cross-generational mentoring programs to establish and grow a more talented workforce (DOD, 2011). Another way of increasing workforce capability is the incorporation of both Reserve and National Guard cyber capabilities (DOD, 2011). This will allow for greater diversity, capacity, expertise, and flexibility across DOD, federal, state, and private sector activities (DOD, 2011). The DOD has also dedicated more resources for continuing education and exchange program opportunities (DOD, 2011). The objective of these programs is a more entrepreneurial workforce and preservation of intellectual capital (DOD, 2011).

In recent years, the DOD has realized it lags behind the private sector regarding innovation and applying emerging computing concepts (DOD, 2011). To address this, it has adopted five important principles to increase the effectiveness of its acquisition processes:

- The first principle states that both DOD acquisition processes and regulations must match the technology development life cycle of the private sector (DOD, 2011). Having been implemented, the agency has shown a drastic reduction in its mean cycle times from years to months.
- The second principle addresses the employment of incremental development and testing practices, rather than a single deployment of large and complex cyber systems.
- The third principle emphasizes DOD willingness to sacrifice or defer some customization to achieve more rapid and incremental improvements.
- The fourth principle promotes the importance of adopting varying levels of oversight based on the agency's prioritization of critical systems.
- Lastly, the DOD has made great efforts to improve both the software and hardware security of products and services that they acquire.
  (DOD, 2011, p. 11)

Applying and executing these five principles has had a positive effect on the DOD's ability to manage its acquisition process, as well as mitigate its cyber risk (DOD, 2011).

Recently, the DOD has promoted opportunities for small- and medium-sized businesses. To achieve this, the agency works with entrepreneurs in established U.S. technological innovation hubs to move concepts at a rapid rate from innovative idea, to pilot program, to scaled adoption across the DOD enterprise (DOD, 2011). This has increased accessibility to innovative technology and ideas, as well as fostered collaboration across the scientific community and the public sector. This forward-leaning approach has increased the DOD's exposure to more advanced cybersecurity architectures and methodologies, both of which are crucial to boosting its network defense.

The recent development and employment of the National Cyber Range—a large, joint training platform—has played a critical part in allowing the DOD, its partners, and international allies to deploy, test, and evaluate new cyberspace concepts, policies, and technologies (DOD, 2011). This has been a huge upgrade to the DOD's overall network capability, considering that until recently many military commands had limited access to

areas to conduct cyber simulations and exercises (DOD, 2011). By providing a means to rapidly employ and conduct real-time testing of innovative cyber architectures and methodologies, the National Cyber Range has made an immediate impact on DOD and U.S. national strategic network infrastructure defense.

The DOD has encouraged private sector participation in cyberspace development by empowering organizations to serve as clearing houses for innovative concepts and technologies (DOD, 2011). The agency has started incorporating a system that rewards those firms that develop impactful and innovative technologies. In recent years, the agency has more effectively leveraged the innovation and agility of small businesses and entrepreneurs through the use of such initiatives as Small Business Innovation Research (SBIR), creative joint ventures, and targeted grants and investments.

D. SOCIAL MEDIA POLICIES

1. U.S. Strategic Command

In June 2009, the SECDEF directed the Commander of USSTRATCOM to establish a subordinate unified command identified as USCYBERCOM (United States Strategic Command, 2015). Full operational capability (FOC) was rapidly achieved in October 2010. Located at Fort Meade, Maryland, USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to:

- Direct the operations and defense of specified DOD information networks.
- Prepare, and on direction, conduct a wide range of cyberspace operations and actions across all identified domains.
- Ensure U.S. military and allied freedom of action in cyberspace, while maintaining adversarial denial capabilities.
- Defend the DOD information network.
- Provide support to all COCOMS for execution of their missions throughout the world.
- Strengthen the nation's ability to withstand and respond to advanced cyberattacks. (United States Strategic Command, 2015, p. 1)

There were many reasons for the establishment of USCYBERCOM. It unifies the direction of cyberspace operations, strengthens DOD cyberspace capabilities, and integrates and bolsters the DOD's cyber expertise (United States Strategic Command, 2015). It also improves the DOD's capabilities to operate resilient and reliable networks,

counter cyberspace threats, and assure access to cyberspace (United States Strategic Command, 2015). Upon its inception, USCYBERCOM began to immediately address the DOD's cyber workforce structure, as well as the training requirements and certification standards that enable each of the DOD services to build the cyber force required to execute their assigned missions (United States Strategic Command, 2015). Lastly, USCYBERCOM works closely with interagency, private industry, and international allies to execute its overall mission (United States Strategic Command, 2015).

Through its broad cybersecurity framework, USCYBERCOM allows each service element to establish its own distinct set of guidelines with regard to social media application and use (United States Strategic Command, 2015). Command service elements include ARCYBER, AFCYBER, Fleet Cyber FLTCYBERCOM, and MARFORCYBER (United States Strategic Command, 2015). While each policy is unique to each of the services, there remain a number of distinct similarities; however, the debate continues as to whether or not current social media adequately addresses OPSEC within the DOD.

2. DOD Service Policies

In the Appendix section of this project, the following policies are analyzed: The overall instruction set forth by the DOD in regards to the use of Internet services and Internet-based capabilities; U.S. Army guidelines for the use of social media; U.S. Air Force's version; U.S. Navy's version, and the U.S. Marine Corps' version.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY AND ANALYSIS

A. METHODOLOGY

For a chosen strategy to be successful, organizations must be able to identify and adapt to the rapidly changing environment they operate within. Not only does this depend on effectively analyzing the external environment, it requires an organization to properly assess its internal capabilities and how best to utilize them to respond to external factors ("SWOT Analysis," 2013). One common method of doing this is through the application of a SWOT analysis ("SWOT Analysis," 2013). When applied, SWOT allows organizations to more accurately identify and address complex issues that have the most impact on their operations and strategy ("SWOT Analysis," 2013).

The concept of SWOT analysis was first described by Edmund P. Learned, C. Roland Christiansen, Kenneth Andrews, and William D. Guth in *Business Policy, Text and Cases* during the 1960s ("SWOT Analysis," 2013). In essence, SWOT analysis is an analytical framework that evaluates an organization's respective strengths, weaknesses, opportunities, and threats relative to its strategy ("SWOT Analysis," 2013). This is done by identifying the internal factors (strengths and weaknesses) and external factors (opportunities and threats) that are favorable and unfavorable, with the goal of achieving an attainable strategy ("SWOT Analysis," 2013). When successfully applied, it reveals opportunities that can be exploited and further mitigates threats by understanding those weaknesses that have been identified (Goodrich, 2015).

While a SWOT analysis is typically conducted in a 4 x 4 matrix, generating a list is also acceptable as long as it is comprised of each of the four key elements:

- **Strengths:** Consists of those positive factors that are internal to the organization and that provide the organization with a competitive advantage over its competitors.
- **Weaknesses:** Consists of those negative factors internal to the organization that places the organization at a disadvantage relative to its competition.

- **Opportunities:** Those positive external factors that increase and support organizational performance.
- **Threats:** Those negative external factors that are beyond the organization's control and that could degrade overall performance. ("SWOT Analysis," 2013, p. 11)

B. ANALYSIS

With the SWOT identified, analysis is conducted to determine potential courses of action to achieve the objective. The analysis performed is commonly referred to as matching and converting. Matching is conducted by matching strengths to opportunities and converting. When strengths are matched to appropriate opportunities, a competitive advantage is developed. Conversion is conducted by converting weaknesses into strengths and threats into opportunities. The conversion takes the negative attributes of an organization and converts them into positive aspects. Conversion may not be possible in all situations; in these cases, mitigation of weaknesses and threats should be considered. Table 1 is an example of a SWOT matrix.

Table 1. An example of a SWOT matrix.

	POSITIVE	**NEGATIVE**
INTERNAL	Strengths	Weaknesses
EXTERNAL	Opportunities	Threats

IV. FINDINGS, SUMMARY, AND RECOMMENDATIONS

A. FINDINGS

Table 2 provides a snapshot of the findings as a result of applying a SWOT analysis to the DOD's current social media policy:

Table 2. A DOD SWOT matrix.

	POSITIVE	**NEGATIVE**
	Strengths	**Weaknesses**
INTERNAL	• Acceptance of social media • Authority to enforce policy	• Lack of OPSEC consideration and guidance • Lack of oversight • Social media tied to personnel rights
	Opportunities	**Threats**
EXTERNAL	• Collaboration with private industries • Monitor social media	• Geotagging • Data mining • Social engineering • Hacking

B. SUMMARY

The SWOT analysis of each branch's social media policy yielded close to identical results. The only deviation worth noting is in the U.S. Army's policy. The Army's policy provides the best OPSEC guidance and the only discussion of the threat environment. The discussion of the threat environment provides a basic overview of OPSEC's importance and the consequences of careless use, providing valuable insight into the real-world impact of social media.

1. Strengths

Analysis of DOD social media policy yielded two strengths. The first and greatest strength is the *acceptance* of social media by the DOD. Choosing to adapt and embrace social media was the right choice for the DOD, as its acceptance allows the DOD to engage with personnel and educate them on safe social media practices. Prohibition of social media would have likely encouraged clandestine use by personnel without having received any education on safe practices. Social media use by DOD organizations provides several effective networks, which the DOD can use to alert personnel about OPSEC threats and provide guidance to mitigate threats. Additionally, social media acceptance permits the DOD to leverage future social media opportunities.

The second strength of the DOD's policy is its authority to regulate personnel conduct. Policy establishes the expectations of an organization, but achieving the desired objectives relies on enforcing expectations. The DOD has the authority to exert control over personal conduct, which permits enforcement of DOD social media policy.

2. Weaknesses

Analysis of DOD social media policy produced three weaknesses. The first notable weakness is a lack of OPSEC consideration and guidance. The current policy focuses primarily on personnel conduct of, emphasizing that personnel should represent their organization in a respectable manner while operating online. The services' policies, however, inadequately address OPSEC. The Navy and Air Force policies fail to even mention OPSEC, while the Marine Corps' policy just briefly mentions the topic. Only the Army policy provides guidance on maintaining OPSEC. This leaves OPSEC, a major threat to social media use, largely unaddressed by DOD policy.

The second identified weakness is an inherent lack of oversight. DOD social media policy does not require oversight of personnel using social media, which leaves the DOD vulnerable to breaches in OPSEC. Oversight provides a mechanism to detect policy violations, with the desire that internal detection occurs before information can be gathered and exploited by adversaries.

Lastly, social media usage is tied to personal rights. Despite the liability created by DOD personnel using social media, the DOD policy is limited in actions it can take to address the liability. The simple answer—to forbid social media use by DOD personnel—would infringe on military members' freedom of speech, as guaranteed by the First Amendment. Even if the DOD could defeat legal challenges to prohibition of social media use by its members, the action would likely create problems in retention and recruitment, especially of younger personnel. Regardless of its desires, the DOD is forced to balance OPSEC with the rights of its members.

3. Opportunities

Two significant opportunities exist for improving OPSEC through changes to the DOD's social media policy. Adoption of social media platforms has bolstered dialogue between the DOD and the private sector. The first opportunity is policy change aimed at promoting DOD collaboration with private industry to develop a policy that addresses OPSEC and technical solutions, which can aid the DOD in monitoring the social media activity of members. There may be resistance to aid the DOD in monitoring its members' activities, but some companies may be willing to assist, since the monitoring is not clandestine.

The second opportunity is the addition of a directive to DOD social media policy that requires online monitoring of DOD personnel using social media. The policy change is an attempt to prevent OPSEC breaches by removing compromised information before it can be exploited. The monitoring would not be hidden from DOD personnel.

4. Threats

DOD social media policy does not provide policy users with an adequate picture of the threat environment. What's more, the DOD's policy does not adequately address the threat that hackers, geo-tagging, data mining, and social engineering pose to OPSEC through social media. Hackers, which can consist of individuals, organized criminal groups, terrorist networks, and advanced nation states, remain a chief concern of the DOD (White House, 2010). These entities utilize a number of varying methods to exploit

social media and networking platforms. Geo-tagging[4] and data mining[5] are both significant concerns for the DOD, as these methods are commonly utilized to exploit it and its service members. Another major threat exists through social engineering.[6]

C. RECOMMENDATIONS

While the DOD's adoption of social media into its network infrastructure has provided a number of benefits, its current social media policy, and that of each of the military services, suffers tremendously from a lack of direction, uniformity, and effective management with regard to OPSEC. Not only do these flaws present a significant risk to the operations, personnel, and networks of the DOD, they pose a significant threat to the national security of the United States. In order to best address OPSEC, USCYBERCOM must ensure that the DOD's social media policy provides effective guidance, oversight, and training. While each of these plays its own distinct role in policy development, all are highly dependent on one another to be effective in mitigating OPSEC incidences.

1. Guidance

Current policy set forth by USCYBERCOM lacks the appropriate level of guidance that is required by each of the services. This flaw results in each branch developing their own social media policy. While this affords each of the services the ability to tailor their particular policy to their respective needs, the end result is a significant gap in uniformity. In order to address this risk factor, USCYBERCOM must provide a more structured set of guidelines and hold each of the services accountable for operating within a designated set of parameters.

Additionally, USCYBERCOM must increase its dialogue with the private sector. This allows for increased exposure to alternative approaches to policy development and

---

[4] Geo-tagging is the process of adding geographical information to various media in metadata form ("What Is Geo-Tagging," 2014).

[5] Data mining is the process of analyzing data from a number of different perspectives and putting it into a useful format (Alexander, 2014).

[6] Social engineering is a nontechnical method where a hacker attempts to manipulate individuals to gain access to confidential information or access to a network. The manipulation is aided by gaining an understanding of one's social circles, which provides insight into choosing the best method for exploiting a target (Criddle, n.d.).

guidance. It also increases exposure to current social media and networking trends. Early visibility can play a key role in the organization's ability to adapt to any significant changes in social media trends.

2. Oversight

The best laws and regulations are meaningless unless there is oversight to ensure that they are followed. With that in mind, three solutions have been identified to provide oversight of DOD personnel's social media usage. First, service members and civilian personnel must be screened on entry into their respective service to determine what social media sites they use. Additionally, they will be instructed to provide updates to their command if they adopt additional social media sites during their tenure. This will provide the DOD with a list of social media profiles that require monitoring. Failure to provide accurate information will subject the service member to administrative action at the command level.

The second solution is to monitor service member and civilian personnel activity on social media. The list of active social media profiles developed from the screening process will be evaluated periodically, which will require the development of an automated search system. Search protocols can then be applied to search for specific key words, dates, times, and photos. The metadata in the photos can then be searched for GPS coordinates to determine if service members are posting pictures of sensitive locations. In the event that a profile is flagged, the service member's command will be notified.

Lastly, commands will be required to document all OPSEC violations occurring on social media. This will be aided by the automated search system. All commands will be required to submit reports of violations to USCYBERCOM, which will allow them to develop data on violations. The data can then be analyzed to provide metrics that describe personnel at risk of committing OPSEC violations throughout the DOD.

3. Training

The human element is the number one threat to OPSEC. Therefore, periodic training for DOD personnel should occur to help ensure that OPSEC is maintained at all times. It is recommended that all service members and civilian personnel be required to

take the OPSEC Awareness training provided by the Center for Development of Security Excellence, on a semiannual basis. This course, whether completed online or in-house, provides basic information to protect unclassified information at both the personal and operational levels (Joint Knowledge Online, n.d.). Additionally, every command at all levels of the DOD must be required to conduct semiannual social media and networking use training. The benefit of this is two-fold: it reinforces the broader training received from the Center for Development of Security Excellence, while also holding each respective command accountable for the actions of their personnel.

D. AREAS FOR FUTURE RESEARCH

The cybersecurity threat landscape is rapidly changing. Included in this, are the ongoing cultural shifts in social media and networking adaptation, and social media use by both individuals and organizations. It is important to note that the analysis, conclusions, and recommendations provided in this project represent a relatively specific viewpoint for a very broad subject matter. In order to increase understanding of social media's impact on DOD OPSEC, we recommend the following be considered when conducting future research and analysis:

- Conduct a CLASSIFIED SWOT analysis
- Explore further integration of private industry policy into DOD policy
- Analyze and compare OPSEC incidents between services to better determine potential causal factors
- Analyze and compare OPSEC incidents between warfare domains, within each service, to better determine potential causal factors
- Conduct analysis to determine which social media platforms have a higher percentage of OPSEC-related incidents
- Compare demographic factors and their potential relationship with OPSEC incidents
- Analyze and compare OPSEC incidents between different countries[7]
- Conduct analysis using alternative methods such as the value, rarity, imitability, and organizations (VRIO) framework[8]

[7] The United Kingdom's cybersecurity strategy was published in November 2011, and is available on https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (Cabinet Office, 2011).

[8] The value, rarity, imitability, and organizations (VRIO) framework was developed and introduced by Jay B. Barney as a strategic management tool to analyze a company's internal resources and capabilities in order to sustain competitive advantage (Barney, 1995).

APPENDIX. DOD SOCIAL MEDIA INSTRUCTIONS EXCERPTS

The following are from the official social media instructions provided by the DOD, Army, Air Force, Navy, and Marine Corps.

Department of Defense Internet Services and Internet-Based Capabilities
(Department of Defense, 2012)
(Department of Defense, 2014)

PURPOSE. This Instruction:

A) Incorporates and cancels Deputy Secretary of Defense Memorandum, and Directive-Type Memorandum (DTM) 09–026.
B) Establishes policy, assigns responsibilities, and provides instructions for establishing, operating, and maintaining DOD Internet services on unclassified networks to collect, disseminate, store, and otherwise process unclassified DOD information. Use of Internet-based capabilities (IbC) to collect, disseminate, store, and otherwise process unclassified DOD information.

APPLICABILITY. This Instruction:

A) Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DOD Field Activities, and all other organizational entities within the DOD (hereinafter referred to collectively as the "DOD Components").
B) Applies to DOD Internet services and use of IbC provided by morale, welfare, and recreation (MWR), military exchanges, and lodging programs for use by authorized patrons.
C) Applies to contractors and other non-DOD entities that are supporting DOD mission-related activities or accessing DOD Internet services or IbC via DOD information systems, to the extent provided in the contract or other instrument by which such authorized support or access is provided.

Does NOT:

A) Prevent unit commanders or Heads of the DOD Components from providing alternate, stand-alone capabilities to allow access to IbC for mission or morale purposes.
B) Prohibit DOD employees from using IbC from personal Internet-capable devices for personal purposes.

C) Apply to using IbC specifically for penetration testing, communications security monitoring, network defense, personnel misconduct and law enforcement investigations, and intelligence-related operations.

POLICY. It is DOD policy that:

A) Decisions to collaborate, participate, or to disseminate or gather information via DOD Internet services or IbC shall balance benefits and vulnerabilities. Internet infrastructure, services, and technologies provide versatile communication assets that must be managed to mitigate risks to national security; to the safety, security, and privacy of personnel; and to Federal agencies.

B) DOD Internet services and IbC used to collect, disseminate, store, or otherwise process DOD information shall be configured and operated in a manner that maximizes the protection (e.g., confidentiality, integrity, and availability) of the information, commensurate with the risk and magnitude of harm that could result from the loss, compromise, or corruption of the information. This applies to both public and non-public DOD information. With regard to use of IbC, this applies to the integrity and availability of public DOD information. IbC shall not be used to collect, disseminate, store, or otherwise process non-public DOD information, as IbC are not subject to Federal or DOD information assurance (IA) standards, controls, or enforcement, and therefore may not consistently provide confidentiality.

C) DOD information systems (IS) hosting DOD Internet services shall be operated and configured to meet the requirements in DOD 8500.01E and DODI 8500.2, and certified and accredited in compliance with DODI 8510.01.

D) Effective information review procedures for clearance and release authorization for DOD information to the public are conducted in compliance with DODD 5230.09 and DODI 5230.29. DOD information intended for non-public audiences requires similar review and consideration prior to dissemination. DOD employees shall be educated and trained to conduct both organizational and individual communication effectively to deny adversaries the opportunity to take advantage of information that may be inappropriately disseminated.

E) Public DOD websites shall be operated in compliance with established laws and requirements. Detailed explanations, and implementation guidance are provided at the Web Manager's Advisory Council website at http://www.howto.gov/web-content/.

F) DOD Internet services and the information disseminated via these services, where appropriate, shall be made available to Federal initiatives such as Data.gov, Recovery.gov, and USA.gov to reduce duplication and to foster greater participation, collaboration, and transparency with the public. Where feasible and appropriate, such DOD information shall be provided as datasets in raw (machine readable) format as defined in DepSecDef Memorandum.

G) All unclassified DOD networks (e.g., Non-classified Internet Protocol Router Network (NIPRNET), the Defense Research and Engineering Network) shall be configured to provide access to IbC across all the DOD Components.

H) Authorized users of unclassified DOD networks shall comply with all laws, policies, regulations, and guidance concerning communication and the appropriate control of DOD information referenced throughout this Instruction regardless of the technology used. Furthermore, all personal use of IbC by means of Federal government resources shall comply with paragraph 2–301 of DOD 5500.7-R.

Army Cyber Command (ARCYBER)

(Brown, 2012)
(Department of the Army, Office of the Chief of Public Affairs, 2013)
(United States Army, 2011)

The Army recognizes that social media gives personnel the ability to communicate expeditiously with larger audiences in a number of different ways. It has become an important tool for Army messaging and outreach. The Army uses a variety of social media platforms designed to support a range of media from text, audio, pictures and videos, all of which are generated and maintained by organizations and individuals within the department. The Army understands the risks associated with social media and has developed training to help both Soldiers and family members use social media responsibly.

Social media is a powerful communications tool and when used correctly, it can help Army commands reach an enormous audience. Social media can help organizations engage in the conversation while at the same time promoting awareness of the organization's main communication priorities. But not all Army commands use it effectively. Most of social media failures can be attributed to organizations rushing into social media before determining what exactly the organization aims to achieve with social media platforms. Using social media effectively is a process and it requires strategy, goals, manpower and foresight.

Soldiers have always been the Army's best and most effective messengers. Within today's warfare environment, social media enables the Army family around town, around the country and around the world to stay connected and spread the organization's key themes and messages. Every time a member of the service joins social media, it increases the timely and transparent dissemination of information. It ensures that the Army's story is shared honestly and directly to Americans where they are and whenever they want to see, read or hear it. Social media allows every Soldier to be a part of the Army story and it allows America to connect with the service component. Social media is a cheap, effective and measurable form of communication. The Army uses social media to tell the Army's story, but it also uses social media to listen.

Developing a successful social media presence does not happen overnight, it is a detailed process that requires extensive planning and execution. It starts with stating the organization's missions, messages and themes. Once an organization establishes a direction, it can begin to develop a detailed social media communication strategy that provides input into all the social media platforms supported by the organization. The purpose of using social media is to place your unit's messages in the social media space. However, in order to keep people coming back to the pages, units should develop a strategy that mixes messages with items the audience finds interesting. Language should be conversational, fun and engaging. It must also be noted that official use of social media platforms must be in compliance with Army public affairs policy. Content must be in the public domain or approved for release by the commanding officer. Commands are ultimately responsible for content posted on their platforms.

The Army classifies social media sites as External Official Presences (EOP's). In 2010, the office of the Secretary of the Army released a delegation of authority approving the use of EOPs. This directive covers both command units as well as Army Family Readiness Groups. All Army EOP's must adhere to the following standards. The Office of the Chief of Public Affairs has the right to deny any page during the approval process if one or more of the following standards are not met:

A) *Whenever the option is available, EOP's should be categorized as a government page.*
B) *Installation Facebook pages should be named U.S. Army XXX (e.g. U.S. Army Fort Riley). For other pages, include the Commander-approved names and logos (e.g. 1st Brigade, 25th Infantry Division [Family Readiness]), not nicknames nor mascots (e.g."Dragons").*
C) *Branding (official name and logos) across all social media platforms (i.e. Facebook, Twitter, Google+) should be uniform. If needed, use http://www.army.mil/create/ to download the Army's social media branding toolkit.*
D) *Include a statement acknowledging this is the "official [Facebook, Twitter, Google+, etc.] page of [enter your unit or organizations name here] [Family Readiness]."*
E) *Include contact information (AKO email address).*
F) *Facebook pages must include "Posting Guidelines" under "General Information." Use the U.S. Army's Facebook rules of engagement (http://www.facebook.com/USarmy/info) as a reference and/or visit the Department of Defense Social Media user agreement at http://www.defense.gov/socialmedia/user-agreement.aspx.*
G) *Be recent and up-to-date. Updates must not be older than one month.*
H) *Ensure Operations Security Training is completed on an annual basis. The Information Assurance Training Center offers the Social Media and Operations Security Training Course: https://ia.signal.army.mil/sms.asp. EOP operators must also take the Defense Information Systems Agency's social networking class: http://iase.disa.mil/eta/sns_v1/sn/launchPage.htm.*

I) *FRSAs/FRG leaders should provide all page administrators and FRG members with the U.S. Army Social Media OPSEC presentation and the FBI Briefing on Identity Theft located on the U.S. Army's share site at www.slideshare.net/usarmysocialmedia*

J) *Page administrators are solely responsible for ensuring that the content posted on EOP's adheres to Operations Security guidelines. Administrative departments are responsible for documenting and removing any OPSEC violations prior to bringing them to the attention of their local OPSEC Officer or the U.S. Army's OPSEC Program Manager.*

K) *EOP's should not be used as a place for personal advertisements nor endorsements.*

L) *All pages must be registered through the U.S. Army at www.army.mil/socialmedia. Prior to submitting a link for inclusion on the registry, users must confirm that social media pages adhere to the submission guidelines.*

Since social media use is so commonplace in our day-to-day interactions, it is easy to become complacent. In order to maintain OPSEC, it is important to remain vigilant at all times. Sharing seemingly trivial information online can be dangerous to loved ones and fellow Soldiers—and may even get them killed. America's enemies scour blogs, forums, chat rooms and personal websites to piece together information that can harm the U.S. and its Soldiers. One recommendation is to never accept a friend request from someone you don't know, even if they know a friend of yours. Another is to not share information that you don't want to become public. Someone might target you for working in the DOD and one should exercise caution when listing your job, military organization, education and contact information. Providing too much information in your profile can leave you exposed to people who want to steal your identity or sensitive operational information. Understanding what you can and cannot post on social media platforms goes a long way in protecting yourself online, but adjusting your privacy settings can do more.

Another area of concern entails geotagging. Geo-tagging is the process of adding geographical identification to photographs, videos, websites and SMS messages. It is the equivalent of adding a 10-digit grid coordinate to everything posted on the Internet. Some smartphones and digital cameras automatically embed geotags into pictures, and many people unknowingly upload photos to the Internet that contain location information. A variety of applications are capitalizing on user desire to broadcast their geographic location. The increased popularity of location-based social networking is changing the way we view security and privacy on an individual level and creating OPSEC concerns on an Army level. One Soldier exposing their location can affect the entire mission. Deployed Soldiers or personnel conducting operations in classified areas should not use location-based social networking services. These services will bring the enemy right to the Army's doorstep.

Air Forces Cyber (AFCYBER)
(United States Air Force, 2009)

In the past, the Air Force did not officially engage blogs or other forms of social media. Air Force leaders now realize the broad reach, both positive and negative; these forms of communication have on Airmen and society, as well as the value of maintaining a presence in this information domain. While communication with media and the public has traditionally been the responsibility of Public Affairs, today all Airmen are communicators. All Airmen are encouraged to use social media to communicate about topics within their areas of expertise, or their interests. The more traditional form of vertical communication is critical for the Air Force, but new technologies give Airmen the opportunity to horizontally inform the media, the public and each other.

In an effort to manage resources more effectively, the Air Force issued a policy to end its long-standing tradition of producing printed base newspapers in lieu of online publications. This action provides a good start for the Air Force to take advantage of disseminating its news via Web 2.0 avenues. Progress is being made toward helping Airmen engage each other across the social media spectrum with a higher goal of transparently reaching out to industry leaders, other agencies and the general public. The Air Force is currently creating an official, and active, presence in the larger world of social media and with the help of Airmen that presence will grow and flourish.

Strong social media policies and guidelines are necessary to actively engage Web 2.0 applications and Internet audiences. The guidelines allow Airmen to understand what is and is not allowed, thereby setting expectations. Good policies can also help protect people from getting in trouble. Considering that security is critical and is at the source, all policies will be reviewed by Air Force officials to ensure that legal and ethical problems are addressed. Airmen should note that anytime they engage in social media they are representing the Air Force and therefore should not do anything that will discredit himself or herself or the organization. In general, the Air Force views personal Websites and blogs positively, and it respects the rights of Airmen to use them as a medium of self-expression.

In today's warfare environment, Airmen must abide by certain restrictions to ensure good order and discipline. All Airmen are on duty 24 hours a day, 365 days a year and all actions are subject to the Uniform Code of Military Justice (UCMJ). Even if Airmen state they are not representing the Air Force other audiences may not interpret the information that way. Airmen, by the nature of the business, are always on the record and must always represent the core values, even on the Web: integrity first, service before self and excellence in all that is done.

Current Air Force guidelines consist of the following:

A) *No Classified Info: Do not post classified or sensitive information (for example, troop movement, force size, weapons details, etc.). If in doubt, talk to your supervisor or security manager.*
B) *Replace Error With Fact, Not Argument: When you see misrepresentations made about the Air Force in social media, you may certainly use your blog or someone else's to point out the error. Always do so with respect and with the facts. When you speak to someone with an adversarial position, make sure that what you say is factual and is not disparaging. Avoid arguments.*
C) *Admit Mistakes: Be the first to respond to your own mistakes. If you make an error, be up front about your mistake and correct it quickly. If you choose to modify an earlier post, make it clear that you have done so (such as by using the strikethrough function).*
D) *Use Your Best Judgment: Remember there are always consequences to what you write. If you're still unsure, and the post is about the Air Force, discuss your proposed post with your supervisor. Ultimately, however, you have sole responsibility for what you choose to post to your blog.*
E) *Avoid The Offensive: Do not post any defamatory, libelous, vulgar, obscene, abusive, profane, threatening, racially and ethnically hateful, or otherwise offensive or illegal information or material.*
F) *Avoid Copyright: Do not post any information or other material protected by copyright without the permission of the copyright owner.*
G) *Don't Breach Trademarks: Do not use any words, logos or other marks that would infringe upon the trademark, service mark, certification mark, or other intellectual property rights of the owners of such marks without the permission of such owners.*
H) *Don't Violate Privacy: Do not post any information that would infringe upon the proprietary, privacy or personal rights of others.*
I) *Avoid Endorsements: Do not use the Air Force name to endorse or promote products, opinions or causes.*
J) *No Impersonations: Do not forge or otherwise manipulate identifiers in your post in an attempt to disguise, impersonate or otherwise misrepresent your identity or affiliation with any other person or entity.*
K) *Use Disclaimers: Identify to readers of a personal social media site or post that the views you express are yours alone and that they do not necessarily reflect the views of the Air Force. Use a disclaimer such as: "The postings on this site are my own and don't necessarily represent Air Force positions, strategies or opinions."*
L) *Stay in Your Lane: Discussing issues related to your AFSC or personal experiences is acceptable but do not discuss areas of expertise for which you have no background or knowledge.*
M) *Link: You may provide a link from your site to an Air Force website.*

There are movements within the DOD to explore a broader, more aggressive and holistic approach that must be developed and employed in order to integrate. The rules of the game have clearly changed. Until now, the Air Force has not had an official stance on engaging bloggers, social media and Web 2.0 initiatives. However, by being a part of this trend, the organization's Public Affairs department is embarking into a new world of communication for the Air Force. Because Airmen are the voice of the organization, he Public Affairs department has the responsibility to tell the Air Force story in a thoughtful, engaging and exciting manner by taking advantage of the same popular Web 2.0 tools and services used by corporate and industry leaders.

Fleet Cyber Command (FLTCYBERCOM)
(Department of the Navy, Office of the Secretary, 2012)

The mission of the U.S. Navy's Fleet Cyber Command is to serve as the central operational authority for networks, cryptologic/signals intelligence, information operations, cyber, electronic warfare, and space capabilities in support of forces afloat and ashore. It is also to direct Navy cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace, to organize and direct Navy cryptologic operations worldwide and support information operations and space planning and operations. Furthermore, the goal is to execute cyber missions as ordered and to direct, operate, maintain, secure, and defend the Navy's portion of the Department of Defense Information Networks (DoDIN). By doing so, the organization will be able to deliver integrated cyber, information operations, cryptologic, and space capabilities to provide a common cyber operational picture.

As directed by DOD Directive 5122.05, it is the policy of the DOD to make available timely and accurate information so that the public, Congress, and the news media may assess and understand the facts about national security and defense strategy. Requests for information from organizations and private citizens shall be answered in a timely manner. In carrying out the policy, the following principles of information will apply:

- *A) Information will be made fully and readily available, consistent with statutory requirements, unless its release is precluded by current and valid security classification. The provisions of the Freedom of Information Act will be supported in both letter and spirit.*
- *B) A free flow of general and military information will be made available, without censorship or propaganda, to the men and women of the Armed Forces and their dependents.*
- *C) Information will not be classified or otherwise withheld to protect the U.S. government from criticism or embarrassment.*
- *D) Information will be withheld only when disclosure would adversely affect national security, threaten the safety or privacy of the men and women of the Armed Forces, or if otherwise authorized by statute or regulation.*

E) The DOD's obligation to provide the public with information on its major programs may require detailed public affairs planning and coordination within the DOD and with the other governmental agencies. The sole purpose of such activity is to expedite the flow of information to the public; propaganda has no place in the DOD public affairs programs.

The Internet is a powerful information tool. The appearance, accuracy, currency, and relevance of the information presented by Navy and Marine Corps commands on the Internet reflect upon the Department of the Navy's (DON's) professional standards and credibility. Additionally, information residing on a Web server associated with a "navy.mil" or "marines.mil" domain is interpreted by the worldwide public, including the American taxpayer and media, as reflecting official Navy or Marine Corps policies or positions. Therefore, all information presented must be accurate, truthful, current and in compliance with DON public information policies.

Official DON guidance with regard to publicly accessible Web presences is based on Federal law and specific DOD policy. This instruction applies to all DON commands and activities and all publicly-accessible DON website's, related technologies, and Internet-based capabilities (IbC), collectively termed as 'web presences', designed, developed, procured, or managed by DON activities or by their contractors. A designation of 'Unofficial' is not recognized for any DON Web presence.

A command presence within an IbC, while an official presence, is considered to be a part of that social media site and not an independent presence. IbC's are defined as publicly accessible information capabilities and applications available across the Internet in locations not owned, operated, or controlled by the DOD or the Federal government. IbC include collaborative tools such as social networking sites (SNS), social media, user-generated content, social software, Web-based email, instant messaging, and discussion forum. Some examples of IbC include YouTube, Facebook, Flickr, Twitter, and Google applications among.

Individual members of the DON are authorized to participate in or operate blogs or other social networking services. The DON recognizes the value of these communication channels in posting current information and supporting the morale of personnel, their families, and friends. As long as personnel adhere to specific restrictions on content, the DON encourages the use of blogs and social networking services, and recognizes this free flow of information contributes to legitimate transparency of the DON to the U.S. public whom the DON serves. In any instance in which an individual member of the DON is identified as such, either directly or indirectly, on a blog or other social media service, that individual is considered as representing the DON and must act accordingly.

In addition to the types of information listed in paragraph 3c of Section 0702, the following information must not be displayed on personal IbC operated by individual members or on presences to which the individual may publish:

A) *Any image, still or motion, of any military operation or activity unless that image is personal and has been cleared by the proper authority if there is a potential for a security or privacy violation.*
B) *Language that may tend to diminish the confidence in or respect due to his or her superior officer(s), per the Uniform Code of Military Justice.*

Marine Forces Cyber Command (MARFORCYBER)
(United States Marine Corps, 2012)

The U.S. Marine Corps (USMC) must continuously innovate to communicate in media-intensive environments, to remain the nation's force in readiness. This mission is based on the Marine Corps Vision and Strategy 2025 and the public affairs tasks outlined in the Marine Corps Service Campaign Plan for 2009–2015. While building and launching a social media program or accessing a favorite social media site can sometimes be fast, easy, and inexpensive. Existing rules for public affairs as well as personal conduct still apply.

The USMC encourages Marines to explore and engage in social media communities at a level they feel comfortable with. The best advice is to approach online communication in the same way we communicate in person, by using sound judgment and common sense, adhering to the USMC's core values of honor, courage and commitment, following established policy, and abiding by the UCMJ. While some may assert that social media has improved the way we connect and communicate as a culture, it presents dilemmas for USMC leaders, ranging from being a social media 'friend' of a subordinate to "following" those you lead. The point to consider, though, is that social media is about connecting. Just as USMC leaders may interact and function in their local community alongside their Marines, similar conduct holds true for interacting in the same social media spaces as their subordinates. It is how the connections and interactions take place with subordinates that set the tone for communication. Basically, online USMC relationships should function in the same manner as any professional relationship would.

With social communication, you essentially provide a permanent record of what you say; if you wouldn't say it in front of a formation, don't say it online. If you come across evidence of a Marine violating command policy or the UCMJ on social media platforms, you should respond in the same manner you would if you witnessed the infraction in any other environment. When using social media tools and platforms, everything you say and do, as a leader is more visible and taken more seriously. As such, you have a greater responsibility to speak respectfully and intelligently about issues. Remember, when making statements online, you are being viewed as the authority on that topic and may appear to be speaking on behalf of the entire command or even as a spokesperson for the USMC, depending on the audience or venue.

The following guidelines are must be followed if leadership decides to utilize social media:

A) *Listen to active audiences to determine how to best engage. The paradigm of telling everyone what they need to know no longer carries significant weight when communicating via social media channels-social media requires, and begins with, listening. If you don't know and understand the audiences you are communicating with, then the interaction will be of limited value. Listening to the online community and complying with DOD policies is paramount to communication success.*

B) *You are key to uniting the voice of all Marines using social media speaking on behalf of your command. These Marines must have an accurate understanding of the information that should be communicated to the public in order to ensure accuracy, preserve safety, assure security, and establish credibility.*

C) *The Corps' actions are legitimate and, the assumption is, an informed public will agree with this principle. To strengthen this position, the Freedom of Information Act emphasizes the importance of transparency in military activities. We do not "spin" information or stories and do not condone manipulating the social media flow by creating posts designed to mislead followers or control a conversation. Every website, 'fan page', or other online destination managed by Marines must make that fact known to users.*

D) *Marines and staff moderating and managing USMC online presences must be authorized to track and monitor the activity that takes place there. Just as you grant release authority for information by public affairs or unit information Marines, the same authority is applicable for command personnel representing your unit through social media.*

E) *Timeliness is defined in terms of the information interests and demands of the public. Empower your Marines to anticipate these interests and effectively balance the timing of communications. The basic guidance for this concept applies both maximum disclosure and minimum delay.*

F) *Security of operations, personnel, equipment, information, and facilities must be anticipated and evaluated before information is communicated to the public such as preventing the premature disclosure of dates, times and locations of deployments or deployed locations, and homecomings to and from the continental U.S. or ports of call.*

G) *Privacy of individual service members must be protected. The Privacy Act of 1974 set this principle into law. Marines must remain conscientious with regard to any personally identifiable information that we collect, including how we collect, store, use, or share that information; all which should be done pursuant to applicable privacy policy, laws and information technology rules.*

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alexander, D. (2014). Data mining. Retrieved from http://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/Alex/

Anderson, J., & Rainie, L. (2014, July 3). Net threats [Report]. Retrieved from http://www.pewinternet.org/2014/07/03/net-threats/

Barney, J. B. (1995). Looking inside for competitive advantage. *Academy of Management Executive*, *9*(4), 49–61. Retrieved from http://www.jstor.org/stable/4165288?seq=1#page_scan_tab_contents

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Meditated Communication*, *13*(1), 210–230. doi:10.1111/j.1083-6101.2007.00393.x

Brinkley, D. (2014). *Fundamentals of information technology GB3020: Welcome to information technology* [PowerPoint slides]. Retrieved from Naval Postgraduate School Sakai website: https://cle.nps.edu/xsl-portal

Brown, B. (2012, December 4). *Standardizing official U.S. Army external official presences (social media)* [Memorandum]. Washington, DC: Department of Defense.

Budzyna, T. (2010, August 31). Social media shapes markets, the military and life. *DoD News*. Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=60665

Burson-Marsteller. (2010). *Burson-Marsteller Fortune global 100 social media study*. New York, NY: Author. Retrieved from http://www.burson-marsteller.com/bm-blog/burson-marsteller-fortune-global-100-social-media-study/

Cabinet Office. (2011). *The UK cyber security strategy: Protecting and promoting the UK in a digital world*. London, United Kingdom: Author. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Coate, P. (2007). *Focus on strategic management*. Bradford, United Kingdom: Emerald Group Publishing.

Criddle, L. (n.d.). What is social engineering? Retrieved from http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

Department of the Army, Office of the Chief of Public Affairs (2013). *The United States Army social media handbook*. Washington, DC: Author. Retrieved from http://www.arcent.army.mil/docs/default-document-library/social_media_handbook_version3-1.pdf?sfvrsn=2

Department of Defense. (2011). *Department of Defense strategy for operating in cyberspace*. Washington, DC: Author. Retrieved from http://www.defense.gov/news/d20110714cyber.pdf

Department of Defense. (2012, September 11). *DOD Internet services and Internet-based capabilities* (DOD Instruction 8550.01). Washington, DC: Author. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/855001p.pdf

Department of Defense. (2014, March 14). *Cybersecurity* (DOD Instruction 8500.01). Washington, DC: Author. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

Department of the Navy, Office of the Secretary. (2012, February 21). *Department of the Navy public affairs policy and regulations* (SECNAV Instruction 5720.44C). Washington, DC: Author. Retrieved from http://doni.documentservices.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-700%20General%20External%20and%20Internal%20Relations%20Services/5720.44C%20CH-1.pdf

Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015a, January 9). *Frequency of social media use*. Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/2015/01/09/frequency-of-social-media-use-2/

Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015b, January 9). *Social media update 2014*. Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/2015/01/09/social-media-update-2014/

Edwards, J. (2014, July 24). Facebook Inc. actually has 2.2 billion users now—Roughly one third of the entire population of earth. *Business Insider*. Retrieved from http://www.businessinsider.com/facebook-inc-has-22-billion-users-2014-7

Goodrich, R. (2015, January 1). SWOT analysis: Examples, templates & definition. *Business News Daily*. Retrieved from http://www.businessnewsdaily.com/4245-swot-analysis.html

Huergo, J. (2014, February 12). NIST releases cybersecurity framework version 1.0. Retrieved from http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm

Hughes, M. (2015, February 19). What are APIs, and how are open APIs changing the Internet. Retrieved from http://www.makeuseof.com/tag/api-good-technology-explained/

Jeyarathmm, M. (2008). *Strategic management*. Mumbai, India: Himalaya Publishing House.

Joint Chiefs of Staff. (2011, August 11). Joint Publication 3: Joint Operations. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf

Joint Chiefs of Staff. (2013, March 25). Joint Publication 1: Doctrine for the Armed Forces of the United States. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp1.pdf

Joint Chiefs of Staff. (2014, November 20). Joint Publication 3-13: Information Operations. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

Joint Knowledge Online. (n.d.). OPSEC awareness [Interactive web-based course]. Retrieved from https://jkodirect.jten.mil/Atlas2/faces/page/login/Login.seam

Kaplan, A. M. (2012, March/April). If you love something, let it go mobile: Mobile marketing and mobile social media 4x4 [Abstract]. *Business Horizons, 55*(2), 129–139. Retrieved from http://www.sciencedirect.com/science/article/pii/S0007681311001558

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons, 53*(1), 59–68. Retrieved from http://www.michaelhaenlein.eu/Publications/Kaplan,%20Andreas%20-%20Users%20of%20the%20world,%20unite.pdf

Langer, E. (2014). What's trending? Social media and its effect on organizational communication. *University of Wisconsin-La Crosse Journal of Undergraduate Research, 17*, 1–14. Retrieved from http://www.uwlax.edu/urc/JUR-online/PDF/2014/Langer.Emily.CST.pdf

Lynn, W. J. (2010, September/October). Defending a new domain. *Foreign Affairs, 89*(5), 97–108. Retrieved from http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

National Institute of Standards and Technology. (2013). *Improving critical infrastructure cybersecurity: Preliminary cybersecurity framework.* Gaithersburg, MD: Author. Retrieved from http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf

National Institute of Standards and Technology. (2014). *Framework for improving critical infrastructure cybersecurity: Cybersecurity framework*. Gaithersburg, MD: Author. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Pew Research Center. (n.d.). *Social networking fact sheet* [Fact sheet]. Washington, DC: Author. Retrieved from http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/

Pew Research Center. (2010). *Updated: Change in Internet access by age group, 2000–2010*. Washington, DC: Author. Retrieved from http://www.pewinternet.org/2010/09/10/updated-change-in-Internet-access-by-age-group-2000-2010/

Schroer, W. J. (n.d.). Generation X, Y, Z, and others. Retrieved from http://www.socialmarketing.org/newsletter/features/generation3.htm

Solis, B. (2013). The conversation prism. Retrieved from http://www.conversationprism.com/

SWOT analysis. (2013). In *Free Management Ebook*. Retrieved from http://www.free-management-ebooks.com/dldebk-pdf/fme-swot-analysis.pdf

United States Air Force. (2009). *Social media and the Air Force*. Washington, DC: Author. Retrieved from http://www.24af.af.mil/shared/media/document/AFD-091210-043.pdf

United States Army. (2011). *6 social media considerations for deployed soldiers and their families* [PowerPoint slides]. Retrieved from http://www.arcent.army.mil/docs/default-document-library/smr-week-37-social-media-considerations-for-deployed-soldiers-and-their-families.pptx?sfvrsn=2

United States Marine Corps. (2012). *The U.S.M.C. social media principles*. Washington, DC: Author. Retrieved from http://www.jbsa.af.mil/shared/media/document/AFD-120412-038.pdf

United States Strategic Command. (2015). U.S cyber command [fact sheet]. Retrieved from http://www.stratcom.mil/factsheets/2/Cyber_Command/

Weisgerber, M. (n.d.). The Pentagon spends too much time and money on buying weapons that don't deliver, and that's hurting national security. *Government Executive.* Retrieved from http://www.govexec.com/feature/slow-and-steady-losing-defense-acquisition-race/

What is geo-tagging? Securing yourself, your family, and your assets. (2014). [blog]. Retrieved from https://www.fishnetsecurity.com/6labs/blog/what-geo-tagging-securing-yourself-your-family-and-your-assets

White House. (2010). *National security strategy*. Retrieved from http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

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