NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INFORMATION SHARING WITHIN THE FLTCYBERCOM/C10F ORGANIZATION

by

Eva Castillo

June 2020

Thesis Advisor: Dan C. Boger
Second Reader: Sharon M. Runde

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
INFORMATION SHARING WITHIN THE FLTCYBERCOM/C10F ORGANIZATION

5. FUNDING NUMBERS
19RFMN1

6. AUTHOR(S) Eva Castillo

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)
Fleet Cyber Command

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.

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

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Effective information sharing between various commands is essential for an organization to effectively and efficiently meet the mission. The U.S. Fleet Cyber Command/U.S. 10th Fleet (FLTCYBERCOM/C10F) organization, per their home page, is composed of more than 14,000 active and reserve Sailors and civilians organized into 28 active commands, 40 cyber mission force units, and 27 reserve commands around the globe. Operators within the organization are charged with providing real-time information for decision-makers at all operational levels. In the current and future cyber environment, it is fundamentally important for commanders to have real-time information at their disposal for decision-making. This thesis has two goals. The first goal is to assess whether existing information systems, mandates, policies, or service-level agreements (SLAs) are limiting information sharing within the FLTCYBERCOM/C10F organization. The second goal is to seek solutions that support current and evolving requirements.

14. SUBJECT TERMS information sharing, enterprise information sharing, U.S. Fleet Cyber Command, FLTCYBERCOM, interoperability	**15. NUMBER OF PAGES** 71
	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.

INFORMATION SHARING WITHIN THE FLTCYBERCOM/C10F ORGANIZATION

Eva Castillo
Lieutenant, United States Navy
B, Excelsior College, 2017

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN NETWORK OPERATIONS AND TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
June 2020

Approved by: Dan C. Boger
Advisor

Sharon M. Runde
Second Reader

Thomas J. Housel
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Effective information sharing between various commands is essential for an organization to effectively and efficiently meet the mission. The U.S. Fleet Cyber Command/U.S. 10th Fleet (FLTCYBERCOM/C10F) organization, per their home page, is composed of more than 14,000 active and reserve Sailors and civilians organized into 28 active commands, 40 cyber mission force units, and 27 reserve commands around the globe. Operators within the organization are charged with providing real-time information for decision-makers at all operational levels. In the current and future cyber environment, it is fundamentally important for commanders to have real-time information at their disposal for decision-making. This thesis has two goals. The first goal is to assess whether existing information systems, mandates, policies, or service-level agreements (SLAs) are limiting information sharing within the FLTCYBERCOM/C10F organization. The second goal is to seek solutions that support current and evolving requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ABWC	Assistant Battle Watch Captain
AWS	Amazon Web Services
BAO	BMC Atrium Orchestrator
BBNA	BMC Blade Logic Network Automation
BPPM	BMC Blade Logic Performance Management
BSA	BMC Blade Logic Server Automation
BWC	Battle Watch Captain
C10F	U.S. Tenth Fleet
C2	Command and Control
C4ISR	Command, Control, Communications, Computers Intelligence, Surveillance, and Reconnaissance
CCIR	Commander's Critical Information Requirements
CDO	Cyber Defense Operations
CIO	Chief Information Officer
CNO	Chief of Naval Operations
CONUS	Continental U.S.
COP	Common Operating Picture
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DOD	Department of Defense
DODIN-N	Department of Defense Information Networks - Navy
DoN	Department of Navy
EIS	Enterprise Information Systems
ENMS	Enterprise Network Management System
FCC	U.S. Fleet Cyber Command
GNOC	Global Network Operations Center
GNOSC	Global Network Operations and Security Center
GOTS	Government Off the Shelf
HBSS	Host Based Security System
HCI	Human Computer Interactions

INOSS	Integrated Navy Operations Support System
ISP	Internet Service Providers
IT	Information Technology
IT-21	Information Technology for the 21st Century
ITSM	IT Service Management
ITSO	IT Service Operations
JFHQ	Joint Force Headquarters
JFTOC	Joint Fleet Telecommunications Operations Center
JRSS	Joint Regional Security Stack
MADSS	Mission Assurance Decision Support System
MOC	Maritime Operations Center
NAVSOC	Naval Satellite Operations Center
NAVWAR	Naval Information Warfare Systems Command
NC3	Nuclear Command and Control Communications
NCSA	Navy Cyber Situational Awareness
NCSS	National Cyber Security Strategy
NCTAMS	Naval Computer and Telecommunications Area Master Stations
NCTS	Naval Computer and Telecommunications Station
NENS	Navy Enterprise Networks
NETOPS	Network Operations
NGEN	Next Generation Enterprise Network
NMCI	Navy/Marine Corps Intranet
NNWC	Naval Network Warfare Command
NOC	Network Operating Centers
NTOC	Network Tactical Operations Center
NWC	Naval War College
OCONUS	Outside Continental U.S.
ONE-NET	Navy Enterprise Network
PAC	Pacific
PACOM	Pacific Command
PAPM	Principal Assistant Program Manager
PEO	Program Executive Officer

PMW 130	Information Assurance and Cyber Security Program Office
PMW 790	Shore and Expeditionary Integration
POR	Program of Record
PRNOC	Pacific Region Network Operations Center
PRSOC	Pacific Region Security Operations Center
SENAV	Secretary of the Navy
SIPR	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SPAWAR	Space and Naval Warfare Systems Command
STACC	Shore Tactical Assured Command and Control
USCYBERCOM	U.S. Cyber Command
USD AT&L	Under Secretary of Defense for Acquisition, Technology, and Logistics
VTC	Video Teleconference
WO	Watch Officer

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to the following individuals: my advisor, Dr. Dan Boger, for his guidance and patience; Chloe Woida, a writing coach, for not only for deciphering my madness but also for pushing me to be a better writer; and my second reader, Sharon Runde, for her guidance.

It would take a separate thesis to recognize all the others who helped me cross the finish line, so I would like to broadly thank the support given by all military and civilian organizations that supported this research. Without you, this thesis would not have been possible.

Attending NPS as a single mom of two was very stressful at times. I am forever indebted to my family and friends who supported me while working on my thesis. Without their support, I would never have finished with my sanity.

Lastly, I would like to specifically acknowledge my parents, and both my boys, Jayden and Liam, for their unconditional love and support. Without knowing it, they push me to be better!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

This thesis has a primary and secondary purpose. The primary purpose is to determine if existing enterprise information systems (EIS), mandates, policies, and service-level agreements (SLAs) are impacting U.S. Fleet Cyber Command (FCC)/U.S. Tenth Fleet (C10F)'s ability to efficiently share information within its organization by ensuring that existing enterprise information systems (EIS), mandates, policies, and service-level agreements (SLAs) are performing in the desired manner that promotes information sharing. The secondary purpose is to recommend reliable, efficient, and secure information systems, mandates, and policy solutions furthering FCC/C10F's ability to effectively execute its mission.

The Department of the Navy relies on timely information for all operations and the ability to analyze and use that information effectively and efficiently in real-time is imperative. At the very foundation of efficiently utilizing information, is proper and real-time information sharing between organizations. Lack of information sharing is typically due to various obstacles that may limit an organization's ability to send, receive and process data in real-time. Experts have commented that barriers often prevent organizations from being fully interoperable (Chen, 2006). According to Chen, "barriers are incompatibilities of various kinds and at various enterprise levels" (Chen, 2006, p. 2). A real-world example of this is an operator being unable to provide the real-time status of a system or subordinate organization due to specific service-level agreements (SLAs) verbiage that does not support 100% data sharing. Information sharing and real-time statuses are impossible without the free flow of timely and accurate data.

FCC's command mission is, according to their public homepage, to "plan, coordinate, integrate, synchronize, direct, and conduct the full spectrum of cyberspace operational activities required to ensure freedom of action across all of the Navy's warfighting domains in, through, from cyberspace, and to deny the same to the Navy's adversaries" (FCC/C10F, n.d., para. 2). C10F is considered more operational vice administrative. They are charged with carrying out specific missions and exercises in support of FCC. According to C10F, their mission is to "to plan, monitor, direct, assess,

communicate, coordinate, and execute operations to enable command and control and set the conditions for subordinate success through a task force structure similar to other warfare commanders" (FCC/C10F, n.d., para. 3). They can conduct operational tasking through their Maritime Operations Center (MOC) located in Fort George Meade, Maryland (FCC/C10F, n.d., para. 2).

A. SIGNIFICANCE OF RESEARCH

In 2018, then FCC/C10F Chief of Staff (COS), Captain James Mills (now retired) directed the N9 to head up research on visualization of data, human computer interactions (HCI), and identify the most efficient way to display network health and status to a watch stander and decision-maker. Specific guidance included:

1. Using the Integrated Navy Operations Support System (INOSS) architectural framework, evaluate existing software tools for deployment to Department of DODIN-N watch floors, NOCs, and for use by afloat IT personnel. As of April 2020, the term INOSS has been changed to Integrated Navy Operations Command and Control System (INOCS). Due to the advanced stage of writing of this thesis, the author chose to continue using INOSS.
2. Consider industry and other government implementations, best practices, and employment of similar systems.
3. Integrate existing and novel malicious activity notifications into the INOSS framework to allow appropriate personnel the freedom to quarantine and investigate the activity.
4. Identify how these tools will support existing Navy programs of record.

B. PROBLEM STATEMENT

Organizations within the FCC/C10F organization utilize an array of tools and processes to support and defend and protect Navy networks, however, they lack a common infrastructure and an interoperable tool or enterprise policy that permits technology to best support network operations (NETOPS). In today's environment,

employing technology to solve operational issues is pivotal. Reliable, timely, and accurate information sharing is required for the most basic of operations. Interoperability or effective information sharing should not be impeded by EISs, policies, or SLAs. Information systems are continuously exploited and attacked. The ability to share information is important at all levels; however, this thesis will focus on processes within the FCC/C10F organization.

The U.S. Navy relies on the transport, exchange, and processing of data in both ashore and afloat environments. Commanders require the ability to monitor Navy networks for management, situational awareness, and initiatives. Field observations for this thesis revealed that in the current operating environment, commands are inundated with various systems that are not interoperable, do not work to their full potential, or do not work at all for the contested environment the Navy operates in today. According to a DOD instruction, the information environment is a "complex layering of multiple networks with overlapping, duplicative roles and responsibilities" (DOD, 2013b, p. 28) that do not fully support information sharing. The hindrance of information exchange due to technical limitations, mandates, policies, or SLAs can place the Navy at a massive disadvantage.

In today's world, organizations need, according to Panetto and Cecil (2013), "collaboration using information technology and other tools to succeed" (p. 1) in a competitive environment. Enterprise information sharing is essential for ashore and afloat commands. The process is often complicated by rapidly changing opportunities, technologies, policies, or legislation (Panetto & Cecil, 2013). Often, an organization may find themselves in an immediate need or opportunity to acquire new technology and they make decisions without long term thought to enterprise communication over time. Ideally, all data, services, processes, and entities within the organization should operate at an enterprise level. When there are subordinates within an organization operating at different policy and access control levels, that can negatively impact the overall ability of the organization to share information effectively.

Changes in software, hardware, mandates, and policies can help an organization align processes conducive to information sharing and reduce barriers. This positive

change is due to software, hardware, mandates, and policies supporting each other for the free flow of information throughout the organization. It is integral to information sharing that mandates, policies, and orders are positively contributing to the organization's ability to share information.

C. RESEARCH QUESTIONS

1. What information technologies in use are negatively affecting FCC/C10F's ability to share and receive timely information across the organization?
2. How might changes in information technologies positively affect FCC/C10F's ability to share and receive timely information across the organization?
3. What mandates or policies in use are affecting negatively FCC/C10F's ability to share and receive timely information across the organization?
4. How might changes in mandates or policies positively affect FCC/C10F's ability to share and receive timely information across the organization?
5. What contractual issues are negatively affecting FCC/C10F's ability to share and receive timely information across the organization?
6. How might contractual changes positively affect FCC/C10F's ability to share and receive timely information across the organization?

D. PRELIMINARY RESEARCH APPROACH

The goal of this thesis is to assess whether the available tools, existing policies, or contractual agreements are undermining information sharing within the FCC/C10F organization, and to seek technical solutions, mandates or policy changes to support current and evolving requirements. This thesis will focus on technology, policy, and SLA concerns that prohibit or restrict information sharing and that increase latency and reduce accuracy for the decision-makers.

The scope of systems to be researched include any software, hardware, applications, or architectures in use that could be improved upon for better information sharing. This research is limited to the Navy/Marine Corps Intranet (NMCI) and the information systems, mandates, policies, and SLAs within that network. Due to scope limitations, it does not include the afloat Information Technology for the 21st Century network (IT-21) or the Navy Enterprise Network (ONE-NET).

In this research environment, mandates and policies are dispersed at different levels. Operational orders are directives that drive military operations at all levels. They serve as the principal means by which the commander expresses decisions, intent, and guidance. They are directives issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. They can be utilized for short-term and long-term operations. Regulatory measures and policies include directives from the Department of Defense (DOD), Executive Branch, and legislation from Congress to protect information and systems. The policies will focus on Tier 1, Tier 2, and Tier 3 organizations in three key policy areas: Technical Policy, Organization Policy, and Regulatory/Executive Policies.

Issues within SLAs can lead to poor information sharing within an organization. Per a Department of the Navy (DON) Chief Information Officer (CIO) Enterprise Commercial Information Technology (IT) Strategy Team member, SLAs "provide an agreed upon framework for the delivery of services and the measurement of service quality" (Panaro, 2010, para. 21). They detail the responsibilities of the vendor to the organization. Some of the field research conducted implied that information sharing was reduced because current SLAs in place were not granular enough to support such a requirement. For example, an information system used by Logistics may suit their needs but the same system does not provide enough detail for a Comptroller to project budgets. To share information effectively across multiple entities, all programs need to have the ability to share and receive information. This research will broadly examine SLAs and how they can impact information sharing.

The research objectives include:

- Describing the current organizational relationships between the Tier 1, 2, and 3 organizations,
- Describing current mandates and policies at the organizations,
- Describing current technological tools in use,
- Describing potential contractual issues,
- Explaining how changes in technological tools, mandates, policies, and contracts can increase information sharing within the organization, and
- Providing recommendations.

The overall approach is based on a survey of relevant academic literature and field observations. This will be discussed in more detail in the chapter on the research design.

E. OVERVIEW

As a portion of a larger research project funded by FCC, this information sharing research focuses on the impact on network operations at the unit and operational levels. Chapter II provides an overview of the entire project encompassing autonomous actions, network traffic anomaly detection, and visualization on Navy networks. The overall goal is to establish positive and negative effects to facilitate access to real-time information on Navy networks.

To fully grasp the concepts of information sharing, it is important to understand what is gained from effective information sharing and what is lost by inefficient information sharing. Chapter III provides literature that supports this research while also examining pitfalls that contribute to decreased information sharing.

To identify positive and negative impact areas, it was imperative to research efforts and processes that were successfully and unsuccessfully implemented. Field research and interviews were conducted with various military and civilian industry leaders. Chapter IV details the results of those visits.

Information learned through field research and interviews are further analyzed in Chapter V. This chapter will detail specific technologies, policies, mandates, and SLAs and their individual limiting factors, solutions, and best practices.

Chapter VI will summarize the main points of this research and provide recommendations for concrete actions to enhance information sharing within a DOD organization.

THIS PAGE INTENTIONALLY LEFT BLANK

II. FLEET CYBER COMMAND PROJECT

A. NAVY'S CYBER VISION

> Our Navy will protect America from attack, promote American prosperity, and preserve America's strategic influence. U.S. naval operations—from the seafloor to space, from the blue water to the littorals, and in the information domain—will deter aggression and enable resolution of crises on terms acceptable to the United States and our allies and partners. (Chief of Naval Operations, 2018, p. 1)

This is part of the mission statement that was promulgated by Admiral John M. Richardson, in A Design For Maintaining Maritime Superiority. From this statement, one can gather that now, more than ever, the information domain plays a vital role in protecting our country. Within the information domain falls the cyber domain and FCC/C10F, which have been charged with defending and delivering effects in and through cyberspace. From FCC's command page, part of their mission is to "conduct operations in and through cyberspace, the electromagnetic spectrum, and space to ensure Navy and Joint/Coalition freedom of action and decision superiority while denying the same to our adversaries" (FCC/C10F, n.d., para. 1). FCC and C10F are co-located in Fort Meade, MD, and also have a dual-hatted commander.

B. FCC/C10F TASKING

In 2018, then-FCC/C10F Chief of Staff (COS) Captain James Mills directed the N9 to head up research on visualization of data, human computer interactions (HCI), and identify the most efficient way to display network health and status to a watch stander and decision-maker. Specific guidance included:

Using the Integrated Navy Operations Support System (INOSS) architectural framework, evaluate existing software tools for deployment to the Department of DODIN-N watch floors, NOCs, and for use by afloat IT personnel.

1. Consider industry and other government implementations, best practices, and employment of similar systems.

2. Integrate existing and novel malicious activity notifications into the INOSS framework to allow appropriate personnel the freedom to quarantine and investigate the activity.

3. Identify how these tools will support existing Navy programs of record.

This led to the funding for NPS research to be conducted by thesis students. Dr. Dan Boger was appointed as the Principal Investigator and then selected students with skill sets that aligned with the requirements of the aforementioned research. The theses and their respective deliverables are as follows:

C. ARCHITECTING AUTONOMOUS ACTIONS IN NAVY ENTERPRISE NETWORKS (NENS)

Dr. Dan Boger and Dr. Luqi are co-thesis advisors for LT Max Geiszler. This thesis investigates Navy Enterprise Networks (NENs) in an attempt to better understand the fundamental operation of the Navy's networks. The main idea behind that research is to explain how NENs can conduct NetOps to meet unique Navy mission sets and ensure adequate information is given to higher up organizations. The investigation covers some of the use-cases in which the Navy has an intensive need for human-driven processes to accomplish necessary critical tasks. It also explores where man-hours are being inefficiently spent due to process redundancy and limited human watch-stander proficiency. It then suggests a technical architectural change to NEN infrastructure utilizing the INOSS framework, which helps to facilitate automated solutions to problems that have been presented by FCC/C10F. It also suggests a change to tightly integrate DevOps in operational processes.

D. NETWORK TRAFFIC ANOMALY DETECTION ON A NAVY NETWORK

Dr. John Monaco is the thesis advisor for LT Michael Laws and LT Greg Bunder. This thesis determines the viability of using existing unsupervised machine learning techniques to detect anomalous network traffic from an unclassified Navy network with a level of accuracy equal to current anomaly detection systems. Upon completion, this thesis gives a recommendation as to whether unsupervised machine learning can be used

for anomaly detection. If the hypothesis is accurate, that this is possible and is a more efficient method than what is currently used, then a detailed analysis of which features are most important for anomaly detection along with any lessons learned and obstacles met during research are provided. Lastly, this thesis addresses what an architecture might look like that would be used to implement network anomaly detection via unsupervised machine learning within the INOSS framework.

E. THE FUNCTIONAL AND CONCEPTUAL APPROACH TO NETWORK OPERATIONS

Dr. Dan Boger is the thesis advisor for Commander Henry Lee Bush. The thesis analyzes the current visualization efforts at various organizations, the private sector, and the public sector, to better understand how visualization provides a network's health and status. The main idea behind the thesis is to evaluate visualization in key focus areas: a single pane of glass, information immersion, information framework, and information concept. It does this by covering case studies that were done through the site observation to identify how information is collected, processed, analyzed, and visualized to support command and control of the network. Through the case studies, the thesis also reviews the information not captured because of stovepiped systems, limited shared management information, and those manual processes which reduce the information in visualization. The information not captured in turn impacts situational awareness and decision-making which negatively impacts command and control of the network. The thesis recommends the use of the INOSS functional framework to improve processes to support visualization of information and information immersion through space design. Lastly, it introduces an information management concept to support the command and control of the network.

F. HOW INFORMATION SHARING AFFECTS NETWORK OPERATIONS

Dr. Dan Boger is the thesis advisor for this author. Effective information sharing between various components are crucial to FCC/C10F successfully and efficiently meeting the mission. The thesis has two goals. The primary goal is to examine whether existing information systems, mandates, policies, or Service Level Agreements (SLAs) are limiting information sharing within the FCC/C10F organization. The secondary goal

is to seek technical and non-technical solutions to support current and evolving requirements. The thesis will evaluate solutions studied that can positively impact information sharing for the organization. Research approaches include interviews and observations in academia, civilian IT sector, defense organizations, programs of record, and Tier 1, 2, and 3 providers. From the research gathered, conclusions are drawn to the effectiveness of current technologies, mandates, and policies, and proposed solutions are offered.

III. LITERATURE REVIEW

Literature and policies distinctly discuss the importance of information sharing but there appears to be a gap between theory and implementation in the fleet. Government and DOD documents connect information sharing to capabilities needed to meet the mission and acknowledge the importance of alignment between technology and policies which are also supported in preliminary research into barriers of effective information sharing. The 2018 National Cyber Security Strategy (NCSS) specifically identifies and establishes the importance of information sharing. The Secretary of the Navy's (SENAV) 2019 Cyber Readiness Review expressed concern for the DON to "take immediate steps to lower the barriers to communication to enhance information sharing and collaboration" (SECNAV, 2019, p. 16). Ample scholarly literature has reinforced the necessity for effective information sharing, thus making this research pivotal. This chapter will examine national strategy, DOD documents, and various literature through primary and secondary research methods to research information systems, policies, and SLAs that are limiting information sharing, and provide recommendations that will have a positive effect on information sharing.

A. NATIONAL STRATEGY

The NCSS emphasizes the importance of better information sharing to improve awareness and reduce duplicative activities (White House, 2018). Both the military and the nation are growing increasingly reliant upon critical infrastructures and cyber-based information systems. The NCSS identifies that reliable information analysis that is quickly available has continued to be an enduring challenge. According to the President, "New threats and a new era of strategic competition demands strategy that responds to new realities and deters adversaries " (White House, 2018, p. 2). To accomplish the national strategy, effective information sharing is essential. According to the NCSS, a purely technocratic approach is insufficient to address the ever-changing problems the Navy continues to face; effective policies are also required. Every goal and intention within the NCSS requires effective information sharing. Most external research is

conducted in support of cyber threat information; however, this research will examine different approaches to positively impact information sharing to include technologies, policies, and SLAs at an operational level within the FCC/C10 organization.

B. DOD DOCUMENTS

Information sharing is a critical enabler of situational awareness of the DODIN-N and DOD missions. According to DOD Instruction 8320.02, "data, information, and IT services are considered enablers of information sharing to the DOD" (Department of Defense [DOD], 2013a, p. 2). The instruction specifies that "data, information, and IT services will be made visible, accessible, understandable, trusted, and interoperable throughout their life cycles for all authorized users" (DOD, 2013a, p. 14). The instruction establishes the role of the DOD CIO is to:

> Guide and oversee matters related to the sharing of data, information, and IT services to ensure interoperability down to the technical level internally with DOD and externally with mission partners, including: establishing, maintaining, and enforcing governance of the DOD's IT policies and processes to enable secure sharing of DOD data, information, and IT services, including information assurance, discovery, accessibility, and dissemination requirements. (DOD, 2013a, p. 6)

DISA is a supporting agency of the DOD. Its main goal is to support and defend the DODIN. Under the DOD CIO, the Defense Information Systems Agency (DISA) is responsible for:

> Enterprise technical feasibility assessments with recommendations for sharing all DOD data, information, and IT services as directed and make available enterprise services and the interface standards and specifications for the sharing of data, information, and IT services in order to meet the needs of the DOD. (DOD, 2013a, p. 6)

Lastly, according to a DOD instruction, the "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD AT&L) shall update defense Acquisition System policies and procedures and provide guidance to program managers and Program Executive Officer to evaluate and approve system or program implementation of data sharing practices" (DOD, 2013a, p.7).

C. LITERATURE

The literature suggests that information technology, policies, and SLAs must be aligned to be effective. The U.S. Navy understands this concept and has been actively pursuing all avenues that provide better situational awareness for commanders. At the core of all military operations across forces, situational awareness is paramount. In 2015, Rear Adm. David Lewis, the commander of the Space and Naval Warfare Systems Command (SPAWAR) (now known as the Naval Information Warfare Systems Command (NAVWAR)), stated, "Emerging technology and improved cyber performance are inexorably linked" (SPAWAR, 2015, para 3). Research has been conducted into individual systems and the level of details they provide to the common operating picture (COP), consolidation of command and control (C2) systems, and defining a common architecture across all surface combatants and maritime domain awareness. As Leedom (2019) pointed out, a COP is a repository of information for decision-makers. That repository depends on real-time information sharing. Furthermore, Leedom asserts the repository should present organized information that is easily identifiable and relevant to the decision-maker.

Barriers that affect effective information sharing include conceptual, technological, and organizational barriers (Chen, 2006). Chen (2006) goes on to suggest that, conceptual barriers pertains to syntactic and semantic compatibility, technological barriers pertains to platform and software technology and organizational barriers to overall responsibilities and structure. These barriers include who is responsible for what, who is authorized to do what, and overall structure of the organization. When attempting to exchange data in an environment where all the data is coming from differing sources, each receiving systems needs to be able to process the data. Syntactic differences focus on syntax and format whereas semantic differences focus on systems end to end being able to exchange and utilize the information being passed.

The Naval War College (NWC) has studied how well the Navy and industry are prepared for network-centric warfare. Dombrowski and Ross pointed out that "the Navy's abilities to collect and share information, sustain operations, operate in a more stealthy fashion, and directly contribute to the defense of the American homeland will improve"

(Dombrowski and Ross, 2003, p. 20). Information sharing is pivotal to a network-centric environment. Network-centric warfare consists of a battle group or joint task force that can share real-time knowledge through common communications systems. The research conducted focused on command, control, communications, computers, intelligence, surveillance, reconnaissance (C4ISR) requirements, but success would have been impossible without effective information sharing. According to the Deputy Chief of Naval Operations for Information Dominance, "Capabilities required across the DOD to enable information sharing, collaboration, and interoperability will be provisioned as enterprise services" (Office of the Deputy Chief of Naval Operations for Information Dominance, 2012, para 4). Although just a theory years ago, the need for information sharing in support of real-time operations and network status is vital for a military organization with interoperability as a goal.

IV. RESEARCH OBSERVATIONS

This thesis is a small part of a larger research project. The research was conducted as a team with individual emphasis on each of our individual thesis topic areas. Fieldwork was conducted to gather information through live observations and interviews with subject matter experts. This approach allowed an opportunity for one-on-one demonstrations that facilitated thorough research. On-site visits were conducted at military and civilian organizations. The objective was to understand the watch/organization environment, view firsthand current technologies, processes, procedures, and best practices utilized regarding real-time information sharing in support of the status of networks. Follow up research was conducted with some organizations to ascertain whether or not any updates or changes had been completed since the site visit.

This chapter will provide an overview of the setup of each organization visited to include its mission, watch setup, and tool usage if any. Further analysis to identify problems and possible solutions will be discussed in Chapter V. Some of this information will be covered broadly as there are hundreds of thousands of policies that may impact a command, and it was beyond the scope of this research to address all of them. Therefore, this thesis broaches key policies as a starting point to improve network-centric warfare practices for situational awareness and information sharing.

A. MILITARY

This section will detail multiple organizations' missions and watch team set up to show the scope of responsibility of the organization and the importance of real-time information sharing. This section will also discuss tool usage at each organization. Due to individual missions, some organizations may utilize more tools than others. The research team visited several military sites. A majority of the sites had relatively large and disjointed networks that isolated themselves from other applications and systems. Many of the sites displayed issues due to multiple programs of record (PORs), decentralized management, lack of common tools, varying installation methods, and lack of NetOps

framework, all of which greatly affect an organization's ability to efficiently share information.

On-site visits were conducted with larger military commands within the FCC/C10F organization such as Navy Network Warfare Command (NNWC), Navy Computer Telecommunication Master Area Station Pacific (NCTAMS PAC), Defense Information Systems Agency (DISA), Information Assurance and Cyber Security Program Office (PMW 130) and Shore and Expeditionary Integration (PMW 790), all identified in Table 1. Not all commands under the FCC/C10F were able to be visited or contacted for this research.

Table 1. Research Team's Visits (Military)

Short Name	Name	Location
FCC/C10F	Fleet Cyber Command/U.S. Tenth Fleet (Telephone)	VA
NNWC	Navy Network Warfare Command	Norfolk
NCTAMS PAC	Navy Computer Telecommunication Master Area Station Pacific	Hawaii
DISA	Defense Information Systems Agency	Hawaii
PMW 130	Information Assurance and Cyber Security Program Office	San Diego
PMW 790	Shore and Expeditionary Integration	Charleston

a. FLTCYBERCOM/C10F

Per the FCC/C10F Strategic plan, globally, FCC/C10F is responsible for "directing the operations and defense of the Navy's networks and operating shore-to-ship communications systems, including Nuclear Command and Control Communications

(NC3)" (FCC/C10F, 2015, p. 10). As an Echelon II command, they report directly to the CNO. FCC/C10F does not rely on any tools that are generic to the watch floor. They rely entirely on reporting from subordinate commands via human interaction or message traffic.

To better support their mission, information sharing in support of real-time network status is crucial. At the heart of the command is the Battle Watch Captain (BWC), who maintains real-time situational awareness and is the principal advisor to the commander. They are able to meet their responsibilities with the support of an Assistant Battle Watch Captain (ABWC) and a watch team that includes a watch section for Network Operations (NETOPS), Signal Intelligence (SIGINT), Intel, NMCI, and Video Teleconference (VTC), among others not expanded upon in this research.

The DODIN OPS Watchstander monitors all message traffic and notifies the BWC of any pertinent information or network outages. Additionally, they coordinate with NNWC if necessary, to determine the resolution of network outages that meet FCC Commander's Critical Information Requirements (CCIR) criteria and monitor the health and status of the NC3 infrastructure. The DODIN OPS watch is typically filled by junior enlisted personnel. The SIGINT WO works with the regional task forces and ships monitoring point guard and Secret Internet Protocol Router Network (SIPR) connectivity from the ship to the shore. They also monitor any cryptologic collections and connectivity of systems on afloat units to provide real-time situational awareness for afloat units. This is typically filled by Petty Officer Second or Petty Officer First class. The watch also maintains dedicated 24/7 VTC and NMCI representative support. All watch stations collectively, with other support staff support, the commander's decision cycle through real-time information and network statuses. The commander's decision cycle is displayed in Figure 1.

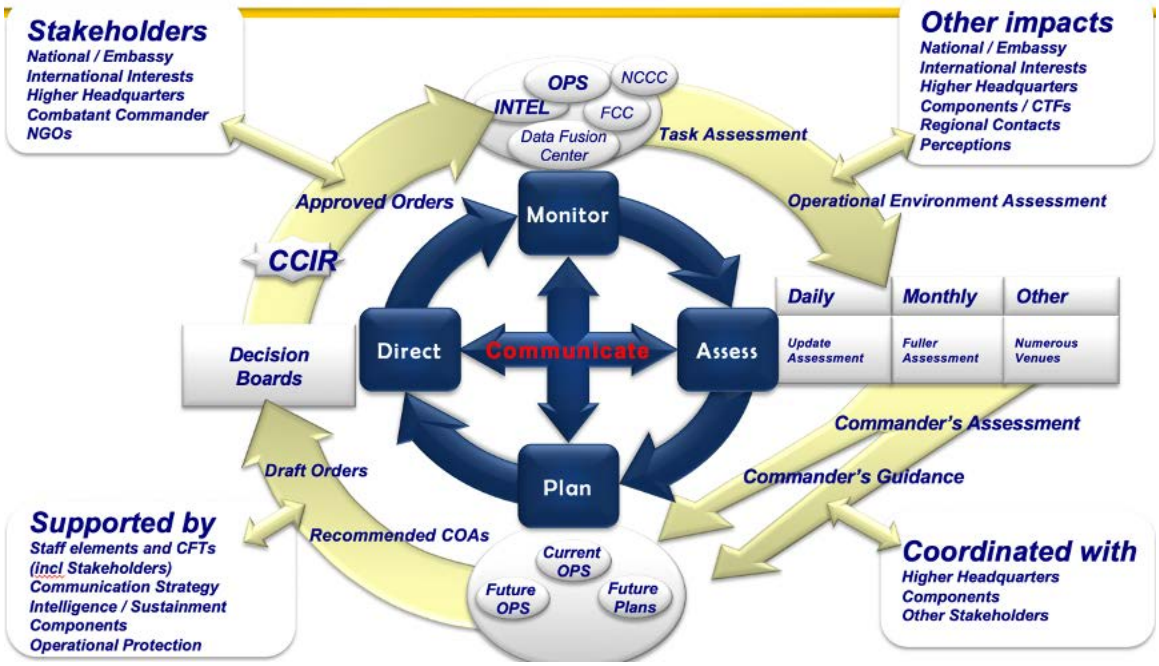

Figure 1. Commander's Decision Cycle. Source: FCC/C10F MOC (2015).

FCC/C10F is responsible for reporting the statuses of many commands. If any of the organizations beneath them were to lose connectivity, they would not know the network status in real-time. According to NNWC:

> In 2002, some 23 organizations from several commands, including the former Naval Space Command, Naval Computer and Telecommunications Command, Fleet Information Warfare Center, and Navy Component Task Force - Computer Network Defense were brought together to form Naval Network Warfare Command, emphasizing the organization's focus on the operation and defense of the Navy's networks. (NETWARCOM, n.d.-b, para. 1.)

As a tactical arm of FCC/C10F, NNWC reports to FCC/C10F. The current process of notification is for components subordinate to NNWC to report them via phone, email, or update brief and then that information is passed up the chain of command to FCC/C10F. As a Fleet Commander, FCC may not have an interest in knowing the real-time status of certain components that are not considered critical. Despite the priority of various components, this thesis attempts to explore a way for NNWC to receive and provide reports closer to real-time.

b. Naval Network Warfare Command (NNWC)

NNWC's mission, according to its public homepage, is to "execute tactical-level command and control to DOD Information Networks; leverage Joint Space capabilities for Navy and Joint Operations" (NETWARCOM, n.d.-a, para. 1). NNWC reports their status and those of their subordinates directly to FCC/C10F. Subordinate commands are identified in Figure 2. NNWC is able to accomplish its mission with over 13,000 personnel and is responsible for multiple commands and detachments. They implement critical requirements for subordinate commands for decision-making and situational awareness. NNWC is focused on operating, securing, and managing the network and utilizes a variety of tools.

NNWC has several sites that report to them and they report to FCC/C10F, which in turn reports to Joint Force Headquarters (JFHQ) DODIN. The Navy has many different command relationships, and information sharing in support of the mission is vital in every single entity. As a part of a larger relationship, NNWC's subordinate commands that require continuous monitoring and reporting include the Global Network Operations and Security Center (GNOSC), NMCI, Naval Computer and Telecommunications Area Master Station Pacific (NCTAMS PAC), Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT), Naval Computer and Telecommunications Station (NCTS) Bahrain, NCTS Naples, NCTS Far East and Naval Satellite Operations Center (NAVSOC). The BWC plays a vital role in monitoring and reporting to higher headquarters. The NNWC structure can be seen in Figure 2 This organizational chart is an overview of the subordinate commands that fall under NNWC purview. This thesis will focus on NNWC's ability to share and receive real-time information throughout the larger organization.

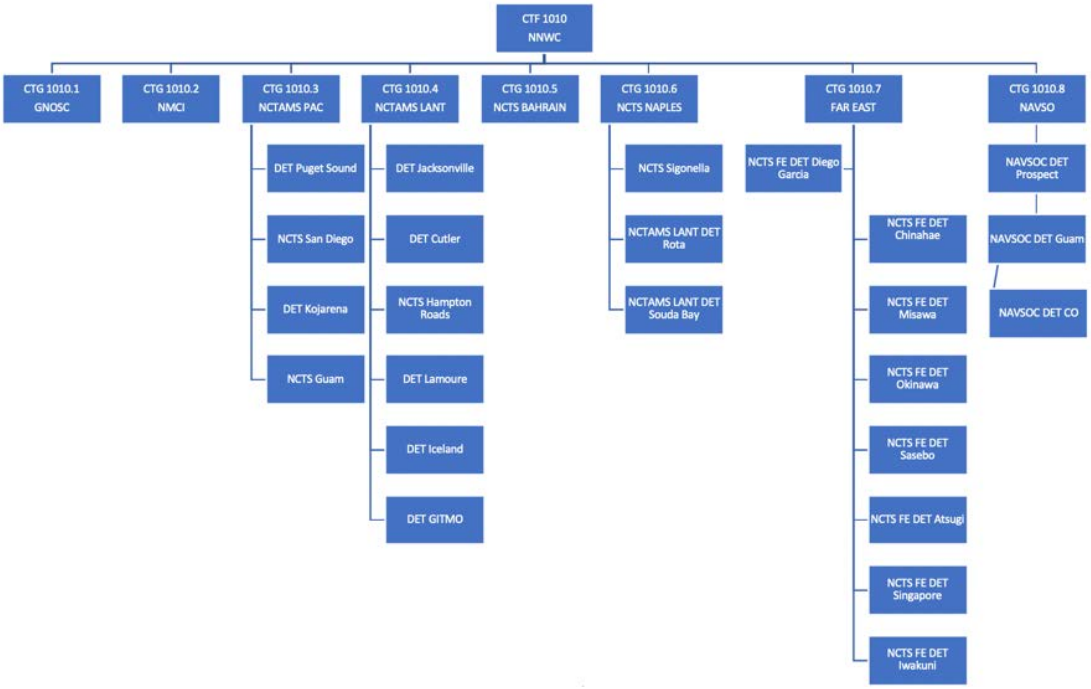

Figure 2. NNWC Organization Chart. Adapted from NETWARCOM (n.d.).

The watch stations observed at NNWC in support of the BWC included the IT Service Operations (ITSO), Network Tactical Operations Center (NTOC), Joint Regional Security Stack (JRSS), and the Host Based Security System (HBSS). Per the NNWC BWC, NNWC currently does not have a real-time COP where they can see the entire network and receive updates real-time. NNWC currently relies on daily updates via VTC, briefs, chat, and telephone. Shared cyber awareness via information sharing is integral for the critical information that NNWC is responsible for. Extended outages, not knowing exactly where the outages are, or reporting inaccurate information are all errors that could be rectified significantly with improved information sharing across the enterprise.

In the absence of a central automated COP, NNWC relies on data aggregation or analysis from various tools that are available to everyone to include: Splunk, Forescout, NETSCOUT, Mission Assurance Decision Support System (MADSS), Enterprise Network Management System (ENMS) and Tanium.

- SPLUNK is a tool that allows the ability to search, analyze, and visualize large amounts of data. This is a popular tool in the fleet to assist in helping organizations meet compliance requirements, implement continuous monitoring, detect patterns, and provide overall real-time situational awareness in operations. Splunk is dependent upon data inputs from various POR systems.

- Forescout allows the ability to automate security and compliance with its agentless software. The software conducts discovery and classification of all devices on the network to better facilitate system administration. In the cyber world, to defend a network, it is vital to know what assets are connected to it. Forescout solutions can help in that realm but do not provide a "one-stop" solution that is geared toward real-time information sharing.

- NETSCOUT is a live monitoring tool that can monitor and analyze network and application traffic flows through all of the NMCI nodes. NETSCOUT offers several different products; however, NETSCOUT is not one of the organizations the research team visited or researched further in this thesis. Additional research should be conducted to see how NETSCOUT can fit into the picture of delivering real-time information flow throughout the FCC/C10F organization.

- MADSS allows the BWC team the ability to see the status of all DISA circuits, maintenance, or authorized service interruptions (ASIs). According to DISA, "Whether it's part of the deliberate planning process or analyzing courses of action for a contingency, such as a natural disaster, the Mission Assurance Branch ensures the Defense Information Systems Network (DISN) experiences minimal disruption" (DISA, 2018, para. 3). The criticality of real-time information sharing is further stressed according to DISA, "because the DOD relies so heavily on the DISN, any interruption to the critical infrastructure could severely affect DOD's

ability to execute its mission, thus negatively impacting the warfighter" (DISA, 2018, para. 6).

- ENMS is said to be providing a "COP-like" picture for the Fleet NOCs. A lot of commands use it largely for their ticketing system. A Principal Assistant Program Manager (PAPM) at PMW 790 described ENMS as a capability under the Shore Tactical Assured Command and Control (STACC) POR that supports Network Operations (NetOps). One of the NetOps capabilities is to provide a NetOps COP, and this is accomplished with the use of several tools. The overarching tool for presentation is Edge Appboard. This tool interfaces with Edge Technologies enPortal web server that collects data from various servers such as BMC IT Service Management (ITSM), BMC Atrium Orchestrator (BAO), BMC Blade Logic Server Automation (BSA), BMC Blade Logic Network Automation (BBNA), BMC Blade Logic Performance Management (BPPM), and others. One of the most used tools is the AfloatSA, which is government off-the-shelf (GOTS) developed code to infer as much as possible about afloat systems based on what watch standers can see from the shore. This provides an overarching view of all the afloat units in the area of responsibility (AOR). This research focuses on the capability of shore units. There is a similar tool for Ashore NOC components under Ashore SA.

- Tanium is another tool in use by NNWC. It allows for visibility and control of endpoints on a network, but it is not a full solution that would support information sharing on an enterprise level. In layman's terms, it allows you to ask a question against the network, e.g., does any user on X network have Y file, and you will get an answer very quickly from over 290,000 devices. Tanium is deployed on NIPRNet. Tanium is very powerful but it has its disadvantages, which will be explored in Chapter V.

The Tanium organization is not one of the organizations the research team visited or researched further in this thesis.

The tools discussed previously individually do not help with ensuring the FCC/C10F organization can share information efficiently in support of real-time network statuses. They are discussed to give an idea of the current capabilities of NNWC and an overview of some of the tools in use. Further analysis and recommendations will be in Chapter V.

c. Naval Computer and Telecommunications Area Master Station Pacific (NCTAMS PAC)

With a force of over 700 personnel, NCTAMS PAC has a three-part mission. Part I of the mission is to provide operational C4I capabilities to assets in the Pacific and Indian Ocean areas of operation. Part II of the mission is to operate, maintain, secure, and defend the Navy's portion of the DODIN in its AOR. Finally, part III of the mission is to direct the day to day operations of two subordinate commands, two detachments, and eight activities across 12 time zones (NCTAMS PAC, n.d., p. 1). NCTAMS PAC AOR can be seen in Figure 3 NCTAMS PAC reports directly to NNWC.

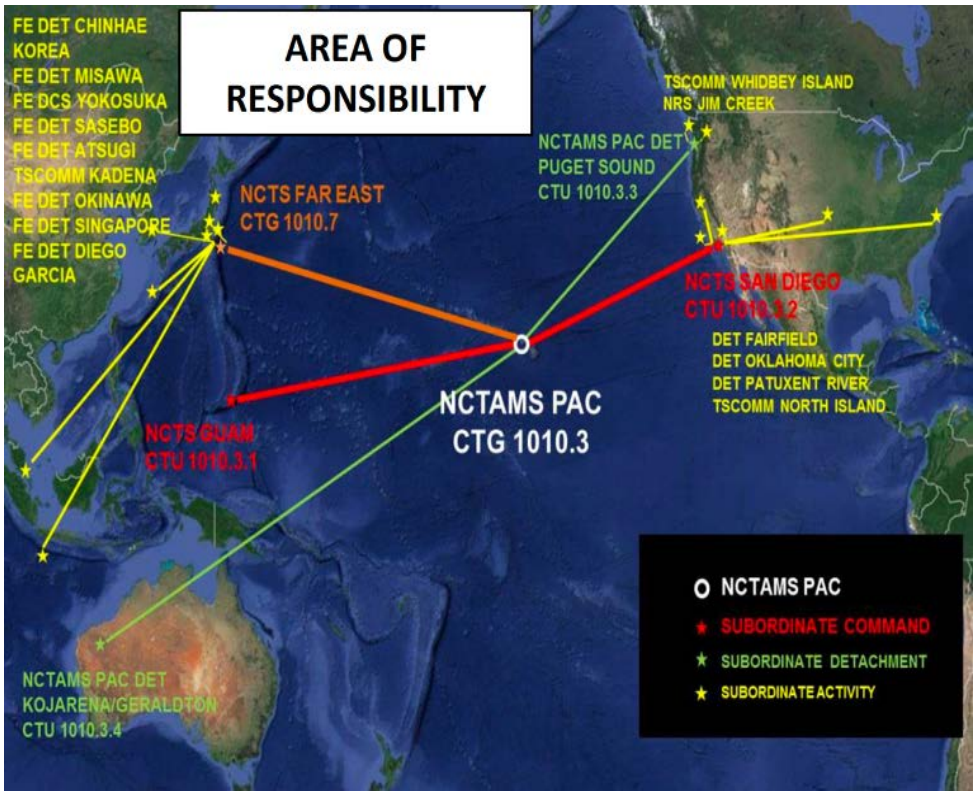

Figure 3. NCTAMS PAC AOR. Source: NCTAMS PAC (2017).

At the time of the site visit, the watch team was split into multiple watch sections with approximately 30 personnel on watch during the day watch rotation. The different sections included the Pacific Message Center, Pacific Region Network Operations Center (PRNOC), Tech Control, Joint Fleet Telecommunications Operations Center (JFTOC), Next Generation Enterprise Network (NGEN), and the Pacific Region Security Operations Center (PRSOC). For the purpose of this research, we will focus on the JFTOC. The JFTOC Watch Officer (WO) is the principal advisor for all things transpiring on the watch floor, and they must be operationally aware of current Navy missions at all times. There is a tangible need for information sharing and real-time network statuses for decision-making and reporting. The JFTOC WO had various applications available that they could use to pull information from, but none of these applications worked in a COP-like manner that was synchronized and populated with real-time information. The closest view the JFTOC WO was able to utilize was the Navy

Cyber Situational Awareness (NCSA) application and even that was not fully populated at the time of our visit. NCSA is only as good as the inputs it receives. They also utilized ENMS but the tickets were input manually and hindered real-time capability. At that time, NCTAMS PAC was also working on a proposal to create a small demonstration network for out-of-band management.

On a second visit, NCTAMS PAC had stood up a Security Operations Center (SOC) on the watch floor for Cyber Defense Operations (CDO). According to the Naval Enterprise Networks, a SOC is a "centralized unit in an organization that deals with organization and technical security issues" (NEN, 2013, p. 114). The SOC focuses on enhancing their personal use of ENMS capabilities such as Afloat SA, Live Action, and Email Queue functions to provide security situational awareness of the many networks and organizations under their purview. From the first visit, they had made substantial progress concerning system discovery, link status information, mail server information, configuration management, and live-action information through ENMS. Information sharing and real-time network status were a large part of their effort to support their DCO and subordinates. A major problem identified at the time, expounded upon in Chapter V, was the lack of simple network management protocol (SNMP) data from all PORs to support a fully integrated COP.

d. Defense Information Systems Agency (DISA) Pacific (PAC)

The Plans and Programs Technical Director of DISA PAC provided a DISA mission brief and NOC tour. DISA has many customers, including Indo-Pacific Command (PACOM) for whom it provides sensor taps to monitor transport services for malicious activity. Many service components rely on DISA transport services.

DISA PAC has partnerships with internet service providers (ISPs) to provide internet access and circuits to the customer. DISA PAC's mission is, according to their public home page is to "provide, operate, and assure command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to the joint Warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations" (DISA, n.d., p.2). The DISA

NOC operational commander is U.S. Cyber Command (USCYBERCOM) via DISA. Because DISA NOC is in the PACOM AOR, it receives various tasking from PACOM which has to be cleared with DISA. This type of relationship creates authority ambiguity among the echelons. In peacetime, PACOM does not have full authority over DISA or some service components. Of course, in wartime PACOM has complete authority. To date, tasking from PACOM, regardless of the threat environment, does not have to be acted upon by DISA NOC until approved by DISA. Despite chain of command (COC) issues, DISA monitors their circuits in real-time and is aware when circuits are down. They have a watch section that is responsible for following up on any outages and gaining an understanding of the full scope of impact. As with most providers, DISA also receives contacts and updates from customers when there are outages.

e. Information Assurance and Cyber Security Program Office (PMW 130)

PMW 130 "plans, manages and executes program resources to ensure continued protection of Navy and joint information, telecommunications and information systems from hostile exploitation and attack" (Vitha, 2018, para 14). PMW 130 is an echelon III command that reports to PEO C4I. PEO C4I reports to NAVWAR.

The site visit to PWM-130 revealed information on the current state of Navy applications and the development of Navy future networks. PMW 130's NCSA and SHARKCAGE are applications that are receiving new and innovative data captures from many different points of Navy Networks. PMW 130 facilitated access to the NCSA Lab, located in San Diego, for a hands-on demonstration and detailed discussions of NCSA and SHARKCAGE. The visit allowed us the ability to become more familiar with programs the Navy is currently utilizing for current and future requirements. NCSA is used by most of the commands we visited. It is used to provide near real-time situational awareness of operations via information sharing between systems and links. The application can analyze multiple different streams of data to present a fully interconnected view for a watch stander or decision-maker. According to the 2018 SPAWAR List, "SHARKCAGE utilizes one-way passive taps in a protected, out-of-band, classified environment, SHARKCAGE consolidates cyber event data from multiple

platforms and networks, providing Navy DCO forces with a shared environment and common platform for integrated workflow, collaboration, and analysis" (SPAWAR, 2018, p. 8). It is the goal of PMW 130 to provide a centralized, thorough, and real-time view of their organization. Many of the commands we visited utilized these applications; further analysis will be conducted in Chapter V and recommendations will be provided in Chapter VI.

B. CIVILIAN INDUSTRY

On-site visits and telephone conversations were conducted with larger civilian organizations within the information technology field such as the NMCI NOC, AT&T, and Amazon, as identified in Table 2. Information provided in this section will detail only information uncovered during the onsite visits or phone conversations.

Table 2. Research Team's Visits (Civilian)

Short Name	Name	Location
NMCI NOC	NMCI Network Operations Center	HI/VA
AT&T	AT&T	NJ
Amazon	Amazon (Telephone)	San Diego

a. Amazon

Amazon is a leading cloud provider. Per a Senior Navy Account Representative, they can provide capabilities across all military classification levels. For this research, we specifically wanted to look at how Amazon was able to accomplish in-house real-time information sharing to support a real-time network status picture. We were unable to get any proprietary details into Amazon's internal procedures/processes and our research concluded without further research into individual services provided by Amazon. Additional research can be conducted into the various solutions that Amazon may be able to provide to the FCC/10F organization.

b. NMCI Network Operations Center (NOC)

NMCI is responsible for an immense amount of information services in use by the FCC/C10F organization. “NMCI provides end-to-end secure Information Technology (IT) services to more than 400,000 seats and 900,000 users, across 2,500+ locations that vary from major bases to single user locations” (Naval Enterprise Networks [NEN], 2013, p. 14). To provide services, NMCI has several NOCs around the world that provides network operations, defense monitoring, and situational awareness. The NOCs are responsible for day-to-day operations, maintenance, remote management, change control, and to respond to network service anomalies in their given AOR (NEN, 2013).

The NMCI NOC is located on Ford Island in Oahu, Hawaii and, is responsible for 24/7 monitoring of network traffic throughout the United States. Overall, it was manned less than NCTAMS PAC and the roles were different in comparison. They have a C2 watch that is 24/7, a customer relationship management area, and a performance management area. On-site processes were ill-defined and/or non-existent which complicated every issue that came in. They did not have a defined rule set to base their response actions on. We were unable to gain much insight into the network infrastructure and how data was passed. Details of watch responsibilities were not available and did not visually appear to be structured. The NOC supports NNWC and NCDOC in network operations and defensive cyberspace operations (DCO). In support of their responsibilities, they utilized the following tools:

- HPE Network Node Manager (NMNi) is a proprietary network status COP. It provides outer/inner router information, Intrusion Prevention System (IPS) information, and some network node monitoring. All the information gathered is put in a COP-like display where it can be sorted and filtered.

- iSPY is a proprietary plugin for NMNi. This tool gives 90-day reports, pulls information from a network by probing with ICMP dropped packets and analyzing round-trip reports.

- HP Service Manager (HPSM) is a proprietary Perspecta ticketing tool which may have some automation built in for alarming on built-in cases. It is updated manually based on information seen in NMNI.

- Enterprise Content Management and Delivery (ECMD) is a proprietary ticket escalation tool that follows static rules, which when alerted, are prioritized by Perspecta to be followed up on. The information for this tool is always 24 hours behind. NNWC BWC has access to view this information via a web interface. This tool can be used for trend analysis.

- Enterprise Navy Management System (ENMS) is a Navy system which Perspecta updates via a web-interface manually when CCIRs get tripped or Service Level Requirements (SLRs) are not met.

c. AT&T

AT&T facilitated a team visit to their Global Network Operations Center (GNOC) located in Bedminister Township, NJ to learn how AT&T's underlying network administration technology functioned to include watch stander employment, processes, and automation which are discussed heavily in the other shared theses.

AT&T's GNOC is a sophisticated command and control center that monitors and manages hundreds of petabytes of global data 24/7 (AT&T, n.d., para. 2). The GNOC is very visual in its display of real-time information. With the many screens displaying information, watch standers can visually see information sharing and make a quick assessment in real-time. As a service provider, they are set up in a proactive posture vice reactive.

AT&T divides its network management into a three-tier system to include Tier I, Tier II, and Tier III. Tier I is the GNOC which is their overarching command and control center to include incident and outage management. They receive inputs from the network that are processed through various algorithms and then presented to the watch stander. Tier II is the advanced technical support located in Georgia. Tier III is the regional component consisting of its network and service application reliability centers. They

receive work requests from the other two tiers and may have multiple Tier II assets under their scope of responsibility. Inputs into the tier system include alarms from physical systems such as IT operations, network service operations, mobility (Radio Access Network), IP backbone, transport, and voice switching.

AT&T utilizes several proprietary software that can retrieve network status information by the GNOC on a timed synchronization. If for some reason the synchronization fails, the system is automatically considered offline and will send out an alert while taking the entire system offline. Equipment failures and other “alarm” type information is analyzed and put through a system that will have an algorithm for developing “alerts.” When a pattern of alarm types triggers an alert type, this is called a “threshold,” and AT&T has identified approximately 150 different threshold criteria which are very similar in intent to C10F/NNWC CCIR criteria.

The ability to visit several different military and civilian organizations provided important insights into the research. It allowed the research team to look at various setups and try to objectively figure out hindrances to information sharing and possible solutions that could positively impact current situations. At the end of the visits, it was evident that the ability to share information effectively in a real-time manner was not possible across the FCC/C10F organization.

V. ANALYSIS

This chapter will detail the analysis of some of the tools and issues that were encountered during the research phase. It will talk about issues within the following three realms: technology, policies, and contracts. This chapter will mainly address issues that impact information sharing in various organizations. Examples will be provided from relevant field observations and are selective, not comprehensive.

A. TECHNOLOGY

In an information technology environment, technologies and their usage can help an organization run more effectively and efficiently. This research included looking at various applications and/or services utilized at various commands within the FCC/C10F organization and how they utilized them. It should be noted that each command used tools differently based on their operational level and mission. At this point in time, no one tool is used across the FCC/C10F organization that can provide real-time information exchange in support of real-time network statuses. This section will discuss some of the key concerns with technology that may limit information sharing including POR reluctance to share data, scalability issues, manning issues, security concerns, slow access to partially useful tools, or being overwhelmed with tools.

1. POR reluctance to share data

The lack of ability for devices to push data to management systems greatly inhibits an organization's capability to effectively share real-time information. During the visit to NCTAMS PAC, NCSA was popular and appeared to be a rather good tool if it was able to be populated effectively. An issue identified included some POR systems not sharing SNMP V3 which would allow assets the ability to share information with ENMS and allow ample data for further analysis. Without SNMP V3, the only information ENMS can receive is "On" or "Off" (Up or Down). The PORs specific reasons for reluctance to share SNMP data is unvalidated but assumed to be contractual, proprietary, or ownership issues. SNMP data allows communication between devices that can be pulled into another application for analysis. The sharing of SNMP data would increase an

organization's ability for information sharing. If NCTAMS PAC or any organization under the FCC/C10F organization were to receive SNMP V3 data from any systems they deemed necessary, they would have the ability to receive and analyze much more data in support of information sharing. Organizations would be able to create a relatively complete, near real-time status picture. SNMP has long been considered an insecure protocol because it is not encrypted. As defined by Coulombre (2013),

> SNMP is based on a model consisting of a manager, an agent, a database of management information, managed objects and the network protocol. The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical device(s) being managed. The information to be accessed is stored in a specified format in the device database, known as a Management Information Base (MIB), used by both the manager and the agent. MIBs contain the parameters to be collected for reporting, captured for notifications or configured by the corresponding management software. (p. 1)

There are many different reasons why an organization would decide to not enable SNMP data on a network. Common concerns include security and bandwidth management. Security is a valid concern; however, that has been addressed in future versions of SNMP. A hash is a value that is produced after running data through a specific algorithm. It allows the ability to see whether or not data has been manipulated. Encryption is a method where the data is essentially encoded. Both hashing and encryption increased security. "Version 3 provides for far better security and privacy through authentication (using MD5 or SHA hash) and DES or AES encryption" (Coulombre, 2013, p. 1). As future versions are created, it is reasonable to assume that the security measures will only increase. As for bandwidth, that is always a tough process to manage. With bandwidth, you start with a given bucket size. It is up to that organization to find a healthy balance and not overfill the bucket because the network and the ability to information share will be impacted negatively. A healthy balance has to be applied thus another reason why some but not all SNMP data is shared on a network.

2. Scalability

A second concern was the scalability of systems or applications being used to monitor or build the information sharing capability within an organization. Sometimes an organization may find itself in the perfect scenario where a tool, system, or software is working flawlessly; however, that quickly changes if the organization were to grow substantially. In these types of cases, an organization and the IT systems it uses must have the ability to grow with them, or their ability to share information will be negatively impacted. PMW 130 research revealed a future scalability issue concerning if they were going to be able to efficiently operate on future networks. If the programs matured any further, they would need a better infrastructure that considered all Navy organizations utilizing the platform and being able to handle the amount of data that would be generated. SHARKCAGE and NCSA are utilized by several organizations. A top concern for SHARKCAGE is that Linux boxes do not support the proper agents to provide the necessary information to various tools. This issue commonly presents itself because of poor design, configuration issues, or limitations of the employed IT system or service. PMW research revealed that a better infrastructure would be required to handle the increasing amount of data generated and analyzed. Without a foundation of anticipating future scalability to support an increase in data generation, tools such as SHARKCAGE and NCSA are at a disadvantage.

3. Manning

With the proper manning an organization can place itself in a posture that allows it to monitor, respond, and resolve in a timely manner increasing their information sharing capability. When an organization is not manned at the proper levels, this can negatively impact its ability to share information. After the visit to NCTAMS PAC, the research team visited the NMCI NOC which appeared to have very low manning in comparison to that of NCTAMS PAC. The level of manning was a concern because it can negatively impact effective real-time information sharing. Without proper manning, an organization may not be able to monitor, respond, and resolve issues for a large AOR, thus, impacting information sharing. This is a repeated issue with the armed forces in

general. To alleviate issues associated with manning, more emphasis can be placed on automation.

4. Security

Security should never be compromised to facilitate information sharing; however, Tanium does exactly that to accomplish the impressive results that it can. Tanium is one of the tools utilized by NNWC. The potential impact on a network utilizing Tanium is significant. If Tanium was ever breached, access to every asset would be successful and information would be compromised. Tanium and HBSS are different means to the same end. Both have the ability for endpoint detection. A user can extract and share information from both of them. However, Tanium is faster. Tanium achieves faster endpoint detection through identifying security compromises and violations of fundamental principles of cybersecurity. It is required to have a static open listening socket. It can be considered a managed botnet. It works fast and to get that speed a compromise in the security posture would have to be made. Tanium has to allow privileged host-to-host communications which are frowned upon. Tanium uses a peer-to-peer protocol and runs in administrative space on each host utilizing a service account. No commands have been compromised as far as our team is aware, but if they ever are, an adversary has immediate quick control of every device on the network. Such an incident would be detrimental to an organization's ability to information sharing among many other things. The vulnerabilities within Tanium are a part of its design and further exacerbated by running it as an in-band tool. As defined by Nevis (2007) p.2),

> The terms in-band and out-of-band generally refer to whether the solution sits in the flow of all network traffic, or out of the flow, analyzing instead only some of the live data streams. It has always been accepted that being in-band can offer better security and greater functionality than an out-of-band approach, but could represent a performance bottleneck or a potential point-of-failure in a mission critical network. (p. 2)

5. Access to Tools

The fifth concern is the ability of an organization to access tools that would increase its ability to information share. NMNi is a commonly requested tool; however, there appear to be some issues with timely account creation with Perspecta, the contractor

responsible for account creations. Account creation can sometimes take months, only to have read-only access and most times, that access is removed inadvertently resulting in the watch stander being required to complete the process from the beginning again. With NMNi, a watch stander would be able to have an understanding of the state of the network through information sharing. Issues surround longer than usual or delayed account creation are due to processes at the approving authority and can be easily fixed if wanted.

Various organizations run into issues when they have too many tools that are all focused on the same goal instead of a few central tools. If an organization has five or more applications/systems that facilitate information to every watch stander, that results in a delay in information sharing or a variety of unnecessary tools in the organizational network. NCDOC from initial research has a very interesting application of how they allowed new tools on their network. This directly impacted one of the contributing problems of having too many tools for efficient operations. They do not allow another vendor or organization to give them a new tool, and they actively try to reduce the amount of unnecessary or outdated tools under their organization through their Cyber Asset Reduction and Security (CARS) program. For an outside vendor to receive an Authority to Operate (ATO), they are requested to provide specified data feeds, Intrusion Prevention Systems (IPS) data, firewall data, and agree to allow an Intrusion Detection System (IDS) on the network with a direct feed to NCDOC. Unless the stated requirements are met, then an ATO is not issued. This requirement tackles two areas of concern. It ensures that an organization is properly managing the tools, and makes sure they do not run into the issue where they are unable to get a complete picture because they do not have access to the data from a vendor or POR.

B. POLICIES AND MANDATES

Policies provide a high-level view and directive on what is allowable on a network. They are integral to information sharing between networks. In the process of ensuring free data flow, security also has to be taken into account for the networks. When looking at policies, the network engineer has to ensure all policies are aligned among the

Network Security Policy, Device Security, Internet Access, VPN, Port Communications, Wireless LAN, Remote Connection, or Firewall Rules. Ensuring well defined and effective policies for thousands of Navy Networks can be time and resource consuming.

Site visits during this research included locations that were heavily involved in Network Operations, some with at least ten different subordinates. During the visits, it was determined that many of the networks did not communicate with each other because of policies. Policies in place hindered information sharing. Some policies denied sharing, some allowed it, and some just lacked the capability. When an organization has a large network, ideally its goal is for all of the pieces to work in harmony and not against each other. The weakest link affects the entire network. If an organization has policies that are not conducive to information sharing throughout the entire organization then information sharing is severely impacted. In most cases, policies are not correctly placed to ensure the free flow/sharing of data.

Navy Networks face many barriers, such as not being able to share information from command to command or POR policies and the ability to share data. To accomplish complete free flow, policies on every level need to be in synchronized to ensure that the information can flow up and down the stack. An environment where all barriers are addressed and thus allowing the sharing of data across various organizations would create a positive environment that fosters information sharing. In the current setup, information sharing is fragmented. Ensuring overarching data sharing policies between PORs, vendors, and organizations to allow complete sharing of information would positively affect an organization's ability to effectively and efficiently share information.

Policies control a significant portion of a network. They can essentially be considered the gatekeeper. They are very complex and can cover several different areas from network operations, security, or privacy. There are various higher policies and guidance that prevent the sharing of information whether it is the responsibility to monitor the network, limit network tool integration, or poor communications with Perspectra and DISA. Policies and guidance prevent understanding of the Network Operational Environment (NOE) for the NOCs and NCTAMs. There is no possibility of

monitoring the environment for health and status without knowledge of the Network Operational Environment.

AT&T is subcontracted by NMCI to provide data transport services to DISA. Because of this, AT&T has tools with the ability to write scripts and find information that Perspecta does not have access to or does not have an SLA to utilize. An example of a policy issue was evident when a technician informed NMCI of an issue via the NMCI helpdesk hotline, their only means for network interface or management. The findings were not elevated by NMCI despite the technician's position as a government employee hired to troubleshoot those exact issues. The issue went unresolved for months until the technician put in enough tickets for the issue to be elevated to the appropriate level for correction. NMCI finally corrected the issue, although the operational impact to the network was already apparent. These actions demonstrate the policy issues where Perspecta is in a reactive state rather than a proactive state, despite the multiple tickets and phone calls on the part of the technician trying to be proactive.

This case illustrates the "unwritten" procedures for how NCMI escalates its issues. It shows that despite position, expertise, and insight on a customer's part, the policy agreements in place are what Perspecta is bound to follow. Given the process by which Perspecta escalates issues, the network is forced to operate in a reactive state, if not in a broken state, where their network operations staff cannot affect much change in the network/system management without running through an unreliable problem stove-piped system. This process affects information sharing on the network.

C. CONTRACTING

Contracts have historically been a major issue for the Navy. Either the contract and SLAs are too broad or nonexistent to support organizational goals. IT contracts can be a government operated (GO) or a contractor operated (CO) network. The Navy is currently on the Navy-Marine Corps Intranet which is government owned, but contractor operated. The Marine Corps went a different route with the Marine Corps Enterprise Network (MCEN) which is government owned and government operated. The difference between CO and GO are evident in how both services can manage their networks. On the

Navy side, it is very costly and time-intensive for us to do anything to be done on the network, whereas, the Marine Corps can make changes in a much shorter time frame because they own and operate their network. The ability for timely changes in network operations is imperative for information sharing, security, and near real-time situational awareness.

The ability to create and maintain a global enterprise health and status network could be greatly improved by improving the communications and coordination between the acquisition and the IT community. It is imperative that what an organization need is translated properly into a contractual agreement. It has to be a team effort with the correct people in the decision-making chain of approval. The end state should be the culmination of the enterprise goals, including constraints and expectations. For example, one of the U.S. Navy's most recent IT acquisition is the Consolidated Afloat Networks and Enterprise Services (CANES) which according to their fact sheet, is the "Navy's next-generation tactical afloat network. CANES represents the consolidation and enhancement of five shipboard legacy network programs to provide the common computing environment for more than 40 command, control, intelligence, and logistics applications" (SPAWAR, 2011, para. 1). One prime example of something particular to CANES that could have been better addressed in the contract was its ability for the system to be rebooted. In a CANES environment, it takes in practice, about two hours to reboot the system, and while the system is rebooting, access to the multiple integrated systems is lost. This is a big problem for a warship in a contested environment. This example is only to show the disparity between what is needed and what is delivered.

Contract issues can be easily fixed by ensuring key players in the IT field are at the negotiating table, details of SLAs are clearly defined, and each organization is aware of their responsibilities within the contract.

D. SUMMARY OF RESEARCH FINDINGS

This section will summarize the research findings. A variety of tools were discussed. Most tools have a very specific purpose and are able to meet one or two uses; however, overall there is no centralized tool that promotes information sharing and is able

to effectively use it for a real-time picture. Information technologies that negatively affect FCC/C10F's ability to share and receive timely information across the organization include:

1) PORs not enabling SNMP V3 protocol on their systems to allow communication of health and status information. The disabling of SNMP V3 protocols by PORs prevents systems from communicating health and status information in near real-time. The lack of system communication complicates near real-time analysis of the health and status information. This lack of communication negatively affects the sharing of timely information across the organization. Exploring how to share this data with minimal impact could positively impact information sharing.

2) Organizations not placing a heavy emphasis on scalability. Various applications may be great for the current environment; however, future growth and expectations of the system/application can impact information sharing as the system/application may become less effective as the organization grows. Ensuring that scalability concerns are addressed in planning phases and/or before any contracts would positively impact information sharing.

3) Tools, such as NMNi account access, are broken. Ensuring a flowing account creation process could positively impact an organization's ability to share information by ensuring the proper access is given promptly.

4) Security is vital in information sharing. Applications such as Tanium pose security risks that could negatively impact information sharing. Prioritizing security and the impact to an organizations ability to share information would positively impact information sharing

5) A frequent concern was the number of tools for use by a watch stander. Being overwhelmed by tools in a stressful environment delays information sharing. Minimizing the number of applications/tools for use would positively impact information sharing.

Manning directly impacts an organization's ability for effective information sharing. This is a long-standing issue for many organizations. Changes in manning or decreasing the number of interactions that require human interaction would positively impact information sharing.

Policies within the FCC/C10F organization are vast and complex. This research did not go into detail on specific policies but instead took a broad approach to the issues that policies create. There are policies in place for internal and external processes, security, and need to know, just to name a few areas. When the policies of an organization do not align for all internal and external entities, the ability to share information is greatly impacted. Changes in these areas would positively impact the organization's ability to share information.

The FCC/C10F organization has a variety of support mechanisms in addition to active duty personnel. Contracts are frequent. If a specific contract does not cover the details to ensure an organization is receiving the support and data necessary to maintain its ability to share information, then it will be in an undesirable position. The Cyber Asset Reduction and Security (CARS) program is an excellent program and provides help in ensuring that civilian contracts are providing the correct support before issuing an ATO.

VI. CONCLUSION

Organizations within FCC/C10F remain unable to utilize information sharing to compile an integrated enterprise network status information. At each command, a common concern is the sharing of information in real-time. This research examined the roles of tools and applications, policies, and contracting agreements in preventing and enabling information sharing.

In the effort to pursue real-time information sharing to support a real-time network picture, commands find themselves inundated with various tools and applications. Many organizations touched on the fact that they had too many tools to log into to investigate issues, which proved to be very cumbersome on an operational watch floor. The Navy communications environment is very complex with a large number of assets spanning various security enclaves and areas of responsibility of the overall network. This complicates the objective. This research revealed that most tools are incomplete in that they can provide real-time information sharing about some data but not all data. Additionally, various POR systems and tools do not fully share information with other systems to allow effective and efficient information sharing.

Lack of interoperability and isolated capabilities contribute greatly to an organization being unable to share information in real-time. As evident in each of the on-site visits, tool usage can vary between each organization. Lack of interoperability has a negative impact due to multiple installations utilized by the DOD, such as SHIPMAN and Navy C5I, FRCB, sub-process, and embarked process, among others. Having so many different ways of installation, there is a lack of the centralized control needed to ensure that all these systems, if necessary, can exchange data with each other. This is the same issue with multiple PORs. Individually, they each have responsibilities, however, within each, they have their own tools, numerous data centers, differing levels of ownership, and ADCON/OPCON/MTE issues.

How an organization is structured plays a huge role in how real-time information can be shared throughout it. A large hindrance to real-time information sharing is stove-

piped network architectures and developments. The DOD has thousands of systems created by different organizations, contracted out to third parties, or applications that are no longer supported but are still being used by organizations. The same approaches recommended for FCC/C10F need to be applied externally to the FCC/C10F organization to support global real-time information sharing across various enclaves.

A. RECOMMENDATIONS

This research looked at various military and civilian organizations and the issues that impacted real-time information sharing and how positive changes could impact the FCC/C10F organization's ability for information sharing. To move towards efficient and effective information sharing to facilitate an integrated COP of network health and status, many changes need to be made.

The organizational and network architecture both need to be able to facilitate real-time information sharing. Policies across the fleet should support and not restrict information sharing due to organizations being dependent on one another for optimal performance and achieving mission objectives.

It was very evident that some of the issues plaguing real-time information sharing included old, antiquated systems. This is addressed by transitioning from legacy systems to IP to provide real-time data to NETOPS systems via information sharing. This research supports the recommendation that the reduction of old legacy systems allows the organization to utilize newer systems with newer capability geared toward better information sharing.

Additionally, the approach to how we deploy technology should be revisited. When deploying technologies for such a large organization, a system of systems approach that takes into consideration the current and future environments as well as the consequences of such changes over time should be of priority.

Information sharing currently requires system administrator privileges. On the current network, that is government owned (GO) and contractor operated (CO), commands such as NNWC may have to insert themselves more regarding network

administration, as they own the process. In reviewing the information available, it appears that the Navy organization has more flexibility to do things within the current NGEN contract. The lines of responsibility and confines should be clearly drawn and understood by all entities. GO includes the network, hardware, and administration. It should be administered via appropriate lines of communication. CO should be operated under dictated constraints. Future government contracts should require the ability for organizations to have the option to self-monitor their networks. More often than not, organizations have found themselves restricted in information sharing because they do not have access to monitor their network and data.

A final recommendation is that applications requiring compromises to security postures be managed in an out-of-band capacity. Placing an otherwise great application like Tanium as far out-of-band as possible could open up additional possibilities of the application with lesser security implications to a vital organization.

In conclusion, global information sharing is possible on a GO/CO network. The risk has to be taken and accepted. The Navy cyber team is highly intelligent and capable and with the right tools and directions, we can share information globally to and from the entire FCC/C10F organization.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

AT&T. (n.d.). *AT&T corporate briefing center*. Retrieved January 7, 2020, from https://www.business.att.com/about/att-corporate-briefing-center.html

Chen, D. (2006, June). Enterprise interoperability framework. [Paper Presentation]. Open Interop Workshop on Enterprise Modeling and Ontologies for Interoperability, Luxembourg. https://dblp.org/rec/conf/caise/DaclinCV06

Chief of Naval Operations. (2018). *A design for maintaining maritime superiority*. http://www.navy.mil/navydata/people/cno/Richardon/Resource/Design_2.0.pdf

Coulombe, R. (2013, September). SNMP primer. *Security Technology Executive*, *23*, 10. http://libproxy.nps.edu/login?url=https://search-proquest-com.libproxy.nps.edu/docview/1462788993?accountid=12702

Department of Defense. (2013a, Aug 5). Sharing data, information, and information technology (IT) services in the Department of Defense (DoDI 8320.02). https://fas.org/irp/doddir/dod/i8320_02.pdf

Department of Defense. (2013b, Sept 18). *Strategy for implementing the joint information environment.* https://dodcio.defense.gov/Portals/0/Documents/JIE/2013-09-13_DOD_Strategy_for_Implmenting_JIE_(NDAA_931)_Final_Document.pdf

DISA. (2018). *DISA's mission assurance branch ensures readiness, lethality across all warfighting domains*. https://www.disa.mil/NewsandEvents/2018/Mission-Assurance-Branch-warfighting-domains

Dombrowski, Peter J., and Ross, Andrew L. (2003) "Transforming the Navy," *Naval War College Review 56*(3) Article 6. https://digital-commons.usnwc.edu/nwc-review/vol56/iss3/6

FCC/C10F. (2015). *Strategic plan 2015–2020*. https://www.public.navy.mil/fcc-c10f/Documents/FCC-C10F_Strategic_Plan_2015-202.pdf

FCC/C10F. (n.d.-a) U.S. Fleet Cyber Command / U.S. Tenth Fleet. Retrieved March 30, 2020. https://www.public.navy.mil/fcc-c10f/Pages/home.aspx

FCC/C10F. (n.d.-b) U.S. Fleet Cyber Command / U.S. Tenth Fleet. Retrieved March 30, 2020. https://www.public.navy.mil/fcc-c10f/Pages/usfleetcybermission.aspx

Fischer,E., & Logan, S. (2015). *Cybersecurity and information sharing: Comparison of H.R. 1560 and H.R. 1731 as passed by the House*. Library of Congress. Congressional Research Service.

Leedom, D. K. (2019, May 31). *Next generation common operating picture*. [Presentation]. 8th International Command and Control Research and Technology Symposium, Washington, DC, United States. http://www.dodccrp.org: http://www.dodccrp.org/events/8th_ICCRTS/Pres/track_4/3_1330leedom.pdf

Naval Enterprise Networks. (2007, June 27). *Next generation enterprise network program performance work statement.* file:///Users/evacastillo/Downloads/attch01performanceworkstatementn00039-13-d-0013.pdf

NCTAMS PAC. (n.d.). *Information about us.* https://www.public.navy.mil/fltfor/nctamspac/Pages/AboutUs.aspx

NCTAMS PAC. (2017). *Consolidated platform card.* [Handbook].

NETWARCOM. (n.d.-a). *Decision superiority for the warfighter home.* https://www.public.navy.mil/fltfor/nnwc/Pages/default.aspx

NETWARCOM. (n.d.-b). *Command history.* https://www.public.navy.mil/fltfor/nnwc/Pages/default.aspx

Nevis Networks. (2007). *An architectural view of LAN security: In-Band versus Out-of-Band Solutions* [Working paper]. Nevis Networks. https://www.nevisnetworks.com/content/white_papers/In-band%20vs%20Out-of-band.pdf

Office of the Deputy Chief of Naval Operations for Information Dominance (OPNAV NS/N6). (2012, December). The Joint Information Environment. *CHIPS, October-December 2012.* https://www.doncio.navy.mil/Panetto, H. & Cecil, J. (2013). Information systems for enterprise integration, interoperability and network: Theory and applications. *Enterprise Information Systems* (7): 1–6. http://doi.org/10.1080/17517575.2012.684802

Panaro, C. (2010, May 22). Software as a service. https://www.doncio.navy.mil/ContentView.aspx?id=1747

SPAWAR. (2018). *The SPAWAR list.* [Handbook]. https://www.public.navy.mil/navwar/Documents/List.pdf

SPAWAR. (2015). SPAWAR commander releases strategic vision for leading the Navy in cyber warfighting. Navy. http://navy.mil/submit/display.asp?story_id=86447

SPAWAR. (2011). *Consolidated afloat networks and enterprise service (CANES)* [Fact Sheet]. http://secnav.navy.mil/rda/Documents/canes+overview+for+asn+rda+11-2-11-s.pdf

Tanium. (2020). *Driving IT hygiene with tanium solution brief.* [Brief]. https://www.tanium.com/it-hygiene.

White House. (2018). National cyber strategy of the United States of America. Washington, DC. http://whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Vitha, J. (2018, March 22). PEO C4I program offices host fleet stakeholders working group summit. Navy. https://www.navy.mil/submit/display.asp?story_id=104773

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