NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SHOULD THE U.S. NAVY ADOPT A TRUE MULTI-LEVEL SECURITY ENVIRONMENT?

by

Ashley M. Mannix

June 2020

Thesis Advisor:	Dan C. Boger
Co-Advisor:	Sue L. Higgins
Second Reader:	Scot A. Miller

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

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

4. TITLE AND SUBTITLE SHOULD THE U.S. NAVY ADOPT A TRUE MULTI-LEVEL SECURITY ENVIRONMENT?	5. FUNDING NUMBERS RFN1W
6. AUTHOR(S) Ashley M. Mannix	
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) NAVWAR San Diego, CA 92110	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)

While the Department of Defense experiments with initiatives that move toward a more seamless and integrated repository of data through cloud computing, it is essential to consider the most effective technologies that will provide Commanders with the tools necessary to make timely decisions, yet at the same time not cause unnecessary risk and sacrifice to national security. This thesis outlines the advantages and disadvantages of the Navy adopting variations of Multi-Level Security (MLS) architectures in comparison to its current Cross Domain Solutions (CDS) architectures. This thesis also analyzes current CDS policies to determine needed improvements that account for emerging CDS technology.

14. SUBJECT TERMS Multi-Level Security, MLS, Cross Domain Solutions, CDS, All-Domain Operations, MDC2, Joint All-Domain Command and Control, JADC2	15. NUMBER OF PAGES 113
	16. PRICE CODE

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

NSN 7540-01-280-5500

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

SHOULD THE U.S. NAVY ADOPT A TRUE MULTI-LEVEL SECURITY ENVIRONMENT?

Ashley M. Mannix
Lieutenant, United States Navy
BS, U.S. Naval Academy, 2013

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
June 2020

Approved by: Dan C. Boger
Advisor

Sue L. Higgins
Co-Advisor

Scot A. Miller
Second Reader

Thomas J. Housel
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

While the Department of Defense experiments with initiatives that move toward a more seamless and integrated repository of data through cloud computing, it is essential to consider the most effective technologies that will provide Commanders with the tools necessary to make timely decisions, yet at the same time not cause unnecessary risk and sacrifice to national security. This thesis outlines the advantages and disadvantages of the Navy adopting variations of Multi-Level Security (MLS) architectures in comparison to its current Cross Domain Solutions (CDS) architectures. This thesis also analyzes current CDS policies to determine needed improvements that account for emerging CDS technology.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
- A. METHODOLOGY....2
- B. RESEARCH QUESTIONS....3
- C. THESIS OVERVIEW....3

II. LITERATURE REVIEW AND BACKGROUND....5
- A. BELL-LAPADULA MODEL....5
- B. OTHER MULTI-LEVEL SECURITY RESEARCH....6
  - 1. 1970s MLS Research....6
  - 2. 1980s-1990s MLS Research....6
  - 3. 2000s MLS Research....7
  - 4. Further MLS Research....8
- C. CONCLUSION....8

III. MULTI-LEVEL SECURITY TECHNOLOGY, ASSESSMENT, AND AUTHORIZATION....11
- A. MULTI-LEVEL SECURITY AND CROSS DOMAIN SOLUTIONS....11
  - 1. Multi-Level CDS....13
  - 2. MLS Considerations....15
- B. CDS ASSESSMENT AND AUTHORIZATION PROCESS OVERVIEW....19
  - 1. GENSER CDS Approval Process....19
  - 2. SCI and SAP Systems....21
- C. DOD AND INTELLIGENCE COMMUNITY'S CDS POLICIES....22
- D. CONCLUSION....25

IV. DIGITAL TRANSFORMATION IN THE NAVY....27
- A. STRATEGIES....27
- B. DOD DIGITAL TRANSFORMATION....28
  - 1. Cloud Strategy....30
  - 2. Artificial Intelligence Strategy....31
- C. MULTI-LEVEL SECURITY IN ALL-DOMAIN OPERATIONS....32

V. ORGANIZATIONAL ISSUES....33
- A. STRATEGY....33
- B. TASKS, PRACTICES, AND TECHNOLOGY....36

C. STRUCTURE 38
1. Roles and Responsibilities 39
2. The Function of Standards Organizations 41
3. Reciprocity 46
4. Collaboration across the DoD 47
D. TRAINING AND EDUCATION 48
E. REWARD SYSTEMS AND INCENTIVES 50
F. CONCLUSIONS 50

VI. CONCLUSIONS, RECOMMENDATIONS, FUTURE WORK 53
A. PROCESS IMPROVEMENT RECOMMENDATIONS 54
1. Add DoD Component "Fast Track" Options to CDS RMF Process 54
2. Consolidate MLS Efforts via JADC2 Process and Wargames 55
3. Investigate Potential Consolidation to a Single AO for Programs that Span Multiple AOs 55
B. RECOMMENDATIONS FOR FUTURE RESEARCH 56
1. Determination of Most Pertinent Label-Aware, Web-Based Applications 56
2. Design a Test to Determine if a True MLS Environment Increases the Speed of the Commander's Decision-Making 56
3. Cost Analysis of the Value Added from an MLS Environment 57

APPENDIX A. RAISE THE BAR STANDARD 59

APPENDIX B. CDS APPROVAL PROCESS IN COMPARISON TO THE ISO PROCESS 61
A. STANDARDS DEVELOPMENT WITHIN THE PRIVATE SECTOR 61
1. International Organization for Standardization (ISO) Structure and Governance 61
2. ISO International Standards Approval Timeline 64
3. ISO Certification and Accreditation Authorities 66
4. ISO representation from the United States 66
B. STANDARDS DEVELOPMENT WITHIN THE DOD 67
1. DoD Executive Agent for IT Standards 68
2. DoD Information Technology Standards Registry (DISR) 68

C. IMPORTANT DOCUMENTS THAT GOVERN CDS REQUIREMENTS 69
1. Cross Domain Policy: DoDI 8540.01 69
2. Risk Management Framework (RMF) for DoD Information Technology (IT): DoDI 8510.01 69
3. Cybersecurity: DoDI 8500.01 70
4. The Defense Counterintelligence and Security Agency (DSCA) Assessment and Authorization Process Manual (DAAPM) 70
5. Executive Order Number 12333, as amended 70
6. Intelligence Community Directive (ICD) Number 503 71
7. Defense Information Systems Network (DISN) Connection Process Guide (CPG) 72
D. MAJOR STANDARDS BODIES AND ENTITIES INVOLVED IN THE RMF PROCESS 72

SUPPLEMENTAL. JOINT ALL DOMAIN COMMAND AND CONTROL CROSS FUNCTIONAL TEAM (JADC2 CFT) ESTABLISHMENT 75

LIST OF REFERENCES 77

INITIAL DISTRIBUTION LIST 89

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Types of Cross Domain Solutions Based on Functionality. Adapted from CDS Design and Implementation Requirements. Source: National Cross Domain Strategy and Management Office (2020). 12

Figure 2. MLS Track Management View. Source: SPAWAR (2016). 14

Figure 3. Traditional CDS Architecture with Data Guards. Adapted from Reed (2004). 16

Figure 4. Traditional CDS vs MLS Architectures. Source: Raytheon (2007). 18

Figure 5. DoD CD and RMF Process. Source: DoD Chief Information Officer (2017). 20

Figure 6. DoD CDS Connection Process Diagram. Source: Defense Information Systems Agency (2016). 21

Figure 7. Emergent Technology Strategies. Source: Norquist (2019). 29

Figure 8. Strategy and Goals. Adapted from Jansen, Gallenson, and Higgins (2015). 34

Figure 9. Tasks, Practices, Technology. Adapted from Jansen, Gallenson, and Higgins (2015). 36

Figure 10. Structure Design Factor. Adapted from Jansen, Gallenson, and Higgins (2015). 39

Figure 11. ISO Standards Routing Process. Source: International Organization for Standardization (2020). 43

Figure 12. Training and Education Design Factor. Adapted from Jansen, Gallenson, and Higgins (2020). 49

Figure 13. Reward Systems and Incentives Design Factor. Adapted from Jansen, Gallenson, and Higgins (2020).....50

Figure 14. ISO Governance Structure. Source: International Organization for Standardization (2020c). 63

Figure 15. ISO Standards Routing Process. Source: International Organization for Standardization (2020a). 64

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. RTB Requirements Baseline Release Timeline. Source: National Cross Domain Strategy and Management Office (2020).....25

Table 2. DoD Standards Consideration. Source: DoD Chief Information Officer (2017). 44

Table 3. RTB CDS Deployment Increments and Implementation. Source: National Cross Domain Strategy and Management Office (2020).....60

Table 4. DoD Standards Consideration. Source: DoD Chief Information Officer (2017b). 67

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

A&A	assessment and authorization
ABMS	advanced battle management system
AFRL	Air Force Research Laboratory
AI	artificial intelligence
AIC	Atlantic intelligence center
ANS	American National Standard
ANSI	American National Standards Institute
AO	authorizing official
AOR	area of responsibility
ATO	authority to operate
BICES	battlefield information collection and exploitation system
C&A	certification and accreditation
C2	command and control
C4I	command, control, communications, computers, and intelligence
CASCO	Committee on Conformity Assessment
CENTRIXS	combined enterprise regional information exchange system
CD	cross domain
CDA	cross domain appendix
CDM	concepts development and management
CDS	cross domain solution
CDSE	cross domain support element
CDTAB	cross domain technical advisory board
CFT	cross functional team
CIA	confidentiality, integrity, and availability
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CNSS	Committee on National Security Systems
ConMon	continuous monitoring
CPG	connection process guide
CSS	central security service

CVNIT	carrier vessel nuclear information technology
DAAPM	Defense Counterintelligence and Security Agency Assessment and Authorization Process Manual
DBS	defense business systems
DCMO	deputy chief management office
DIA	Defense Intelligence Agency
DIL	disconnected, intermittent, low-bandwidth
DISA	Defense Information Systems Agency
DISN	defense information systems network
DISR	defense information technology standards registry
DNI	Director of National Intelligence
DNI CIO	Director of National Intelligence Chief Information Officer
DoD	Department of Defense
DoDD	Department of Defense directive
DoD CIO	Department of Defense Chief Information Officer
DoDI	Department of Defense instruction
DRM	digital rights management
DS	Doolittle series
DSAWG	Defense Information Assurance (IA)/Security Accreditation Working Group
DSCA	Defense Counterintelligence and Security Agency
EA	executive agent
ECDSP	enterprise cross domain service provider
ExSC	Executive Standards Council
FAO	functional authorizing official
FDIS	final draft international standard
FLTCYBERCOM	Fleet Cyber Command
GENSER	general service
GEOINT	geospatial intelligence
GPC	great power competition
HTN	high threat network
IA	information assurance
IAF	international accreditation forum

IC	intelligence community
ICD	intelligence community directive
ICT	information and communication technology
IP	internet protocol
IS	information systems
ISE	information sharing environment
ISRMC	information risk management committee
ISSE	information system security engineer
ISO	international organization for standardization
ISP	information support plans
IT	information technology
ITU	international telecommunication union
ITSAG	information technology strategy advisory group
J-DET	joint intelligence center-Pacific detachment
JAC	joint analysis center
JADC2	joint all domain command and control
JCDX	joint cross domain exchange
JEDI	joint enterprise defense infrastructure
JIPAC	joint intelligence center-Pacific
JROC	Joint Requirements Oversight Council
JS	joint staff
JSCS WG	joint special access program cybersecurity working group
JSIG	joint special access program implementation guide
JTC	Joint Technical Committee
JWICS	joint worldwide intelligence communications system
LTBP	long-term business plan
MAC	mandatory access control
MDC2	multi-domain command and control
MDO	multi-domain operations
MLS	multi-level security
ML Chat	multi-level chat
ML Web	multi-level web
MOU	memorandum of understanding

NAO	Navy authorizing official
NAVAIRSYSCOM	Naval Air Systems Command
NAVFACENGCOM	Naval Facilities Engineering Command
NAVSEASYSCOM	Naval Sea Systems Command
NAVWARSYSCOM	Naval Warfare Systems Command
NCDSMO	national cross domain services management office
NDS	National Defense Strategy
NIA	National Intelligence Agency
NIPRNet	non-secure internet protocol router network
NISP	national industrial security program
NP	new work item proposal
NRL	naval research laboratory
NSA	National Security Agency
NSI	national security information
NSS	National Security Systems
NTC	naval tactical cloud
ODAA	operational designated accrediting authority
OS	operating system
OSD	Office of the Secretary of Defense
ODNI	Office of the Director of National Security
PAO	principal authorizing official
PAS	publicly available specifications
PMW	program management warfare
POA&M	plan of actions and milestones
POR	program of record
RAR	risk assessment report
RMF	risk management framework
RTB	raise the bar
SABI	secret and below interoperability
SAF	Secretary of the Air Force
SAP	Special Access Program
SAPCO	special access program central office
SAR	security assessment report

SC	subcommittee
SCA	security control assessor
SCI	Sensitive Compartmented Information
SDO	standards development organization
SELinux	security-enhanced Linux
SIGINT	signals intelligence
SIPRNet	secure internet protocol router network
SISO	senior information security officer
SP	security plan
SSAA	system security authorization agreement
SSP	system security plan
SWAPC	size, weight, power, and cooling
TA	technical authority
TAG	technical advisory group
TC	technical committee
TCML	tactical cloud multi-level
TMB	technical management board
TS	top secret
TSABI	top secret and below interoperability
UK	United Kingdom
USAF	United States Air Force
USD(I)	Under Secretary of Defense for Intelligence
USG	U.S. government
VM	virtual machine
USAF	United States Air Force
USN	United States Navy
USSTRATCOM	United States Strategic Command
VCJCS	Vice Chairman of the Joint Chiefs of Staff
W3C	Worldwide Web Consortium
WSC	world standards cooperation

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

To my mom: A woman whose depth knows no bounds, whose classiness is inspirational, and whose passion for education increases with age! The radiance in your eyes, the "sunshine" that envelopes you, and the way you live your life clearly speak volumes to everyone. You are the wind beneath my wings, my life coach, closest confidant, and greatest encouragement!

There are so many examples of your impact on my life, but here is one example that I remember just like it was yesterday: it was a weekday afternoon and I wrapped my small arms around the white staircase spindle with the tightest grip, and the most dead-weight that my 60-pound frame could muster. I screamed, "No, Mom, I can't do this! I don't want to go," at which point, your 5′1″ frame pointedly pulled me off the staircase, tossed me over your shoulder, carried me into the garage, and placed me into what would later be coined the "soccer and Girl Scouts mom" van. It was my first gymnastics lesson and I was too nervous and unconfident to even think about trying something new in front of people I did not know.

This physical illustration is a metaphorical word picture of what you did for me in every aspect of my life. You know me best—and you played the critical role as my strong mentor, committed encourager, and dedicated life coach. You instilled me with a deep desire for achievement and learning at a very young age. You taught me how to read by the time I was four years old and you homeschooled me until I entered the 2nd grade—all while you worked as an RDAEF.

You embody the definition of a trailblazer—you were the first person in your entire family to graduate high school. Then, you earned your bachelor's degree in psychology with a minor in Bible and Christian counseling. You accomplished all of these things in spite of the adverse circumstances in which you were raised. I witnessed you study all night long for your dental and college courses, and you instilled the deepest passion in me for learning and mental toughness. You led by example and never let me quit anything. Thank you for demonstrating what a God-fearing woman of faith, mother, and wife look like, and

for your steady and faithful prayers that laid the foundation for our entire family. You were able to pull me off my proverbial "staircases" in life because you followed the Lord and had the tenacity to follow the path less traveled in your own life.

You are my and Dad's "General." You modeled both a strong confidence and command presence in every area; both of which are attributes that you strategically taught us to exude. We later would need to rely on these attributes to succeed as Officers, and in life. Without you, we both would not be *who* we are, or *where* we are at today. Your strong leadership qualities and overcoming in your life is what brought us to where we are today. You have been, and you *are* the wind beneath our wings.

To my dad: Thank you for your demonstration of a hard work ethic, and for your great example of faith and character. My inspiration to join the military began with your service in the Army. You began to take college courses when I was in the fourth grade with aspirations to earn your commission as an Army Chaplain. As a Sergeant First Class Chaplain's Assistant in the Army, you were my first salute upon commissioning. Following my commissioning, you were the first person in your family to earn a master's degree—which consisted of courses that you took simultaneous to your full-time job. After that, you accomplished your goal to commission as an Army Chaplain, and you promoted to O-3 one month before I promoted to O-3. I saluted you upon my promotion to O-3, and now we both continue the race to O-4. Thank you for demonstrating what a God-fearing father looks like, and for your steady love, encouragement, and advice to us! It is such an inspiration to see you walking in God's calling as an incredible Army Chaplain to Army Soldiers who respect and follow you anywhere—in addition to your ability to teach, serve, counsel, and encourage Veterans at the Veterans Administration Hospital.

To my research sponsor, Battlespace Awareness and Information Operations Program Office (PMW 120), thesis advisor, Dr. Dan Boger, co-advisor, CDR (Ret) Sue Higgins, and second reader, CAPT (Ret) Scot Miller—thank you for your dedication and guidance throughout this process.

I. INTRODUCTION

> The Department of Defense does not have an innovation problem; it has an innovation *adoption* problem.
>
> —Eric Schmidt, testimony to Congress, 17 April 2018

Naval leaders call for agility and innovation to prepare for and win the next war. As the world is being transformed by artificial intelligence (AI), cloud computing, and data analytics, the military faces new threats and new opportunities. The confluence of these technologies promises that military leaders will make decisions with greater speed and accuracy, helping to reduce the fog of war.

As the Department of Defense (DoD) experiments with initiatives that move towards a more seamless and integrated repository of data storage via cloud computing initiatives, it is essential to consider the most effective technologies that will provide Commanders with the tools they need to make timely decisions, yet at the same time not cause unnecessary risk and sacrifice national security.

Emergent technology shapes policies across the DoD. The Federal, DoD, and Navy cloud strategies, as well as data and artificial intelligence (AI) strategies are new in the last 12–18 months (Cyber Security and Information Systems Information Analysis Center, 2020, p. 1). As the data generated from these emergent technologies is stored on the cloud, CDSs (including MLS), will need to be employed to access and/or transfer data between security domains with varying classification levels.

An MLS system would allow the use of a single computer to access varying security domains and transfer data between those domains, based on users' security clearances and need to know. Data would be labeled appropriately to preclude breaches of security between security domains. Interest in MLS has increased as computing processing, data storage, and computer memory has increased, making Big Data available now to the operators.

This thesis views the adoption of technology, specifically MLS, through three lenses. A *contextual* lens considers how MLS can integrate into a digitally transformed Navy. A second lens looks at *technical* development. Through an *organizational* lens, the thesis explores what institutional change is needed to sustain adoption. The approach provides a broad framework for leaders who consider adopting any new technology.

A. METHODOLOGY

The methodology used was exploratory and qualitative. The researcher reviewed literature and policies. Conversations were held with subject matter experts in person and electronically. To address the pros and cons of adopting MLS technology the researcher explored ways in which MLS technology is used in other Services and where the Navy could leverage MLS technology better than it currently does, such as mission sets that require size, weight, power, and cooling (SWAPC) considerations. The research considered requirements for developing this technology and explored practical steps needed to implement MLS technology. The policies applicable to this topic were analyzed. Additionally, it considered whether current policies and requirements regarding MLS are sufficient to address the Navy's growing repository of data and the increasing speed of technology advancement.

Prior to reaching out to subject matter experts (SMEs) regarding CDS and MLS, working definitions of relevant terms were outlined using the Committee on National Security Systems' (CNSS) definitions. Once those definitions were established, exploratory qualitative analysis was used to conduct research on MLS and current CDS policies, as well as to visit and talk to subject matter experts (SMEs) from the Defense Information Assurance (IA)/Security Accreditation Working Group (DSAWG), National Security Agency (NSA), NAVWARSYSCOM, Air Force Research Laboratory (AFRL), and others.

B. RESEARCH QUESTIONS

Primary:

1. Should the Navy adopt more Multi-Level Security (MLS) environments in comparison to other Cross Domain Solution (CDS) architectures that are more widely implemented today in the Navy?

Subsidiary:

2. Is an MLS environment a higher risk than the current CDSs in operation?

3. Are the current CDS and MLS policies sufficient or problematic?

4. Are there MLS solutions that other branches of the military have successfully implemented?

5. If so, are there particular Navy mission sets that would be similarly suited for an MLS environment?

6. Are current policies or a cultural mindset keeping the Navy from adopting an MLS environment?

C. THESIS OVERVIEW

- Chapter I: Introduction.

- Chapter II: Literature Review and Background. This section provides a background of Multi-Level security development and implementation.

- Chapter III: MLS Technology, Assessment and Authorization. This section discusses the three different types of cross domain solutions, with a specific focus on MLS. It also provides an overview of the CDS approval process.

- Chapter IV: Digital Transformation. This section discusses Navy and DoD emergent technology strategies that support the National Defense Strategy, and how MLS is leveraged to support these technologies.

- Chapter V: Organizational Issues Related to the Adoption of New Technology. This section applies an adaptation of the Galbraith Star Model™ to determine how well CDS technology (such as MLS) are integrated and aligned with cultural practices within the DoD.
- Chapter VI: Conclusions, Recommendations, Future Work

II. LITERATURE REVIEW AND BACKGROUND

This chapter reviews background and related research. It introduces Multi-Level security (MLS) concepts and definitions.

A. BELL-LAPADULA MODEL

Foundational work on MLS was done in the 1970s for the U.S. Air Force by MIT Research Establishment (MITRE) researchers David E. Bell and Leonard J. LaPadula. They proposed a mathematical model of computer systems security known as the Bell-LaPadula (BLP) model of Multi-Level security (Bell & LaPadula, 1973, p. iii). The second volume of that paper was written two decades later, and it more specifically discusses two properties known as the simple-security property and the *-property (pronounced star property) (Bell & LaPadula, MITRE Technical Report 2547, 1996, p. 2). The simple-security policy (e.g., "no read up") ensures that a process at a lower classification is unable to access information at a higher classification (e.g., a user with a Secret clearance cannot access data classified as Top Secret). A process can include instances of a programs that runs on a computer, such as Microsoft Word. The BLP's *-property (e.g., "no write down") ensures that no user can write data to a lower classification level than it has access to (e.g., programs running at "Secret" cannot write files at "unclassified").

The BLP model implements combinations of discretionary access control (DAC) and mandatory access control (MAC) to achieve specific access controls described in the previous paragraph (Bell, Looking Back at the Bell-La Padula Model, 2005, p. 10). Access control models, such as DAC and MAC, are "generally concerned with whether subjects [e.g., any entity that can manipulate information, such as a user, user process, system process], can access objects [e.g., entities through which information flows through the actions of a subject, such as a directory, file, screen, keyboard, memory, storage, printer], and how this access can occur" (Ausanka-Crues, 2006, p. 2).

DAC policies allow subjects to decide who can achieve access to their objects. DAC policies are implemented by almost every operating system (OS) such as a standard

UNIX OS, Linux, and Windows OS (Conrad, Misenar, & Feldman, CISSP Study Guide, 2016, p. 321).

MAC does not allow users to determine who has access to specific data files and resources. Instead, MAC uses the OS to determine access control based on a user's clearance and data labels (e.g.unclassified, Confidential, Secret, Top Secret) (Conrad, Misenar, & Feldman, CISSP Study Guide, 2016, p. 321). MAC is widely used across Security-enhanced Linux (SELinux) and Windows OS, among other OSs (Ismail, Senousy, & Aboelseoud, 2014, pp. 10-11). Additionally, "MAC is the main access control model used by military and intelligence agencies to maintain classification policy access restrictions…[because] the risk of attack is very high, confidentiality is a primary access control [concern, and] the objects being protected are valuable" (Ausanka-Crues, 2006, p. 2). MLS is a well-known MAC implementation, and the BLP model introduced the basic model of MLS (Rjaibi & Bird, 2004, p. 1010).

B. OTHER MULTI-LEVEL SECURITY RESEARCH

1. 1970s MLS Research

Specific security mechanisms must be implemented to enforce MAC, such as those associated with Dorothy Denning's 1976 "A Lattice Model of Secure Information Flow." This research describes a MAC model to establish a mathematical basis for enforcing information security policies on a computer system (Denning, 1976, p. 242).

In 1977, the Ford Aerospace and Communications Corporation (FACC) began work for the DoD's Kernelized Secure Operating System (KSOS), which was funded by various DoD agencies (Ford Aerospace and Communications Development, 1981, p. 1). The purpose of the KSOS was to instantiate an MLS formula generator that produced prototype support tools that could be used in code proofs (Ford Aerospace and Communications Development, 1981, p. 42).

2. 1980s-1990s MLS Research

In 1983, Honeywell's MLS Secure Communications Processor (SCOMP) was sponsored by the Navy to handle messaging at differing classification levels (National

Bureau of Standards, 1982, pp. 14, 58). Its final report stated future research and development (R&D) investments should be from both the government and industry (National Bureau of Standards, 1982, p. 45).

In the mid-1980s, the DoD used BLACKER as the name for a long-term project that built an integrated device suite to secure the Defense Data Network (DDN) (Weissman, 1992, p. 286). According to the same article, "BLACKER employs the Bell-LaPadula Security Model…in which a DDN host computer is a subject and a cryptographic communication connection between two hosts is an object" (Weissman, 1992, p. 287).

The Sea View project's goal was to create an MLS database for the DoD that met the *DoD Trusted Computer System Evaluation Criteria* (Lunt, Denning, Schell, Heckman, & Schockley, 1990, p. 593). Research from 1989 (by Lunt et al., 1990) created a formal security policy model to incorporate a secure Multi-Level relational database into the Sea View project (Lunt, Denning, Schell, Heckman, & Schockley, 1990, p. 583).

3. 2000s MLS Research

The National Science Foundation and Defense Advanced Research Projects Agency (DARPA) sponsored research to analyze three kernel-based MLS Architectures. (Levin, Irvine, & Nguyen, 2006, p. 3). To determine which MLS architectures are best to employ given specific scenarios, it is important to perform comparative analysis of such architectures. There are no metrics or official common framework to understand what MLS architecture is best to use (Levin, Irvine, & Nguyen, 2006, p. 3). Since these researchers did not have official metrics to understand MLS architectures, they used factors such as: allocation of security functionality, ability to enforce the principle of least privilege, factoring and reusability, runtime resource management, scalability of label space, dynamic security policies, trustworthiness and evaluability, controlled interference, and intransitive information flow (Levin, Irvine, & Nguyen, 2006, p. 8).

That research report states that "[a]fter years of experimentation with alternative techniques, it is apparent that the existence of different levels of data sensitivity in automated environments with heterogeneously-trusted users still calls for multilevel-secure IT systems" (Levin, Irvine, & Nguyen, 2006, p. 10).

An example of an MLS architecture that is specifically purposed to support data aggregation and services with varying data classification levels is the Monterey Security Architecture (MYSEA) (Ong, Nguyen, & Irvine, 2008, p. 294). Researchers tested the MYSEA architecture and found that is fully functional and properly enforces MAC and DAC policies (Ong, Nguyen, & Irvine, 2008, p. 303).

4. Further MLS Research

Some argue that "while there continues to be innovation and research aimed at true MLS at different commercial companies, progress will likely continue to be slow compared to research and development aimed at producing products for a much broader market" (Tipton & Nozaki, 2010, p. 70). The military has a valid need for dealing with various classification levels in different domains. To an extent, the private sector also has this need (especially in the financial industries) but not as much as the DoD.

It appears that "the huge DoD research programme on MLS has disappeared, MLS equipment is no longer very actively promoted on the government-systems market, and systems have remained fairly static…for [the last] decade. Most government systems now operate system high – that is, entirely at Official, or at Secret, or at Top Secret" (Anderson, 2018, p. 303). This sentiment is also echoed in the Air Force Research Lab's (AFRL) Survey of Collaboration Technologies in Multi-Level Security Environments. It states that "[b]ased on the literature reviewed and the finding that little has been done in the MLS domain to assist team performance and decision making through improved collaboration…The approach is drawn from a combination of existing technologies and some technologies that seem feasible, but may not have been developed yet" (Crabtree & Ianni, Survey of Collaboration Technologies in Multi-level Security Environments, 2014, p. 20).

C. CONCLUSION

Today's warfighting environment will integrate both joint and coalition forces, increasing the requirement to share data between differing security domains and platforms. MLS can aid in this collaboration process. As this chapter shows, considerable research

has proven that an MLS approach is possible, practical, and secure. Yet, for many reasons, both the DoD and IC are reticent to employ these capabilities. These significant considerations required to fully adopt this technology are discussed in Chapters III through V.

THIS PAGE INTENTIONALLY LEFT BLANK

III. MULTI-LEVEL SECURITY TECHNOLOGY, ASSESSMENT, AND AUTHORIZATION

This chapter provides an overview of Multi-Level Security (MLS) systems and Cross Domain Solutions (CDSs) concepts, definitions, and authorization processes.

A. MULTI-LEVEL SECURITY AND CROSS DOMAIN SOLUTIONS

The concept of an MLS system is one in which a user on a single workstation is able to access all security domains. MLS systems can be especially valuable when constraints of size, weight, power, and cooling make use of separate networks and computers challenging.

Research from 2006 describes the four basic functions that MLS systems strive to provide, all of which are still relevant today:

- provide, separate, and monitor flows between policy equivalence classes
- MLS policy interpretation and enforcement – which includes allowing high to read from low
- Mediation of a relaxed MLS policy – whereby high information can be securely transitioned to low domains, when appropriate
- Ability to enforce the principle of least privilege on the activity of subjects – to support accountability and confinement of damage (Irvine & Nguyen, 2006, p. 10).

National-level MLS policy forums are hosted by the National Security Agency's Committee on Security Systems (CNSS). The CNSS provides a national level framework by which the U.S. Navy and all U.S. government departments and agencies derive their own cybersecurity policies and guidance. It provides a comprehensive forum for strategic planning and operational decision-making to protect national cybersecurity systems. This thesis uses their definition summaries for the purposes of readability and consistency.

The CNSS defines Multi-Level Security (MLS) as a *concept* used to describe one type of a Cross Domain Solution (CDS). CDSs ensure that only authorized data is able to cross incompatible security classification, releasability, or sensitivity perimeters.

There are three types of CDSs: Access, Transfer and Multi-Level. The latter includes MLS systems. Figure 1 is an overview of the types of CDSs. Appendix A will further discuss the red text portion of Figure 1.

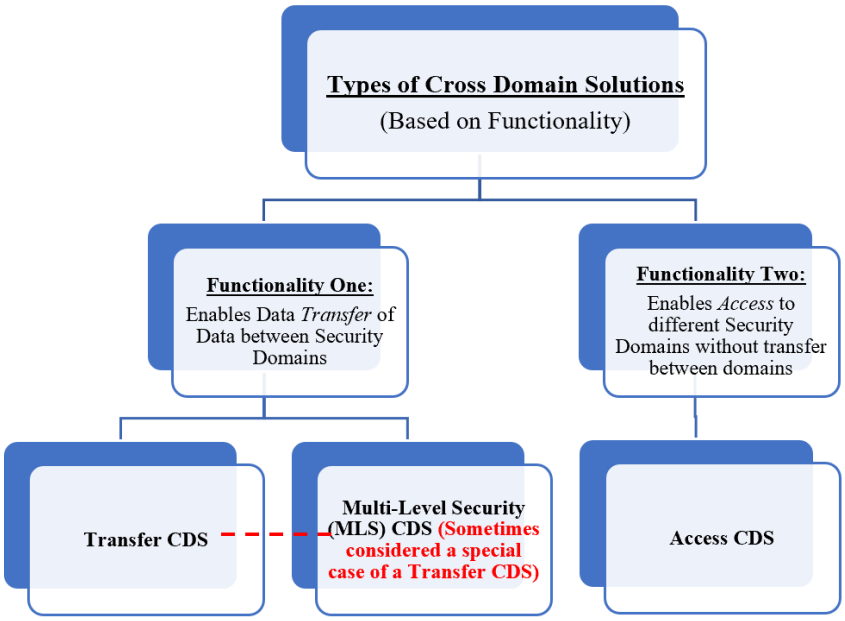

Figure 1. Types of Cross Domain Solutions Based on Functionality. Adapted from CDS Design and Implementation Requirements. Source: National Cross Domain Strategy and Management Office (2020).

An Access CDS provides *access* to the data (not transfer of the data) across domains of differing security classification while maintaining strict network separation. For example, an Access CDS provides users with a remote desktop to access each connected security domain without allowing data transfers between security domains. Usually access is allowed from a higher security domain to a lower security domain.

Transfer CDS' enable the *movement* of data between domains. This action is completed by a process called regrading, which changes the security label to an appropriate level according to the receiving security domain (National Cross Domain Strategy and Management Office, 2020, p. 37). For example, a Transfer CDS can be used to make sure

that a document held at the TS level is properly declassified when downgraded and sent to an unclassified system. A Transfer CDS can also automatically upgrade a Secret document to Top Secret if Top Secret data is added to the document. The overhead associated with regrading (upgrading or downgrading a file to change the security label when content is added or taken away) depends on the specific transfer CDS implementation. For example, some transfer CDS technology may have the ability to automatically regrade based on "dirty word" searches. An example of a dirty word may include specific words or phrases that are classified and should not be transferred to a lower security domain. A transfer CDS may automatically upgrade a document to a higher classification level if it contains dirty words that are not allowed at the destination domain. Although some of these transfer CDS processes can be automatic, humans are still typically required. For example, a human may need to determine if the document should be upgraded due to data aggregation. According to the CNSS, data aggregation is the "[c]ompilation of individual data systems and data that could result in the totality of the information being classified, or classified at a higher level, or of beneficial use to an adversary" (Committee on National Security Systems, 2015, p. 47). For example, the compilation of many individual pieces ofunclassified data may produce Secret data.

1. Multi-Level CDS

A Multi-Level Cross Domain Solution "uses trusted labeling to store data at different classifications and allows users to access the data based upon their security domain and credentials" (Committee on National Security Systems, 2015, p. 84). An MLS CDS is a special case of a Transfer CDS (National Cross Domain Strategy and Management Office, 2020, pp. 36-37). A user must be explicitly granted access to perform "trusted labeling." For example, if a Top Secret (TS) user modifies a Secret file, then a new TS file with the same name will be created by the Multi-Level CDS when the content is saved. The Secret file will not be changed because changing the label (i.e., regrading) is a trusted operation that must be explicitly granted to a user. A Multi-Level CDS can enforce rules that automatically upgrade a file from unclassified to Secret (and store it at the Secret level) if data aggregation warrants its upgrade, or if a Secret piece of data is added to the

document. Some organizations include Multi-Level CDS within the category of a Transfer CDS. Appendix A will discuss the reason for this categorization.

Multi-Level security is the *concept* that describes what Multi-Level CDSs accomplish. The two terms are often used interchangeably. The CNSS defines MLS as a "[c]oncept of processing information with different classifications and categories that simultaneously permit access by users with different security clearances and denies access to users who lack authorization" (Committee on National Security Systems, 2015, p. 84). This enables a warfighter with TS credentials to see data at the unclassified, Confidential, Secret, and TS levels all on the same screen (based on the user's clearance and need-to-know, as well as the classification level of the data). A Sailor with unclassified credentials can only access unclassified data when logging into the same computer workstation. Figure 2 illustrates this concept.

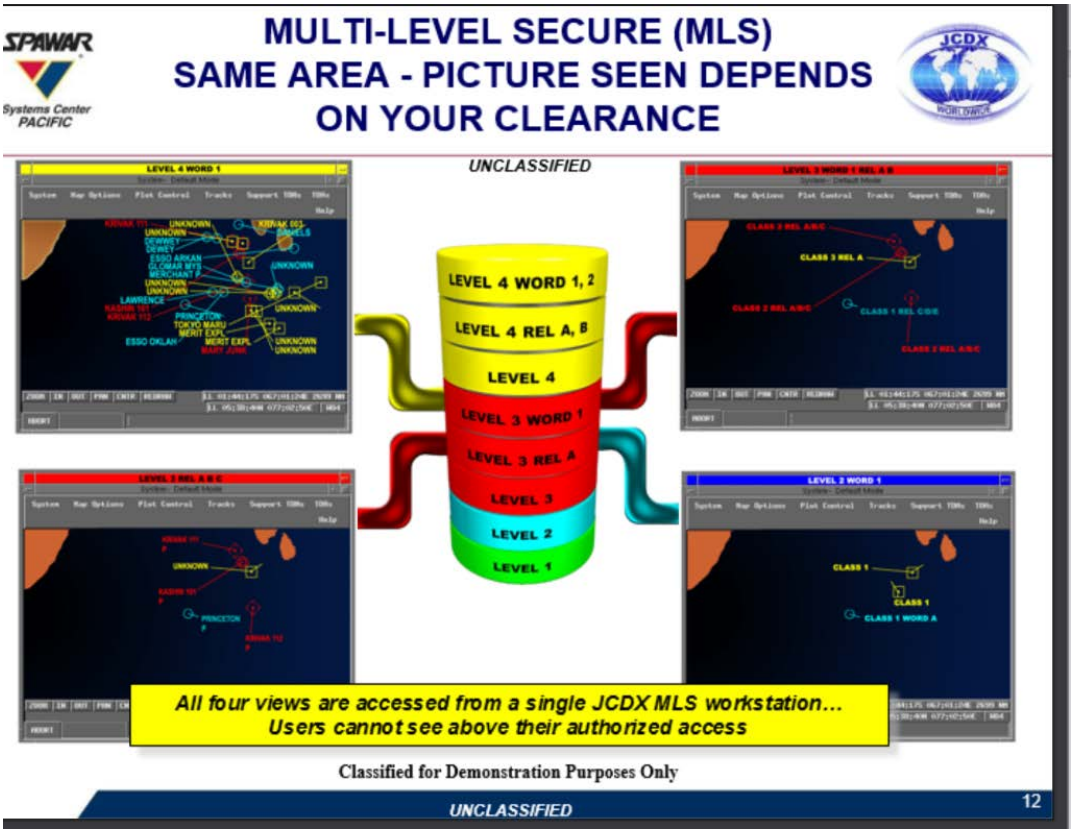

Figure 2. MLS Track Management View. Source: SPAWAR (2016).

2. MLS Considerations

When people picture an operational environment on a ship, such as the Combat Information Center (CIC), their descriptions will likely mirror the following: CIC is a semi-dark room where users sit at their workstation in front of a Windows Operating System (OS) with a Microsoft Office product open on their desktop to read the latest mission details on Powerpoint, as well as their equipment manual on PDF. Each of the user's operational screens (for example, a picture of air or surface tracking information) feeds into the Common Operational Picture (COP) in the front of CIC, which is used to fuse operational displays from each of the workstations spread across the room. The COP is also on a Windows OS and integrates with commercial applications such as Microsoft Office. This setup is familiar and comfortable to operators across the DoD. However, with the proper implementation of a true MLS environment, this scenario would not be feasible. A true MLS environment would disallow the use of a Windows OS and popular commercial products, such as Microsoft Office, Adobe PDF, and Skype, as discussed in the next section.

All users who work in these operational environments, such as CIC, are required to have a Secret clearance, at minimum. There are portions of CIC that are Top Secret, but their screens are hidden from most users in CIC who only have a Secret clearance. Today's DoD traditional CDS environments typically consist of users who are on a single network (e.g., Secret Internet Protocol Router Network [SIPRnet]). In these traditional CDS architectures, a CDS data guard is used to maintain the logical separation of security domains, and they are also used to transfer or access data between security domains (Reed, 2004, p. 1-1). For example, Radiant Mercury is a data guard that "provides an automated means to sanitize, downgrade, guard, and transliterate formatted data at various classifications, compartments and releasabilities" (Research, Development, Test & Evaluation, Navy, 2013, p. 1). Refer to Figure 3 for a visual representation of data guards.

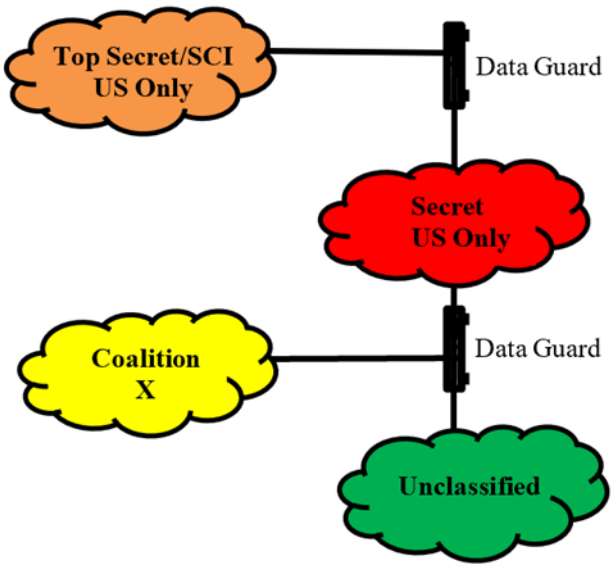

Figure 3. Traditional CDS Architecture with Data Guards. Adapted from Reed (2004).

a. Traditional CDS architectures allow the use of Windows OS and commercial applications—at the cost of limiting other potential DoD seeks

This traditional CDS architecture allows for CIC users to have a Windows OS with their commercial Microsoft applications, because the users are on a single network (e.g., SIPR). Although this CDS architecture affords the benefits of using a popular Windows OS and widely used applications, these advantages limit other potential uses that the DoD needs.

For example, many warfighters desire the ability to run different classifications of data at the same time on the same network, while simultaneously allowing coalition partners on that same network to facilitate C2 and information-sharing (Koelsch, 2013, p. 14). Since this traditional CDS architecture uses a Windows OS on a single network and allows the use of popular applications, it cannot safely allow coalition partners to access the same network without major security risks. More specifically, the Windows OS:

> bases access decisions only on user identity and ownership without considering additional security-relevant criteria such as the operation and trustworthiness of programs, the role of the user, and

> the sensitivity or integrity of the data. As long as users or applications have complete discretion over objects, it will not be possible to control data flows or enforce a system-wide security policy. Because of such weakness of [the Windows OS], it is rather easy to breach the security of [the] entire system once an application [such as Microsoft Word] has been compromised. (Yang, 2003, p. 3).

For example, it is unsafe to allow other countries to connect directly to the DoD network because the DoD's systems have "No foreign nationals" (NOFORN) data on them. This means that material that is supposed to be US-eyes only can easily be compromised through applications (Phillips, Ting, & Demurjian, 2020, p. 90) if other countries were allowed to directly connect. Although certain precautions can be taken to share only coalition data, the Windows OS does not understand labeling and therefore cannot safely separate NOFORN material from coalition partner material (Conrad, Misenar, & Feldman, 2010, p. 42). For example, it would not be feasible for both Israel and Saudi Arabia to each have a bilateral connection with the U.S. on the same network because the Windows OS technology does not have the ability to segregate the data in a secure manner (Ceranowicz & Smith, 2020, p. 2). First, the DoD would not want to risk exposing its NOFORN Secret data to either country by allowing them to be on the same network as the U.S. Additionally, both Israel and Saudi Arabia would likely not want to risk exposing their data to each other by being on the same Secret network as each other with no ability for the Windows OS to segregate the data properly.

b. MLS architectures allow better flexibility in sharing joint and coalition data—at the cost of disallowing the safe use of Windows OS and commercial applications

The introduction of a true MLS environment with SELinux aids in the ability to allow easier data sharing with joint and coalition partners. However, MLS requires an even greater need than traditional CDS architectures to precisely protect the data, because unlike traditional CDS architectures, unclassified, Confidential, Secret, and Top Secret data all reside in a single MLS security domain (Raytheon, 2007, p. 8). See Figure 4 for a visual comparison of a traditional CDS vs. MLS architectures.

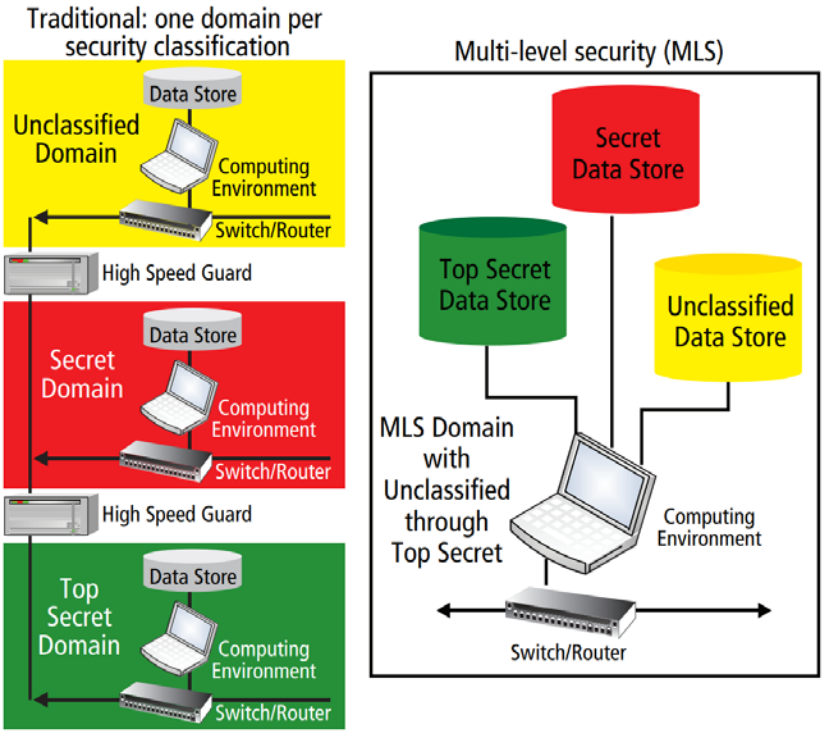

Figure 4. Traditional CDS vs MLS Architectures. Source: Raytheon (2007).

c. Some popular applications do not adequately support labeling requirements inherent to MLS

MLS requires security labels. Security labels in the military security model consist of "two components: a security level with one of the four ratings: unclassified, confidential, secret, and top secret…[and] a set of zero or more categories…For example, (TS, {Crypto, Nuclear})" (Yang, 2003, p. 4). Labels provide the ability for users to query data according to their permission levels, which is required in an MLS environment. For example, a Secret user could see all Secret and below data from their workstation, while an unclassified user on that same machine would see only unclassified information. Unfortunately, neither the Windows OS nor popular commercial applications such as Microsoft Office and Adobe products support the enforced security labeling that MLS requires (Anderson, 2008, pp. 256, 267-270).

To fully implement a true MLS architecture, custom label-aware bespoke applications are required. Standard commercial applications do not have the ability to

enforce security labels on them and are therefore not authorized on MLS systems. All applications that are to be used on an MLS system must be label-aware; new label-aware applications must be created and maintained. The military has moved away from bespoke (customized) applications and it also has recently emphasized the need to leverage industry partnership to obtain relevant technology (Shanahan, 2018a, p. 8).

Label-aware applications will require development and additional maintenance considerations. The military wants to live in a world where it evolves quickly with technology. This goal becomes difficult to achieve with an MLS CDS because every time it undergoes changes it has to be re-tested.

The next section describes the lengthy assessment and authorization process required for CDSs, including MLS.

B. CDS ASSESSMENT AND AUTHORIZATION PROCESS OVERVIEW

This section outlines the CDS (including MLS) Assessment and Authorization (A&A) processes for different classification levels. It also describes the different approval process requirements based on General Service (GENSER), Sensitive Compartmented Information (SCI), or Special Access Program (SAP) systems. More detailed information is included in Appendix B.

1. GENSER CDS Approval Process

The term “GENSER” refers to classified information that does not utilize security protections higher than Confidential, Secret, and TS information. For example, TS with SCI does not follow under a GENSER system, because TS/SCI is a higher security protection than TS. A brief overview of the GENSER CDS approval process is provided in the Risk Management Framework (RMF) for DoD IT Instruction (DoDI 8510.01). The GENSER CDS approval process is further detailed in the Cross Domain (CD) Policy (DoDI 8540.01). The broad overview of the approval process is provided in Figure 5.

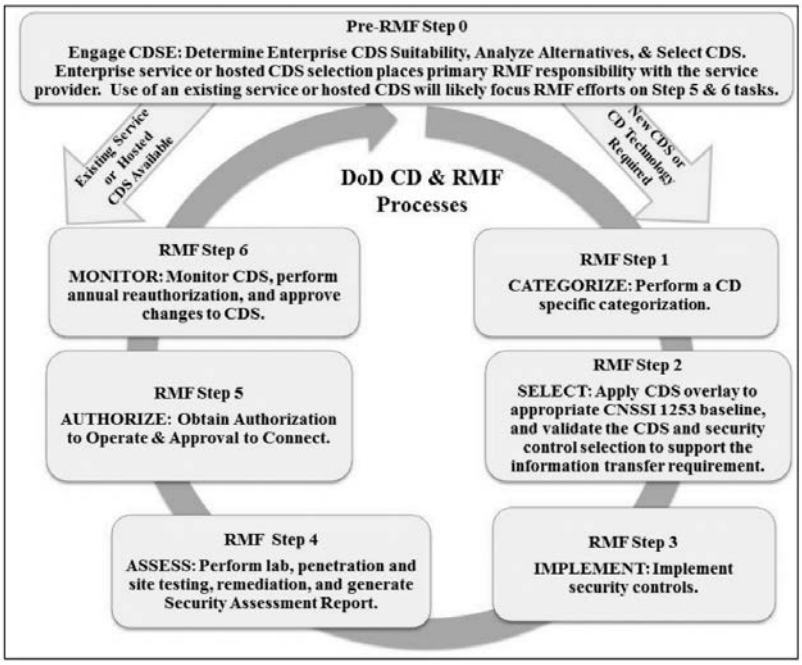

Figure 5. DoD CD and RMF Process. Source: DoD Chief Information Officer (2017).

At the end of each step, CDS documentation is reviewed by the Cross Domain Technical Advisory Board (CDTAB). The CDTAB feeds its recommendations at each step to the Defense Information Assurance (IA)/Security Accreditation Working Group (DSAWG). The DSAWG's stamp of approval after steps 1, 3, 5, and 6 is required prior to entering the next step. Although the CDTAB and DSAWG offer approval after each step, the Authorizing Official (AO) authorization is required prior to final DSAWG or DoD ISRMC CDS approval (DoD Chief Information Officer, 2017c, p. 41).The DSAWG makes connection approval recommendations to the DoD Information Security Risk Management Committee (ISRMC), which holds the final risk decision authority for all Defense Information System Network (DISN) connections. The ISRMC may choose to delegate that final risk decision responsibility to DSAWG for an enterprise CD service or CDS (DoD Chief Information Officer, 2017c, p. 11).

The GENSER Assessment and Authorization (A&A) process adds further complexity with several iterations of the Cross Domain Technical Advisory Board (CDTAB) and Defense Information Assurance (IA)/Security Accreditation Working

Group (DSAWG) reviews, as shown in Figure 6. These layers of approval add additional oversight that can slow CDS adoption.

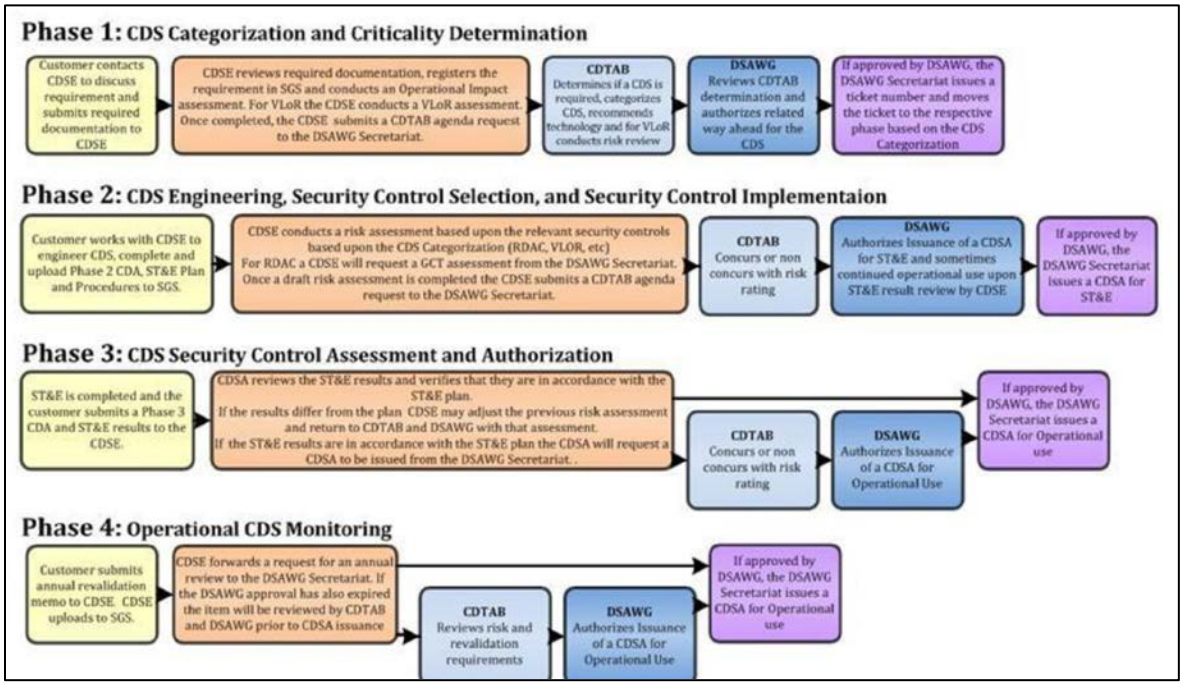

Figure 6. DoD CDS Connection Process Diagram. Source: Defense Information Systems Agency (2016).

2. SCI and SAP Systems

The DoD Joint SAP Implementation Guide (JSIG) governs the DoD SAP cybersecurity and it also provides standardized security and policies for all networks, systems, and components that fall under the cognizance of the DoD SAP Central Office (SAPCO) and DoD Service/Agency SAPCOs (Special Access Program Office, 2016, pp. 1-2). It charters the Joint SAP Cybersecurity Working Group (JSCS WG) to provide DoD SAP cybersecurity implementation guidance (Special Access Program Office, 2016, pp. 1-2).

This JSIG outlines six RMF steps (categorize, select, implement, assess, authorize, monitor), which are the same broad categories as the GENSER RMF categories depicted in Figure 5. One major difference is that the SCI/SAP systems do not contain a Pre-RMF

step depicted at the top of Figure 5. Similar to the DoD CD Policy that details specific actions required under each RMF process, the JSIG also lists specific tasks and documentation that are required outputs from each step.

The SCI/SAP process requires different documents and specific outputs of each step compared to the GENSER process. However, the functionality of each step is generally similar. For example, the first step in both the GENSER and SCI/SAP systems requires CDS categorization. The SCI/SAP process detailed in the JSIG accomplishes this task by directing the IS owner to assign an Information System Security Engineer (ISSE) to work with each other to categorize the IS and document the results in the System Security Authorization Agreement (SSAA)/System Security Plan (SSP). The ISSE is responsible for conducting IS security engineering activities (Special Access Program Office, 2016, pp. 1-20). The roles of the ISSE in this step appears similar to the roles of the GENSER's Cross Domain Support Element (CDSE). In the GENSER process, CDSEs are established at the DoD Component level (DoD Chief Information Officer, 2017c, p. 16). Although the ISSE and CDSE's responsibilities appear similar, the SAP/SCI process states that the IS Owner (ISO) holds the responsibility to assign an ISSE at program inception, which is a lower level than a DoD Component level (Special Access Program Office, 2016, pp. 2-30).

Additionally, a cursory glance of the JSIG appears to show less overhead within the CDS approval process for SAP/SCI systems. For example, there are not several iterations of review boards (such as the CDTAB and DSAWG reviews required in the GENSER CDS approval process) that are intertwined throughout the SCI/SAP CDS approval process.

C. DOD AND INTELLIGENCE COMMUNITY'S CDS POLICIES

The DoD and Intelligence Communities (IC) implement three major policies in this arena, namely the DoD's Cross Domain (CD) policy, the IC's Intelligence Community Directive (ICD) 503, and the Raise the Bar (RTB) standards relevant to both the DoD and IC.

a. DoD Cross Domain Policy

The Department of Defense Cross Domain Instruction provides the policy, responsibilities, and procedures pertaining to the interconnection of different security domains using CDSs (DoD Chief Information Officer, 2017c, p. 1). This instruction applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD. These entities are referred to collectively as "DoD Components" (DoD Chief Information Officer, 2017c, p. 1). Although this instruction encompasses a wide array of entities, it does not alter or supersede the policies that govern DoD ISs with CDSs connected to TS/SCI security domains. The policies that govern TS/SCI ISs are established by the Director of National Intelligence (DNI), as shown in part B.

The DoD's CD policy states that the:

> DoD will employ existing enterprise CD service provider's (ECDSP's) enterprise CD service or enterprise-hosted CDS when their use satisfies the CD mission requirements of DoD Components. Leveraging another operational CDS, deployment of a CDS baseline list point to point CDS or development of a new CD technology will be considered as alternative solutions only when an enterprise solution cannot meet the CD capability requirements. (DoD Chief Information Officer, 2017c, p. 2)

This requirement means that when possible, CDS deployment should consist of pre-established enterprise CDSs, modified versions of the pre-established enterprise CDSs, or existing non-enterprise CDS/MLS solutions. The procurement and deployment of completely new CDS/MLS solutions are usually the last resort. Although this practice is typical, given some of the benefits associated with MLS, it can be argued that it may be beneficial to adopt varying degrees of MLS architectures depending on one's operational environment and mission needs.

b. Intelligence Community Directive Number 503

The Director of National Intelligence establishes many IT policies and procedures apart from other DoD components. These unclassified policies do not appear to be updated as frequently as the unclassified DoD component policies, potentially since the IC is known to operate at more classified levels. The Intelligence Community's IT system security risk management is covered by Intelligence Community Directive Number 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation" (Office of the Director of National Intelligence, 2008, p. 1). This ICD applies to:

> the IC, as defined by the National Security Act of 1947, as amended, and other departments or agencies that may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned as an element of the IC. (Office of the Director of National Intelligence, 2008, p. 1)

c. RTB Standards

In addition to the DoD's CD policy and the IC's ICD 503, continuously updated RTB standards are published annually by the NCDSMO to detail CDS Design and Implementation Requirements (National Cross Domain Strategy and Management Office, 2020, p. 1). In actuality, the RTB standards are published every few months to address changes due to threats. The frequency to which this document is consistently updated shows the DoD's commitment to update its CDS policies. Constraints on which version of the RTB standards can be used are cumbersome. For example, "a CDS entering [Lab-Based Security Assessment] in 2023 would be allowed to use the 2020, 2021, 2022, and, if available, the 2023 version of this document. But it would not be able to use the 2019 version. It is recommended that the latest released version of this document be used" (National Cross Domain Strategy and Management Office, 2020, p. 25). As shown by the RTB timeline summary in Table 1, CDS technologies have finite deployment timelines, which (by paper) enforces the retirement of old technology (National Cross Domain Strategy and Management Office, 2020, p. 25). Further information detailing the RTB standards are shown in Appendix A.

Table 1. RTB Requirements Baseline Release Timeline. Source: National Cross Domain Strategy and Management Office (2020).

RTB Requirements Baseline Release Year	Development, Testing, Deployment, and Sunset Timeline										
	CY19	CY20	CY21	CY22	CY23	CY24	CY25	CY26	CY27	CY28	CY29
2018	Dev & Test			Deployment			Sunset				
2019		Dev & Test			Deployment			Sunset			
2020			Dev & Test			Deployment			Sunset		
2021				Dev & Test			Deployment			Sunset	

D. CONCLUSION

Successful implementation of CDSs (including MLS) will facilitate the ability to seamlessly transfer and/or access shared data between Joint and coalition forces—enabling coordination between forces in conflict. However, lengthy approval processes slow the integration of emergent technologies such as MLS into the broader C2 system.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DIGITAL TRANSFORMATION IN THE NAVY

This chapter looks at MLS in a future context – a digitally transformed Navy. Numerous intersecting strategies were promulgated in the last 12–18 months to initiate and guide the transformation.

A. STRATEGIES

The Department of Defense (DoD) needs to find ways to expand the narrowing gap between near-peer competitors. The next Global Power Competition (GPC) will likely require all physical domains to work together in a synergistic manner to seize the objective. It is difficult to seamlessly integrate Command and Control (C2) and other decision-making data within one physical domain, but that challenge to assimilate data becomes even more magnified when it comes from all physical domains spanning coalition forces from across the world (Erwin, 2013, p. 2). The team that is able to leverage and make risk decisions using data in the most effective, secure way possible is likely to win the next GPC conflict (Shanahan, 2018b, pp. A-4).

The 2018 National Defense Strategy (NDS) states that "[w]e must anticipate the implications of new technologies on the battlefield, rigorously define the military problems anticipated in future conflict, and foster a culture of experimentation and calculated risk-taking" (Mattis, 2018, p. 8). Implementation of the NDS requires the Joint Force and mission partners to employ command and control systems that will ensure speed in decision-making and operational advantage. Commanders will increasingly automate their access to and analysis of data to feed their decision-making process.

The data will come from many different sensors, and it will be labeled and stored at multiple classification levels. These systems are traditionally hosted on different classification enclaves and will need to transfer information between incompatible security domains or levels of classification via a Cross Domain Solution (CDS). To realize the NDS vision, MLS systems will be embedded throughout All-Domain Operations (a concept that will be discussed later in this chapter).

B. DOD DIGITAL TRANSFORMATION

The DoD's Digital Modernization Strategy is the roadmap that supports the National Defense Strategy implementation through the shift to technologies such as cloud storage and AI.

The DoD's Digital Modernization Strategy, first released in 2019, presents DoD Information Technology (IT) modernization goals to support the NDS. It states that, "[m]odernization of the Defense Information Systems Network (DISN), a key component of Department of Defense Information Network (DoDIN), will provide critical enhancements necessary to fully realize the benefits of cloud computing, big data analytics, mobility, Internet of Things (IoT), increased automation and cognitive computing" (Norquist, 2019, p. 14).

The introduction of technologies such as cloud computing has created a need for new strategies to address their use. In the last 12–18 months, DoD and Navy strategies have been released for AI, Cloud, Digital Modernization, Big Data, and Internet of Things (IoT). There are several big data strategies, such as the Federal Data Strategy released June 2019, the DoD's Data Modernization Strategy released Jul 2019, and the Navy Data Strategy released in 2017 (Cyber Security and Information Systems Information Analysis Center, 2020, p. 1).

Three additional strategies, for Cyber Risk, IT Reform and C3 are being drafted. The strategies are shown in Figure 7.

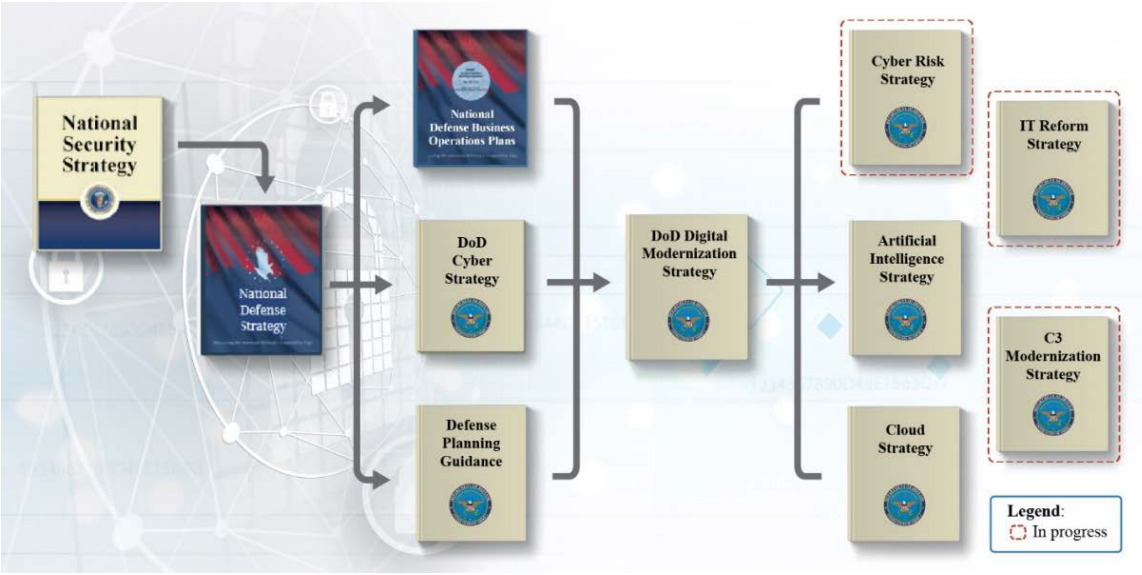

Figure 7. Emergent Technology Strategies. Source: Norquist (2019).

Out of these broad categories, the DoD CIO's specific priorities in digital modernization are: cybersecurity, AI, cloud, and command, control, and communications (C3) (Norquist, 2019, p. 4). Further, the DoD Digital Modernization Strategy states that:

> [c]loud is the foundation upon which DoD will build and scale more effective cybersecurity, advanced analytical capabilities, better command and control, and future enabling technologies. This foundation will enable the Department to organize massive amounts of data and support rapid access to information for improved decision-making, preserving and extending our military advantage. To better take advantage of this information, the optimized enterprise cloud environment will also provide a platform for advanced capabilities such as machine learning (ML) and AI that are necessary to increase decision-making quality, speed, and lethality. DoD will partner with industry to securely deliver commercial cloud capabilities in alignment with mission requirements and will manage these capabilities across the enterprise. (Norquist, 2019, pp. 15-16).

As the DoD Modernization Strategy alludes to, cloud computing is the foundation that will enable data organization to support improved decision-making, and the DoD is leveraging the capability that cloud computing brings to the fight. In September 2017, former Defense Deputy Secretary Patrick Shanahan issued a memo titled, "Accelerating Cloud Adoption," which announced that the Department would make a rapid cloud

adoption. A few months later the Joint Enterprise Defense Infrastructure (JEDI) strategy document was released to solicit industry-based cloud solutions for the DoD's unclassified, Secret, and Top Secret (TS) storage.

1. Cloud Strategy

The adoption of cloud computing is not new to individual agencies within the DoD, but it is new in terms of considering enterprise-wide practice. In 2009, the federal government started to shift its data storage needs to cloud-based services and away from agency-owned data centers. The shift to cloud-based services increased after Executive Branch of the U.S. government released top level guidance in 2010. This 25-Point Plan provided guidelines for agencies to shift to a "Cloud First" policy, and mandated agencies to implement cloud-based solutions whenever a secure, reliable, cost-effective cloud option existed (Kundra, 2010, p. 7) As a result, in 2018 the DoD maintained over 500 public and private cloud infrastructures that supportunclassified and Secret requirements, many of which were supported by the same major industry leaders (yet the DoD manages those contracts individually, vice the enterprise level) (Deputy Secretary of Defense, 2018, p. 1).

According to a Combined Congressional Report that addresses JEDI cloud computing and a framework for the Department to acquire cloud computing services, "[t]he hundreds of cloud initiatives have created numerous seams, incongruent baselines and additional layers of complexity for managing data and services at an enterprise level" (DoD Chief Management Officer, 7). The Report states that this lack of a DoD-wide cloud initiative inhibits the ability to access, analyze, and share critical data; a skill requirement if the DoD wants to expand the narrowing gap between near-peer competitors.

The DoD's Cloud Strategy was released in December 2018 (Shanahan, 2018b, p. 1). It states that "[d]ata stored in an enterprise DoD cloud will be highly available, well-governed, and secure. Data will be the fuel that powers those advanced technologies, such as [Machine Learning] ML and AI" (Shanahan, DOD Cloud Strategy, 2018b, p. 5). Further, it states that:

> DoD must enable decision makers to use modern data analytics, such as Al and machine learning (ML), at the speed of relevance to

> make time-critical decisions rapidly in the field to support lethality and enhanced operational efficiency… This critical decision making data will be made available through modem cloud networking, access control, and cross domain solutions to those who require access. Common data standards will be a key part of the Department's methodology for tagging, storing, accessing, and processing information. (Shanahan, DoD Cloud Strategy, 2018b, p. 5)

2. Artificial Intelligence Strategy

The Artificial Intelligence (AI) Strategy, released 12 February 2019, was a few months prior to the release of the DoD's Digital Modernization Strategy (Cronk, 2019, p. 1). The AI Strategy states that AI leadership will take steps to ready existing AI applications simultaneous to the Department's efforts to create a common foundation of shared data and cloud services (DOD Chief Information Officer, 2019b, p. 7). It states that when a common foundation of shared data, cloud services, and AI are "[t]aken together, these enterprise-wide changes promote the spread of adaptable problem-solving using AI, increase the rate of experimentation and speed of delivery, and streamline the scaling of successful AI prototypes" (DOD Chief Information Officer, 2019b, p. 7). This statement means that cloud services enable effective use of emergent technologies, such as AI, since cloud services enable a common foundation for users to leverage shared data.

Cross Domain Solutions address access control and require common data standards. The MLS type of CDS is especially useful for tagging data, as discussed in Chapter III. These strategies echo the view that cloud computing will be a key enabler of the DoD's ability to use technologies as they emerge.

Maintaining an abundance of data under a DoD-wide cloud and AI initiatives promises to increase efficiencies in many parts of the Department, including to:

- Enable Exponential Growth
- Scale for the Episodic Nature of the DoD Mission
- Proactively Address Cyber Challenges
- Enable AI and Data Transparency
- Extend Tactical Support for the Warfighter at the Edge
- Take Advantage of Resiliency in the Cloud
- Drive IT Reform at DoD (Shanahan, 2018b, p. 3)

As the U.S. Navy and Department of Defense enact the guidance in the Digital Modernization Strategy, it will be necessary to determine the best CDS environment to access this data with the highest confidentiality, integrity, and availability (CIA) to increase the speed at which warfighters can make accurate and informed decisions.

C. MULTI-LEVEL SECURITY IN ALL-DOMAIN OPERATIONS

The United States is gearing up for the next major conflict with the deployment of a concept known as All-Domain [warfighting] Operations. This concept has evolved over the past few years and was originally known as Multi-Domain Battle, followed more recently by the term Multi-Domain Operations (MDO). All-Domain Operations is a joint warfighting concept with a vision to integrate and share kinetic and non-kinetic battle data from the land, sea, air, space, and cyberspace domains, to make decisions and fight at machine-to-machine speed. This vision assumes cloud storage, AI, and wide use of labeled data. MLS is included in this concept.

Command and control (C2) in All Domain Operations is being explored as part of the Joint All Domain Command and Control (JADC2). The U.S. Air Force is the Executive Agent of JADC2. The U.S. Air Force's initial All-Domain Operations wargames (formerly known as Multi-Domain Command and Control) determined that the "[c]urrent [C2] structure is not optimized for the Multi-Domain fight and is only possible if we...develop coalition compatible, Multi-Level Security, shared Multi-Domain SA technical solutions" (Air Force Lessons Learned, 2018, p. 29). The end of the report more bluntly stated that, "Multi-Level security solutions are mandatory for effective information sharing" (Air Force Lessons Learned, 2018, p. 75).

All-Domain Operations and JADC2 concepts include the plan for data to span multiple classification levels from various systems across the DoD and coalition partners. Thus, it will require CDSs (such as MLS) to enable the transfer or access of this data. The JADC2 is further detailed in Appendix C (an FOUO appendix).

V. ORGANIZATIONAL ISSUES

This thesis views the adoption of technology, specifically Multi-Level Security (MLS), through three lenses. Chapter III looked at MLS *technology* and processes. Chapter IV considered how MLS can integrate into a digitally transformed Navy operating in All-Domain Operations, a different *context* than our Navy today. This chapter looks at the institutional change needed to sustain adoption by considering *organizational* issues.

Adoption of new technology requires that organizations change. If adoption is sustained, people within those organizations will do their work differently than they did before. A challenge for Navy leaders is that technology is changing rapidly while organizations change much more slowly. Adopting MLS systems will require a commitment to long term organizational change.

Fortunately, the complex topic of organizational change is well-researched. A framework can be useful to organize the myriad issues associated with technology adoption. The framework used in this research is the Organizational Design Star Model™ developed by Jay R. Galbraith in the 1960s (Galbraith, 2020, p. 1). While the framework includes many subcomponents, only the ones applicable to adopting an MLS strategy are discussed.

A. STRATEGY

Strategy dictates which activities are most necessary, thereby providing the basis for making the best trade-offs in the organization design" (Galbraith, 2020, p. 2). The "strategy" design factor includes strategic communication, leadership commitment, and resource investments in All-Domain Operations, including technology (such as MLS). Strategies for digital transformation of the DoD and the Navy were discussed in Chapter IV. This research focuses on resources as part of the adoption strategy.

Figure 8. Strategy and Goals. Adapted from Jansen, Gallenson, and Higgins (2015).

The USAF stands out in its swift and dedicated focus to MLS resource allocation. The USAF's dedication to Multi-Domain Command and Control (MDC2) led the Joint Requirements Oversight Council (JROC) to name the USAF the lead to run the Joint All-Domain Command and Control (JADC2) technical testing and tactics validation at its Shadow Operations Center at Nellis AFB in Nevada (Hitchens, OSD & Joint Staff Grapple with Joint All-Domain Command, 2019, p. 2). Followed by that testing, the USAF was recently named as the single authority responsible for the JADC2 program and is accountable to meet the Army, Navy, Marine Corps, and Air Force requirements (Clark, Hyten: All Domain Drives Requirements Shakeup, 2020, p. 12). This designation does not mean that all services are required to adopt USAF JADC2 technology, but it will need to be interoperable with the USAF's JADC2 core structure. Because of the USAF's Doolittle Series 2018 (DS18) wargame outcome that MLS is needed for MDC2 operations, the JADC2 framework will likely use an MLS environment in its core structure.

The USAF's pre-established Advanced Battle Management System (ABMS) will allow all platforms to simultaneously "receive, fuse, and act upon a massive collection of data from all [warfighting] domains instantaneously…[and additionally] ABMS will require, software and algorithms so that artificial intelligence [(AI)] and machine learning can compute and connect vast amounts of data from sensors and other sources at a speed and accuracy far beyond what is currently attainable" (Insinna, The Air Force just conducted the first test of its Advanced Battle Management System, 2019, p. 5). ABMS

focuses on interoperability which allows for the Services to not necessarily be required to use all of the USAF's systems that integrate into ABMS if it does not make sense for the other Services to use them.

Similar to the USAF, the Intelligence Community identified the importance of MLS systems. The National Security Act as amended in January 2020 states that the: "[Director of National Intelligence] shall…ensure development of information technology systems that include multi-level security and intelligence integration capabilities" (Senate and House of Representatives, 2020, p. Section 102A). In the wake of the analysis of the terrorist attacks of September 11, the 9/11 Commission identified the need for a unity of effort in information sharing. The Office of the Director of National Intelligence (ODNI) recognized that the culture needed to shift from a "need-to-know" mentality to more of a "need-to-share" mentality (Best, 2011, p. 1). Subsequently, major statutory and regulatory changes were made to facilitate information sharing by the creation of the Information Sharing Environment (ISE), which was established by the Intelligence Reform and Prevention Act of 2004 and a direct result of 9/11 Commission recommendations to establish policies, procedures, and technologies to link people, systems, and information from government agencies" (Office of the Director of National Intelligence, 2020). As a result of the ISE establishment, "[i]n law and in Federal regulations a culture of sharing has been established in the Intelligence Community" (Best, 2011, p. 1).

Throughout this "information sharing" culture shift, the Intelligence Community implemented MLS technology in instances such as Joint Cross Domain eXchange (JCDX) which is an MLS intelligence tracking framework used to provide early warning of potential threats on a global scale (KeySoft Systems, 2020). JCDX is installed at the Atlantic Intelligence Center (AIC) at USACOM Headquarters; Joint Intelligence Center-Pacific (JIPAC) at INDOPACOM headquarters; JIPAC detachment (J-DET) Yokota Air Force Base, Japan; and Joint Analysis Center (JAC) Molesworth in UK. The system enables its users to view intelligence tracking data based on the user's access level and need-to-know. As briefly mentioned at the beginning of this chapter, MLS technologies must be RTB-compliant. In light of the most recent RTB requirements, although JCDX was previously on the approved list of CDS, JCDX is no longer approved by the NCDSMO,

the Defense Information Assurance (IA)/Security Accreditation Working Group (DSAWG), or the DoD Information Risk Management Committee (ISRMC). More information will be provided on the approvals and authorities of these entities in the next chapter, but it is important to make the distinction that though JCDX was previously permitted, without RTB compliance it will no longer be approved without adjusting to the new standards.

B. TASKS, PRACTICES, AND TECHNOLOGY

The second component of adoption is tasks, practices, and procedures, as seen in Figure 9. For MLS adoption, this section focuses on two practices that drive why the Navy does not use MLS today, and a practice that makes it increasingly likely in the future.

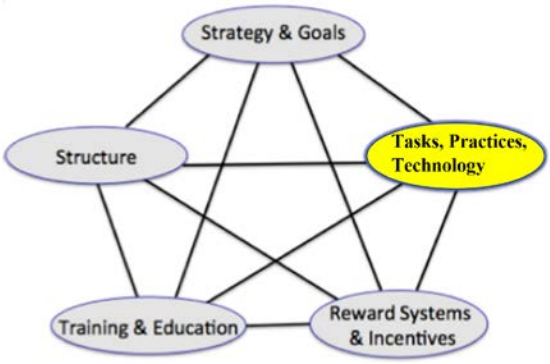

Figure 9. Tasks, Practices, Technology. Adapted from Jansen, Gallenson, and Higgins (2015).

Administrative and operational work in the Navy currently relies on the Windows Operating System (OS) and Microsoft Office products which do not support required MLS features such as security labeling and MAC, a true MLS environment will require a different OS (Yang, 2003, p. 3). For example, Security-enhanced Linux OS (SELinux) can be used:

> Security-enhanced Linux (SELinux) is a reference implementation of the Flask security architecture for flexible mandatory access control [MAC]. It was created to demonstrate the value of flexible mandatory access controls and how such controls could be added to

> an operating system…[It] provides general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement®, Role-based Access Control, and Multi-Level Security. (National Security Agency, 2020, p. 1)

The Windows OS does not have the ability to segregate the data. An SELinux system is more suited for that operation. The SELinux system enforces labeling, so every time data is created, the user is forced to label it. For example, when writing a paragraph in a document, the SELinux enforces the user to add a label and portion mark it. Based on that label and the user's assigned classification level, s/he can access data up to that level, as well as any associated caveats (e.g., a French person classified up to the Secret level can view the Secret//Rel-France and Secret//Rel NATO data). Since practices are typically dictated by using a Microsoft OS (vice SELinux), a hybrid-MLS approach can be taken with the addition of using cloud-based applications that support data labeling better than desktop applications. Cloud-based applications (such as Microsoft Word online) afford the opportunity to label data and place it in a classified cloud computing environment. The Intelligence Community (IC) operates in the IC GovCloud, which is a "big data fusion environment" (Konkel, 2018, p. 1). Cloud-based solutions are helpful to segregate data and pull data based on what is needed.

The MLS database allows for the opportunity to query the data based on its security label. For example, it has the ability to label a user as a notional French, Saudi, U.S., etc., user. MLS databases are important because if a Secret user wants to query stored Secret data and searches "Secret," then that user can only query data based on his or her rights. In other circumstances using non-SELinux OSs, the returned data would be anything that includes a classification of "Secret," including "Top Secret" data. MLS ensures that a user is only able to query data based on his or her rights, regardless of what s/he may try to query.

The U.S. Air Force is moving to MLS because it solves the limitations that aircraft have on size, weight, power, and cooling (SWAPC). Some aircraft (such as the F-35) use a massive MLS switch to protect vital mission data for the entire aircraft, excluding flight-critical systems (L3Harris, 2020, p. 1). This MLS infrastructure consists of two pods that

sit below the pilot; and the operational plans work at the unclassified level all the way up to secret and below interoperability (SABI). Data is passed between pods in this infrastructure, and software is loaded based on the mission set. The goal is to load operational plans up to the TS level eventually; as done with the F-22, U-2, F-18, and other aircraft.

For warfighters on an aircraft, the integration of MLS systems for various mission sets at various classification levels makes sense to address SWAPC considerations. Individual infrastructure for individual classification levels and domains is not feasible given the SWAPC limitations that aircraft pose. Certain parts of this infrastructure also include sensors that are labeled at various SAP levels, and it would certainly be infeasible to build additional infrastructure to account for this. Typical combat missions are labeled at Secret/SAP, but in some cases a mission may be TS, which requires data to be processed up to that level for that mission. After that mission there could be a requirement to go down to the Secret/SAP level for the next mission. Switching infrastructure is used to segregate the data, and in some cases a transfer CDS is required to move data between the levels. In addition to air assets, MLS is popular in ground vehicles as well due to SWAPC considerations.

C. STRUCTURE

Structure includes roles and responsibilities, processes and organizations engaged in CDS and MLS technology authorization (Figure 10). Current assessment and authorization processes for MLS have been addressed in Chapter III. This section addresses organizational roles and how it is very complex, the special roles of standards organizations and how they function to support adopting new technologies, the key interorganizational construct of reciprocity, and lastly, how DoD organizations collaborate on adoption.

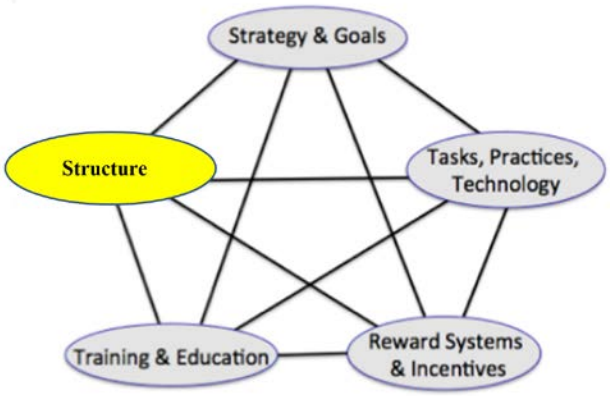

Figure 10. Structure Design Factor. Adapted from Jansen, Gallenson, and Higgins (2015).

1. Roles and Responsibilities

Some Program of Records (PORs) have multiple authorizing officials involved in their approval processes, slowing down the adoption of technology at a rapid pace.

Authorizing official determination is based on whether or not a DoD component wants to implement a CDS on a General Service (GENSER), SCI, or a SAP Information System (IS). Sometimes these delineations are not as clear because they connect various systems that span many different Enterprise Cross Domain Service Provider (ECDSPs). For the DoD and IC, the three primary general purpose ECDSPs are:

- Defense Information Systems Agency (DISA) for Non-Secure Internet Protocol (IP) Router Network (NIPRNet) and Secure IP Router Network (SIPRNet) connections;
- Defense Intelligence Agency (DIA) for NIPRNet, SIPRNet, and Joint Worldwide Intelligence Communications System (JWICS) connections; and
- United States Air Force (USAF) Secretary of the Air Force (SAF)/Concepts Development and Management (CDM) United States (US) Battlefield Information Collection and Exploitation System (BICES) Program Office for coalition and bi-lateral networks including Combined Enterprise Regional Information Exchange System (CENTRIXS) (National Cross Domain Strategy and Management Office, 2019, p. 29).

There are also mission specific ECDSPs for Geospatial Intelligence (GEOINT), Signals Intelligence (SIGINT), and weather (among many other mission sets) (National Cross Domain Strategy and Management Office, 2019, p. 29). AOs are designated within each ECDSP, and there are some ISs that require far more than one AO's approval because they span multiple mission areas. These types of challenges are not unique to CDS technologies such as MLS; they also occur with other emergent technologies.

For example, Project Maven is an, "AI-powered surveillance platform for unmanned aerial vehicles…[that gives] the government real-time battlefield command and control and the ability to track, tag, and spy on targets without human involvement" (Greene, 2019, p. 3). Because this AI platform spans regions that are covered under multiple AOs, the additional oversight caused by the need to gain multiple AO approval creates a challenge to update algorithms in a timely and consistent manner.

More specifically, the Navy's AO determination guide is specified through OPNAVINST 5239 (Office of the Chief of Naval Operations, 2018, p. 5). It states that:

> All IT with direct connections to the Defense Information Systems Network (DISN) must be authorized by signature of the [Navy Authorizing Official (NAO)]. Any IT that was formerly authorized by a [Functional Authorizing Official (FAO)] that is seeking to connect to the DISN will follow DDCIO(N) guidance to renew their [Authority to Operate (ATO)] under NAO's cognizance. This will be done per the requisite memorandums of understanding between the respective program, FAO, and the NAO. (Office of the Chief of Naval Operations, 2018, p. 5)

The Navy Cybersecurity Program Instruction appoints U.S. Fleet Cyber Command (FLTCYBERCOM) as the NAO for all classified and unclassified and GENSER TS and below USN IT assets not under the cognizance of an FAO (Office of the Chief of Naval Operations, 2018, p. 18). This instruction further states that, "NAO signature authority will not be delegated below the O-6/GS-15 level due to the enterprise scope of their cognizance. These delegations must be appointed and maintained by Commander, FLTCYBERCOM with a copy provided to CNO (N2N6)" (Office of the Chief of Naval Operations, 2018, p. 18).

According to the Navy Cybersecurity Program Instruction, FAOs include: Naval Air Systems Command (NAVAIRSYSCOM), Naval Facilities Engineering Command (NAVFACENGCOM), Naval Sea Systems Command (NAVSEASYSCOM), Naval Information Warfare Systems Command (NAVWARSYSCOM), and Strategic Systems Programs (SSP) (Office of the Chief of Naval Operations, 2018, p. 24).

These FAOs provide mission area technical authority (TA) domain-expertise and certification authority. NAVAIRSYSCOM is the TA for, "air systems, aeronautical weapons systems and associated subsystems, support equipment, components and parts, systems integration, software, and human systems" (Office of the Chief of Naval Operations, 2018). This instruction also states that NAVFACENGCOM is the TA for, "all matters related to facilities engineering policies and practices." Additionally, it lists NAVSEASYSCOM as the TA for ships and ship systems, while SSP is the TA for sea-based deterrent missile systems. Finally, it states that NAVWARSYSCOM is the TA for command and control (C2) systems, space systems, force level warfare systems architectures, and FORCEnet. NAVWARSYSCOM is also the command, control, communications, computers, and intelligence (C4I) chief engineer to all other SYSCOMs (Office of the Chief of Naval Operations, 2018, p. 13).

Sometimes the lines are blurred and the IS falls under the purview of both the Navy Authorizing Official (NAO) and Functional Authorizing Official (FAO). The NAO states that, "[a]ll IT with direct connections to the Defense Information Systems Network (DISN) must be authorized by a FAO that is seeking to connect to the DISN" (Office of the Chief of Naval Operations, 2018, p. 5). However, there are examples where equipment that falls under both the FAO and the NAO.

2. The Function of Standards Organizations

Another barrier to MLS adoption is the lack of flexibility and responsiveness embedded in DoD standards bodies versus comparable international standards bodies. There are thousands of Standards Development Organizations (SDOs) throughout the civilian industry sector that are used to develop and publish many International Standards. There are over 200 SDOs used to develop standards for information and communication

technologies (ICT) (Schneiderman, 2015, p. 253). Addition information regarding both organizations is discussed in Appendix B.

a. International Organization for Standardization (ISO)

The ISO International Standard approval process is somewhat lengthy; as such, there is a "fast track" process to account for urgent market needs that may arise. Within this "fast track" framework, a consensus of ISO working group experts publish Publicly Available Specifications (PAS) which have a maximum life of six years (International Organization for Standardization, 2020a, p. 5). Outside entities apart from working groups are also able to use this process to transpose their specifications into an ISO/IEC standards. One such PAS-authorized group is the World Wide Web Consortium (W3C). These PAS specifications are not official International Standards; however, they can either be transformed into an International Standard or withdrawn after the six-year life passes. This injected "fast track" process is shown in Figure 11.

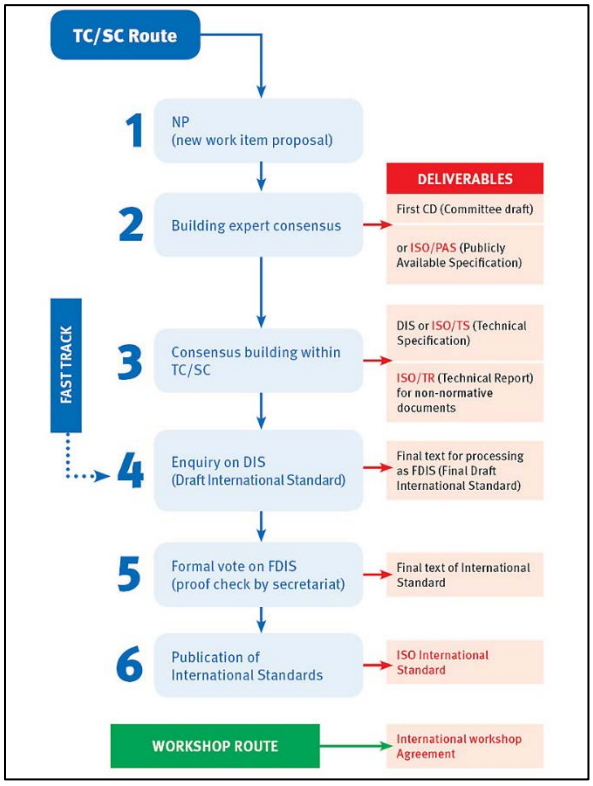

Figure 11. ISO Standards Routing Process. Source: International Organization for Standardization (2020).

The PAS "fast track" process was created in October 1994 by the Joint Technical Committee 1 (JTC 1; purpose is to develop worldwide Information and Communications Technology) after its traditional paradigm was criticized due to its "slow responses to dynamic market pressures, ineffective efforts to develop anticipatory standards, dogged pursuit of perfect solutions when 'good enough' would be tolerable" (Yates & Murphy, 2019, p. 259). JTC1's procedural change to account for quick market changes was unprecedented. JTC1's PAS process allows authorized PAS submitters such as W3C (PAS submitter status is a three-month process) to quickly turn the consortia's publicly available specifications into standards (Yates & Murphy, 2019, p. 259).

Even with this "fast track" PAS addition, JTC1's current Strategic Business Plans discuss the challenges associated with the rapid pace of technological development. The most recent LTBP states that:

> - International Standardization, including JTC 1, is challenged to accelerate its processes to match the speed of market-driven product cycles, and to be viewed as competitive with other standardization organizations in the ICT Sector.
> - The need to establish national body consensus before achieving JTC 1 approvals can also cause standards development delays, even though it will often be seen as an advantage to have such consensus before seeking international standardization.
> - The business models for ISO and IEC still rely significantly on the sale of International Standards (and the protection of copyright interests), which is a challenge for JTC 1 in the face of freely-distributed standards from other groups.
> - Although the use of electronic collaboration tools (e.g., teleconferencing techniques) is rising, the travel costs required to participate in international standards development can be burdensome to some participants. Improved participation and development models are needed. (ISO/ETC JTC 1, 2013, p. 9)

JTC1's goal to produce standards in a timely manner to meet market needs is addressed in every one of its publicly available business plans, dating back from 1998 (ISO/ETC JTC 1, 2013, p. 1).

b. Standards Development Adoption within the DoD

The DoD has practices in place to leverage the emergent standards that Standards Development Organizations (SDOs) create. DoD Instruction (DoDI) 8310.01, "Information Technology Standards in the DoD," establishes "policy, assigns responsibilities, and provides direction for identifying, developing, and prescribing DoD standards for information technology (IT), to include national security systems (NSS) and defense business systems (DBS)" (DoD Chief Information Officer, 2017b, p. 1). The instruction further delineates that the DoD Executive Agent (EA) for IT Standards will track and report IT emerging technologies and standards development of interest to the DoD from organizations such as American National Standards Institute (ANSI) and W3C. More specifically, the adopted DoD standards are chosen from the source categories listed in Table 2.

Table 2. DoD Standards Consideration. Source: DoD Chief Information Officer (2017).

Source	Example
Federal Law, Regulation, or Instruction	U.S. Code, OMB Circular
Internationally Accredited and Treaty Based	International Standards Organization (ISO), International Electrotechnical Commission (IEC), United Nations/Economic Commission for Europe (UN/ECE), International Telecommunication Union (ITU), International Standardization Agreement
National	American National Standards Institute (ANSI)
Professional Society, Technology Consortia, Industry Association	Institute of Electrical and Electronics Engineers, Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), Organization for the Advancement of Structured Information Standards (OASIS), Object Management Group, Open Geospatial Consortium
Federal	Federal Information Processing Standard
Military	MIL-STD, standardization agreement

The DoD Directive (DoDD) 5105.19 designates the Director, Defense Information Systems Agency (DISA) as the DoD EA for IT Standards. In this capacity, the Director, DISA shall:

> [integrate], through standards, DoD information systems and networks serving both U.S. and authorized foreign partners…shall organize, chair, and participate in U.S. military IT standards bodies to develop, publish, and maintain established and developmental interoperability standards…[and] shall also represent [DoD] interests in Federal, nongovernmental, international, and allied IT standards bodies. (Director of Administration and Management, 2006, p. 6)

DISA maintains its list of standards via the DoD Information Technology Standards Registry (DISR). DISR is the unifying DoD registry for, "approved…IT and national security systems (NSS) standards and standards profiles" (Defense Standardization Program Office, 2020, p. 1). Once the DoD approves and adopts those standards, they are listed in the DISR. Mandated DISR standards are to be enforced above competing standards, while emerging DISR standards are authorized for use, but cannot be used in lieu of a Mandated Standard. Additionally, information/guidance standards are used to clarify standards but do not need to be used (Defense Standardization Program Office, 2020, p. 1). The DISR list contains myriads of standards, and the "Information sharing Cross Domain Solution (CDS) Standard" from 15 January 2017 is the sole CDS-related standard on the DISR listing (Defense Standardization Program Office, 2020, p. 1).

According to the Defense Standardization Program, mandated IT Standards on the DISR list are required to be used throughout the DoD Acquisition process and need to be included in Information Support Plans (ISPs). The ISP "identifies…[IT and NSS] information needs, dependencies, and interface requirements, focusing on interoperability, supportability, and sufficiency" (McCaskill, Hicks, & Kmorowski, 2020, p. 4). ISPs are used in the acquisition process and are mentioned in CDS-specific policies.

DoD components are required to comply with RTB standards that are no older than three years, with annual CDS documentation reassessment (National Cross Domain Strategy and Management Office, 2020, p. 25). If it meets certain requirements, a CDS can potentially be deployed for up to six years before being sunset (National Cross Domain Strategy and Management Office, 2019, p. 25). Although these deployment timelines are similar to the ISO "fast track" standards that are valid for up to six years, the DoD has not altered this A&A process to account for rapidly evolving technology such as CDSs.

It can take at least 2–5 years to buy and procure a new CDS, and may cost $5-10 million for development alone, notwithstanding testing costs that are likely also in the millions of dollars (National Cross Domain Strategy and Management Office, 2020, p. 30). If a DoD component wants to employ a CDS more quickly (and cheaply), it will need to buy (or buy and modify) a current CDS technology on the NCDSMO CDS Baseline list (National Cross Domain Strategy and Management Office, 2020, p. 29). Doing so, however, does not necessarily shorten the approval process path. There is a process to request for CD Urgent Operational Requirement that allows the DSAWG Chair to approve an administrative interim CDSA to meet the urgent operational requirement within 24–48 hours when necessary (DoD Chief Information Officer, 2017c, p. 28). This process is for urgent requests only, and it is not something that is permanently fed into the system, such as the "fast track" option that the ISO process offers.

3. Reciprocity

The Defense Counterintelligence and Security Agency (DSCA) Assessment and Authorization Process Manual (DAAPM) is a living document that governs CDS requirements for cleared contractors participating in the National Industrial Security Program (NISP), which includes but is not limited to the DoD, SAPs, and Intelligence Communities (National Industrial Security Program Authorization Office, 2020, p. i). The DAAPM focuses on the adoption of common guidelines to streamline and build reciprocity into the Assessment and Authorization (A&A) process.

Reciprocity, as defined in CNSSI 4009, is a "[m]utual agreement among participating enterprises to accept each other's security assessments to reuse IS resources and/or to accept each other's assessed security posture to share information" (National Industrial Security Program Authorization Office, 2020, p. 1). Though reciprocity does not imply blind acceptance, it does offer the ability for organizations to accept approvals by other organizations to connect or reuse IT without the requirement to spend time, money, and other resources on retesting (National Industrial Security Program Authorization Office, 2020, p. 1).

The DoD's Cross Domain policy requires DoD components to employ existing Enterprise Cross Domain Service Provider's CDSs when possible. Under this guidance, when a DoD component (non-TS/SCI or non-SAP) wants to employ a CD to interconnect systems of differing security domains, it must first look to see if its specific capability requirement is met by a CDS that is already on the National Cross Domain Services Management Office (NCDSMO) Control List, which is a CDS baseline list (DoD Chief Information Officer, 2017c, p. 2).

More specific guidance for the IC via Intelligence Community Directive (ICD) 503 states that it "focuses on a more holistic and strategic process for the risk management of [IT] systems, and on processes and procedures designed to develop trust across the intelligence community [IT] enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions" (Office of the Director of National Intelligence, 2008, p. 1). Reciprocity is certainly emphasized in this directive. In regard to reciprocity, it states that, "[a]n IC element shall accept the certification of a system or other item of [IT] by another IC element without requiring or requesting any additional validation or verification testing of the system or item of IT" (Office of the Director of National Intelligence, 2008, p. 7).

Though the DAAPM streamlines reciprocity for DoD components (governing non-TS/SCI systems), it never mandates that any DoD element *shall* accept the certification of a system completed by another DoD element. The IC's requirement for IC elements to accept certification from other IC elements stands in stark contrast to the non-TS/SCI DoD component's guideline provided by the DAAPM.

4. Collaboration across the DoD

One method of policy collaboration across the DoD is shown with the Committee on National Security Systems (CNSS). The CNSS promulgates its cybersecurity guidance documents through its committees, subcommittees, panels, and working groups to provide the framework by which the U.S. government (USG) departments and agencies derive their own policies and guidance. According to its website, CNSS is the cornerstone for cybersecurity guidance collaboration efforts among Federal National Security Systems

(NSS), Federal non-NSS, and non-Federal systems. It also, "sets national-level cybersecurity policies, directives, instructions, operational procedures, guidance and advisories for U.S. government departments and agencies for the security of National Security Systems...It provides a comprehensive forum for strategic planning and operational decision-making to protect NSS and approves the release of INFOSEC products and information to Foreign Governments" (Committee on National Security Systems, 2016, p. 1).

The adoption of international standards through organizations such as the ISO is helpful for interoperability and community-learned "best practices" on a worldwide scale. However, in this age of rapidly developing technology, there needs to be increased efforts within the DoD to work more collaboratively.

NCDSMO's baseline CDS list is a beneficial way to offer CDS technology collaboration and reciprocity among DoD components. Much more needs to be done to reduce duplicate CDS research efforts, and the JADC2 working group is a helpful start to tackle this issue.

D. TRAINING AND EDUCATION

The fourth component of adoption is training and education (Figure 12). As with any new practice, training and education need to be modified and co evolved, as technologies advance. This research highlights a new occupational specially focused on MLS.

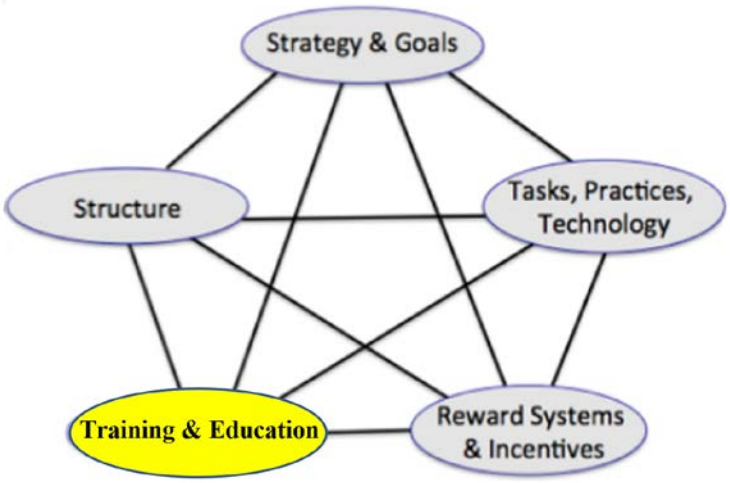

Figure 12. Training and Education Design Factor. Adapted from Jansen, Gallenson, and Higgins (2020).

The first Doolittle Series (DS18) wargame was held 6–8 November 2018 at the LeMay Center Wargaming Institute in Alabama. Its central objective was to figure out how to manage data flows coming from all over the world from every domain: air, land, sea, and cyberspace. It was the inaugural event, and only included USAF, Royal AF, and AUS AF. The DS18 After Action report directly stated that MLS technologies must be leveraged for the MDC2 environment. The report stated that the "Current [C2] structure is not optimized for the Multi-Domain fight and is only possible if we...develop coalition compatible, Multi-Level Security, shared Multi-Domain SA technical solutions" (Air Force Lessons Learned, 2018, p. 29). The end of the report more bluntly stated that, "Multi-Level security solutions are mandatory for effective information sharing" (Air Force Lessons Learned, 2018, p. 75).

The MDC2 Capabilities Office was stood up at the Hanscom Air Force Base in Massachusetts focused on developing new tools and technologies to build networks and technology requirements for program managers to adopt their best practices. Major General Saltzman (formerly the Deputy Chief of Staff for Operations at USAF Headquarters) stated that Doolittle's wargame findings caused that MDC2 office to prioritize its work on Multi-Level Security (Cohen R. , 2018, p. 1). Around the same time as the MDC2 Capabilities Office establishment, MDC2 further moved from research to reality when a select group

of 34 mid-career officers began the USAF inaugural MDC2 training course to prepare for a new career field known as 13O, or "13-Oscar" in April 2019. Major General Saltzman expects for the 13O billets to reach around 500 billets, with around 250 majors, 125 lieutenant colonels, and 25 colonels working on MDC2 (Saltzman, 2018, p. 16).

E. REWARD SYSTEMS AND INCENTIVES

As progress continues All-Domain Operations, JADC2, CDS and MLS development, leaders will need to align incentives for information sharing with their strategic goals for the same (Figure 13).

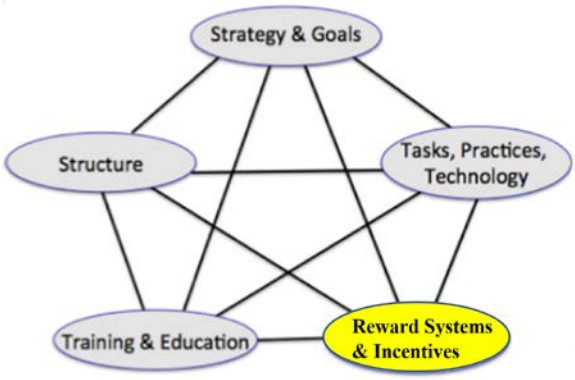

Figure 13. Reward Systems and Incentives Design Factor. Adapted from Jansen, Gallenson, and Higgins (2020).

F. CONCLUSIONS

The endorsement of high-level proponents for All-Domain Operations led to the establishment of the JADC2 Cross Functional Team (CFT) to coordinate C2 efforts appropriate to All-Domain Operations. The USAF and IC are increasing investments in MLS technology as a means to support evolving C2 mission requirements. Although higher authority guidance and champions for All-Domain Operations and MLS are essential, they are not enough to assure adoption of MLS

Continuous evaluation of multiple areas depicted in Galbraith's Star Model™ Framework may reveal areas that will lead to better integration and sustained adoption of

emerging CDS technology (such as MLS) into this process. However, the variety of organizations and cross competing processes highlight that adopting MLS across the services, or even within the Navy, faces formidable challenges.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS, RECOMMENDATIONS, FUTURE WORK

Many different entities inside and outside of the DoD are interested in the efficient adoption of emergent technologies. The failure for the DoD to adopt emergent Cross Domain Solution (CDS) technology in a timely manner may have larger implications than that of the private sector; it could determine the winner of the next Global Power Competition (GPC) conflict.

The DoD is working to integrate emergent CDS technology through its establishment of the Joint All Domain Command and Control (JADC2) construct, the use of the IT Standards EA to identify international standards, and the National Cross Domain Solution Office (NCDSMO) CDS Baseline List to enable reciprocity. Although these organizations and constructs are helpful, the current CDS approval process is inadequate to account for emergent technology. Private standards bodies such as the International Organization for Standardization (ISO) have a "fast track," implemented into its standards approval processes, yet even with these implementations it still struggles to keep up to speed with emergent technology. The DoD does not implement a "fast track" in its CDS approval process; the fastest way to integrate a CDS is by using an already-approved CDS on the NCDSMO Baseline list. Though this is a valid option, there are no "fast track" processes that allow for the integration of emergent technologies that are not already on this list. Additionally, several Authorizing Officials (AOs) span various projects, further lengthening the approval process. Many emergent technologies require frequent updates, which may trigger the need to go through an additional Assessment and Authorization (A&A) process to test the implications that those changes may have on the overall security of the system. Though the A&A process is lengthy for a reason, a "fast track" similar to the ISO is recommended, as well as a solution to require fewer AOs in the approval process for emerging technology that requires frequent updates.

Multi-Level Security (MLS) technology is an example of emergent technology that requires a lengthy approval process. MLS technology could significantly aid in the joint and coalition forces' ability to seamlessly work together in the next GPC conflict, especially in the age where data needs to be fused in an efficient manner to make timely

decisions. Though determination of which types of CDS architectures to employ depend on individual organization's needs, improvements to the A&A process will significantly aid in emergent technology adoption once an organization determines which CDS to employ. Ultimately, improvement in this process will allow organizations to more efficiently adopt ready, relevant technology necessary to stay ahead in the GPC.

A. PROCESS IMPROVEMENT RECOMMENDATIONS

1. Add DoD Component "Fast Track" Options to CDS RMF Process

The DoD CDS A&A requirements do not offer a "fast track" option built into the Risk Management Framework (RMF) process. The General Service (GENSER) A&A process adds further complexity with several iterations of Cross Domain Technical Advisory Board (CDTAB) and Defense Information Assurance (IA)/Security Accreditation Working Group (DSAWG) reviews in between steps. Though this requirement may aid in ensuring that all security aspects are considered, by the time the technology is approved it may be near obsolete, or ready for another update. The ISO standardization process has a built-in "fast track" that is used to speed up emergent technology standardization.

If a DoD component wants to employ a CDS more quickly (and cheaply), it will need to buy (or buy and modify) a current CDS technology on the NCDSMO CDS Baseline list (National Cross Domain Strategy and Management Office, 2020, p. 30). Doing so, however, does not necessarily shorten the approval process path. There is a process to request for a Cross Domain (CD) Urgent Operational Requirement that allows the DSAWG Chair to approve an administrative interim Cross Domain Solution Authorization (CDSA) to meet the urgent operational requirement within 24–48 hours when necessary (DoD Chief Information Officer, 2017c, p. 28). This process is for urgent requests only, and it is not something that is permanently fed into the system, such as the "fast track" option that the ISO process offers.

2. Consolidate MLS Efforts via JADC2 Process and Wargames

Since CDS research is applicable to a myriad of applications, there are varying agencies and organizations inside and outside the DoD that are exploring the most effective ways to implement CDSs. Unfortunately, many of these entities' research efforts are duplicated due to minimal collaboration with organizations outside their purview.

The adoption of international standards through organizations such as the ISO is helpful for interoperability and community-learned "best practices" on a worldwide scale. However, in this age of rapidly developing technology, there needs to be increased efforts within the DoD to work more collaboratively. NCDSMO's baseline CDS list is a beneficial way to offer CDS technology collaboration and reciprocity among DoD components. Much more needs to be done to reduce duplicate CDS research efforts, and the DoD-wide effort to form the JADC2 Cross Functional Team (CFT) is a helpful start to tackle this issue. Technical authority and acquisition commands, such as Naval War Systems Command (NAVWARSYSCOM) would benefit by keeping abreast with JADC2 CFT recommendations and active involvement in JADC2 wargames. Additionally, active involvement with the JADC2 process will afford the opportunity to investigate and recommend MLS adoption as the Navy becomes more engaged in cloud, AI, data labeling, and analysis.

3. Investigate Potential Consolidation to a Single AO for Programs that Span Multiple AOs

In addition to CDS procurement and collaboration challenges, there are Program of Records (PORs) that have multiple AOs involved in their approval process, which slows down the approval process and interferes with the rapid adoption of emergent technology. These challenges are not unique to CDS technologies, but also occur with other emergent technologies.

For example, Artificial Intelligence (AI) platforms (such as those involved with Project Maven) span regions that are covered under multiple AOs. The additional oversight caused by the need to gain multiple AO approval creates a challenge in updating algorithms in a timely and consistent manner. Consideration needs to be taken to determine which

technology should not be required to undergo multiple AO approval, or an alternative process to solve this concern.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

1. Determination of Most Pertinent Label-Aware, Web-Based Applications

It is recommended that future work will provide a detailed pathway of how to adopt label-aware web-based applications. The Navy's decision to adopt more MLS environments may not be determined until label-aware applications become mainstream. Bespoke label-aware application adoption may be beneficial, regardless of the Navy's decision regarding MLS.

A study such as this should consider cost analysis of developing custom applications, as well as determine which non-mission essential applications to develop. Scope creep can easily be introduced in this research area, and before one knows it, s/he can have many more applications required than originally thought.

Another consideration in this area is the determination of how much the integration of bespoke applications creates a cultural resistance and initial lack of productivity. The commercial sector will more than likely continue its use of commercial applications, such as Microsoft Office products. Members in the military use these applications for both personal and professional use, and military members' inclination to use these products in their spare time can potentially cut down the on-the-job training time when needed to use these products at work. A researcher in this area needs to consider the effects of using bespoke versions of everyday applications in the workplace (that are not used for personal use).

2. Design a Test to Determine if a True MLS Environment Increases the Speed of the Commander's Decision-Making

To design a test for this subject, significant controls should be in place. Often times when presented with updated technology, a user may think that s/he "needs" that newer technology simply because it is new; negating the fact that it may not be essential to mission completion. There may also be inherent military bias, where those who are avidly against

MLS systems may not be open to the adoption of an MLS environment. MLS complexity has been around for decades, so naturally experts in this area have more than likely formed an opinion in one direction or another. A test like this would need to prove that the cost (time, training, funds, etc.) is worth it to help commanders achieve quicker and more effective decisions.

This type of a test would need to incorporate real applications in a real environment, all with real data. It may also need to involve people who can show that they do not already have a biased opinion on the subject.

3. Cost Analysis of the Value Added from an MLS Environment

The complexities involved with MLS are astronomical, and the cost is not insignificant. Further research should be conducted to determine the actual cost of implementing a true MLS system, and whether it may be cheaper to put NOFORN on a separate virtualized environment with a CDS in between to transfer and access data. As such, research in this area should include whether the value of MLS decreases due to advancements in virtualization. MLS is certainly achievable with a large budget, but a cost analysis should be carefully considered.

Research in this area may determine that there is very little value added by creating a true MLS environment for a general user-level IT, but that it may be worth it for units with size, weight, power, and cooling (SWAPC) considerations, such as those working with aircraft. If a researcher wants to try that approach, it is necessary to determine the cost of adding bespoke applications and Security Enhanced Linux (SELinux) Operating Systems (OSs), since current commercial applications and Windows OS cannot be used in a true MLS environment.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. RAISE THE BAR STANDARD

In addition to the CNSS documents, the Raise the Bar (RTB) requirements is a continuously updated document that establishes the architecture and implementation requirements for CDSs, including MLS. All CDS developed for use to protect the USG, National Security Information (NSI) and National Security Systems (NSS) are required to implement the RTB requirements per NSA's authorities under National Security Directive 42 to develop standards for systems protecting NSS (National Cross Domain Strategy and Management Office, 2020).

Historically, the MLS CDS was considered a separate class of CDS. This categorization, as defined by the CNSS standards, led to an unsecure and unsafe design and implementation since data filtering during reclassification was not properly implemented (National Cross Domain Strategy and Management Office, 2020, p. 37).

Since MLS is re-categorized as a subtype of transfer CDS, it must meet the new requirements for Access and Transfer CDS, birthed out of RTB standards. One of the most critical requirements is hardware separation which applies to both access and transfer CDS—regardless of the variant used. The RTB standards timeline states that beginning in 2021, a system can no longer connect to High Threat Networks (HTN) without hardware separation (National Cross Domain Strategy and Management Office, 2019, p. 34). The RTB efforts increase IS requirements, with hopes to combat the threats coming from HTNs.

IAW this same guidance, an HTN is defined as, "a network in which a known or suspected highly skilled (e.g., nation-state or transnational organized crime level) cyber actor is operating" (National Cross Domain Strategy and Management Office, 2020, p. 34). Additionally, the RTB standards recognize that an HTN may include cyber actors operating on the network without the knowledge of the primary user of the network.

There are specific milestones that CDSs must meet to be considered RTB-compliant; as discussed in Table 3.

Table 3. RTB CDS Deployment Increments and Implementation. Source: National Cross Domain Strategy and Management Office (2020).

RTB CDS Deployment Increments & Implementation Year	Details
Increment A **By End of 2020**	Implement a Phase 1 Compliant CDS that has been evaluated by an NCDSMO lab
	Comply with DOD CIO "Suspension of New Point-to-Point Cross Domain Solutions and Changes to Existing Point-to-Point Cross Domain Solutions Implementations" memorandum dated 10 October 2018.
	Comply with DOD CIO "Implementing Cross Domain Bug Bounty Remediation" memorandum dated 5 April 2018.
Increment B[4] **By End of 2021**	Implement a NCDSMO lab evaluated hardware-based separation (e.g. diode) mechanism for Unclassified and High Threat Network (HTN)[5] Connections to classified United States Government (USG) National Security Systems (NSS) (Required for ECDSPs for unidirectional and bidirectional dataflows. Required for P2P and Applicable Tactical CDS for unidirectional dataflows)
	Implement a Phase 2 Compliant CDS that has been evaluated by an NCDSMO lab (Required for ECDSPs, others optional)
	Implement NCDSMO compliant Defense Cyber Operations (DCO) of CDS capability (Required for ECDSPs, others optional)
Increment C **By End of 2022**	Implement a NCDSMO lab evaluated hardware-based separation (e.g. diode) mechanism for Unclassified and High Threat Network (HTN)[6] Connections to classified United States Government (USG) National Security Systems (NSS) (Required for P2P and Applicable Tactical CDS for bidirectional dataflows)
	Implement a Phase 2 Compliant CDS that has been evaluated by an NCDSMO lab (P2P and Applicable Tactical CDS)
	Implement NCDSMO compliant Defense Cyber Operations (DCO) of CDS capability (P2P and Applicable Tactical CDS)
Increment D **By End of 2023**	Implement NCDSMO lab evaluated hardware-based separation (e.g. diode) mechanism **with hardware-based filtering** for Unclassified and High Threat Network (HTN) Connections to classified USG NSS (Required for ECDSPs Only, others optional)
Increment E **By End of 2024**	Implement NCDSMO lab evaluated hardware-based separation (e.g. diode) mechanism **with hardware-based filtering** for Unclassified and High Threat Network (HTN) Connections to classified USG NSS (P2P and Applicable Tactical CDS) Implement a Phase 3 Compliant CDS that has been evaluated by an NCDSMO lab (if applicable for environment, usually just ECDSPs)

APPENDIX B. CDS APPROVAL PROCESS IN COMPARISON TO THE ISO PROCESS

As with any information systems (ISs) requirements in the DoD, there are many policies and procedures that govern CDS interconnection approval between security domains. Some of the entities that are engaged with this approval process manage the risk associated with the proposed technology, provide governance approval, and maintain a knowledge of current Cross Domain (CD) technology in use across the DoD. The idea of using IS interconnection approval processes and governing bodies are not unique to the DoD; however, the way in which they are carried out vary vastly between the bureaucratic nature of the DoD and the civilian industry sector.

A. STANDARDS DEVELOPMENT WITHIN THE PRIVATE SECTOR

There are thousands of Standards Development Organizations (SDOs) throughout the world used to develop and publish many International Standards. There are over 200 SDOs used to develop standards for information and communication technologies (ICT) (Schneiderman, 2015, p. 253). One such organization that will be discussed in depth is the International Organization for Standardization (ISO).

The ISO works closely with the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU), and together all three of the organizations form the World Standards Cooperation (WSC) to preserve and advance voluntary consensus-based International Standards systems (World Standards Cooperation, 2020, p. 1). All three of these organizations are known as some of the largest and most well-established standards organizations.

1. International Organization for Standardization (ISO) Structure and Governance

ISO is an “independent, non-governmental organization made up of members from the national standards bodies of 164 countries” (International Organization for Standardization, 2020c, p. 1). The ISO has developed over 23,000 International Standards used to govern various facets of expertise such as quality management standards,

environmental management standards, health and safety standards, energy management standards, food safety standards, and finally Information Technology (IT) standards (International Organization for Standardization, 2020f, p. 3). Designated ISO members submit standards for ISO ratification that detail the best way to accomplish a wide array of activities ranging from process management and supply procurement to security techniques and controls.

There is only one designated member authorized per country, and each member represents ISO in its country. There are three tiers of membership, and each tier experiences varying access levels and influence over the ISO system. The combination of limiting each country to one member, yet simultaneously assigning different tiers of membership allows the ISO to be inclusive while recognizing the capacity that each national standards body maintains. Full members (or member bodies) "influence ISO standards development and strategy by participating and voting in ISO technical and policy meetings. [They also] sell and adopt ISO International Standards nationally" (International Organization for Standardization, 2020b, p. 4). Correspondent members cannot vote in ISO technical and policy meetings, but they are authorized to sell and adopt ISO International Standards nationally. Subscriber members are only able to keep up to date on ISO's work, but cannot participate in it. The conglomeration of members from each country forms the "General Assembly," which is the ultimate authority of the ISO, and it meets annually to discuss strategic objectives.

The ISO Council meets three times a year, and it forms the core governance body of the Organization. It consists of 20 member bodies, as well as various Policy Development Committees, and ISO Officers (International Organization for Standardization, 2020c, p. 2). These entities will not be discussed in depth, but it is important to note that IT advice is provided to the ISO council via the Information Technology Strategy Advisory Group (ITSAG). The ISO Council reports to the General Assembly. The Technical Management Board (TMB) manages technical ISO standards, and consists of Technical Committees that lead standards development and also provides guidance to strategic advisory boards created on technical matters. Figure 14 visually

depicts the ISO Governance Structure. Some of the entities mentioned in Figure 14 are not discussed since they are broader in scope and are not solely specific to the IT community.

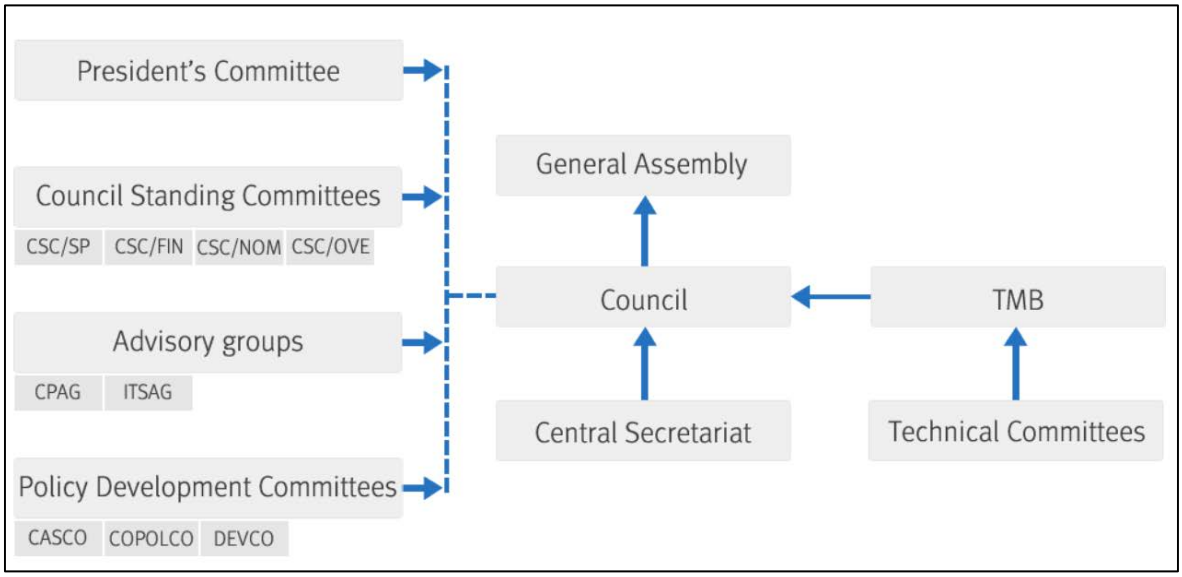

Figure 14. ISO Governance Structure. Source: International Organization for Standardization (2020c).

There are 248 Technical Committees, and the first one is the ISO/IEC Joint Technical Committee (ISO/IEC JTC 1) which develops worldwide Information and Communications Technology (ICT) standards (International Organization for Standardization, 2020g, p. 1). The ISO/ETC JTC1 releases a long-term business plan (LTBP) that is reviewed annually to outline its three to five year plans (ISO/ETC JTC 1, 2013, p. 1). ISO/IEC JTC 1 is comprised of 22 subcommittees which cover specific technologies. Each subcommittee submits a yearly business plan which details specific working group's deliverables, accomplishments, risks, opportunities, and issues (ISO/IEC JTC 1 Subcommittees, 2019, p. 1). The frequency of meetings varies per subcommittee; typically, subcommittees meet on an annual basis. The workhorse of the subcommittees are the individual working groups that are assigned specific problem sets to tackle, as designated by subcommittees' yearly Business Plans. These working groups typically meet twice a year in person, and also hold monthly teleconferences to progress their work.

The Technical Committees' (TCs) subcommittees (SCs) ultimately provide new work item proposals (NPs) to the TC secretariat. The ISO/IEC Consolidated JTC1 Supplement 2017 states that when an NP is submitted, the committee secretariat shall also indicate the selected standards development track to adjust target dates. These development target dates provide 18-, 24-, 36-, and 48-month tracks to publication (ISO/IEC JTC 1 Subcommittees, 2019, p. 1). Upon TC approval from national members from the TC (such as JTC1), that Final Draft international Standard (FDIS) can be submitted to the Central Secretariat for standardization to be published as an International Standard (International Organization for Standardization, 2020e, p. 1). Figure 15 shows the approval process of International Standards within the ISO.

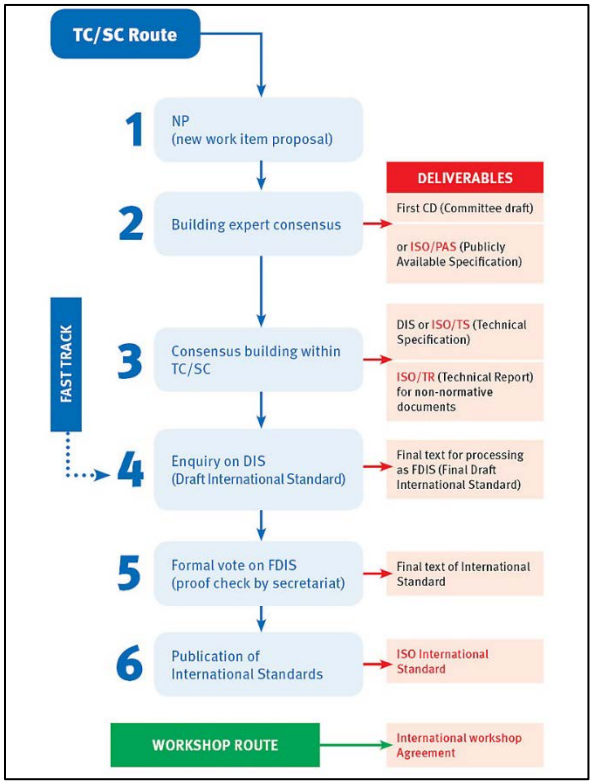

Figure 15. ISO Standards Routing Process. Source: International Organization for Standardization (2020a).

2. ISO International Standards Approval Timeline

The ISO International Standard approval process is somewhat lengthy; as such, there is a "fast track" process to account for urgent market needs that may arise. Within

this “fast track” framework, a consensus of ISO working group experts publish Publicly Available Specifications (PAS) which have a maximum life of six years (International Organization for Standardization, 2020a, p. 5). Outside entities apart from working groups are also able to use this process to transpose their specifications into an ISO/IEC standards. One such PAS-authorized group is the World Wide Web Consortium (W3C) which will be discussed in ensuing sections. These PAS specifications are not official International Standards; however, they can either be transformed into an International Standard or withdrawn.

The PAS “fast track” process was created in October 1994 by JTC1 after its traditional paradigm was criticized due to its “slow responses to dynamic market pressures, ineffective efforts to develop anticipatory standards, dogged pursuit of perfect solutions when ‘good enough’ would be tolerable” (Yates & Murphy, 2019, p. 259). JTC1’s procedural change to account for quick market changes was unprecedented. JTC1’s PAS process allows authorized PAS submitters such as W3C (PAS submitter status is a three-month process) to quickly turn the consortia’s publicly available specifications into standards (Yates & Murphy, 2019, p. 259).

Even with this “fast track” PAS addition, JTC1’s current Strategic Business Plans discuss the challenges associated with the rapid pace of technological development. The most recent LTBP states that:

- International Standardization, including JTC 1, is challenged to accelerate its processes to match the speed of market-driven product cycles, and to be viewed as competitive with other standardization organizations in the ICT Sector.
- The need to establish national body consensus before achieving JTC 1 approvals can also cause standards development delays, even though it will often be seen as an advantage to have such consensus before seeking international standardization.
- The business models for ISO and IEC still rely significantly on the sale of International Standards (and the protection of copyright interests), which is a challenge for JTC 1 in the face of freely-distributed standards from other groups.
- Although the use of electronic collaboration tools (e.g., teleconferencing techniques) is rising, the travel costs required to participate in international standards development can be

> burdensome to some participants. Improved participation and development models are needed (ISO/ETC JTC 1, 2013, p. 9).

JTC1's goal to produce standards in a timely manner to meet market needs is addressed in every one of its publicly available business plans, dating back from 1998 (ISO/ETC JTC 1, 2013, p. 1).

3. ISO Certification and Accreditation Authorities

The ISO develops International Standards, but it does not provide certification and accreditation (C&A) of those standards. According to the ISO.org website, certification is the, "provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements," while accreditation is the "formal recognition by an independent body, generally known as an accreditation body, that a certification body operates according to international standards" (International Organization for Standardization, 2020a, p. 5).

Although the ISO does not perform C&A, it does maintain a Committee on Conformity Assessment (CASCO) that produces many certification process standards used by certification bodies (International Organization for Standardization, 2020a, p. 4). Since C&A is not performed by ISO, a company or organization can only be certified by external certification bodies. The International Accreditation Forum (IAF) works in cooperation with ISO to accredit external certification bodies.

4. ISO representation from the United States

The American National Standards Institute (ANSI) is a full member body designated as the ISO representation for the United States. ANSI accredits standards *developers* to establish a consensus among qualified groups, but it does not write the standards (International Organization for Standardization, 2020d, p. 2). The ANSI Board of Directors established the Executive Standards Council (ExSC) to accredit national standards developers and U.S. Technical Advisory Groups (TAGs) to ISO (American National Standards Institute, 2019, p. 2). ANSI-Accredited Standards Developers are authorized to submit a American National Standard (ANS) to be considered as an ISO or ISO/IEC JTC-1 standard (American National Standards Institute, 2019, p. 5). On the other

hand, ANSI-Accredited U.S. TAGs fulfill the part of ANSI's role to determine the U.S. position in regard to its support of a proposed International Standard. There are 220 developers that are accredited to develop and maintain almost 10,000 ANSs, some of which are national adoptions of global standards (International Organization for Standardization, 2020d, p. 2). All ANSs are voluntary documents, but many U.S. federal, state, and local bodies refer to ANS documentation for regulatory policy.

B. STANDARDS DEVELOPMENT WITHIN THE DOD

DoD Instruction (DoDI) 8310.01, "Information Technology Standards in the DoD," establishes "policy, assigns responsibilities, and provides direction for identifying, developing, and prescribing DoD standards for information technology (IT), to include national security systems (NSS) and defense business systems (DBS)" (DoD Chief Information Officer, 2017b, p. 1). The instruction further delineates that the DoD Executive Agent (EA) for IT Standards will track and report IT emerging technologies and standards development of interest to the DoD from organizations such as ANSI and W3C. More specifically, the adopted DoD standards are chosen from the source categories listed in Table 4.

Table 4. DoD Standards Consideration.
Source: DoD Chief Information Officer (2017b).

Source	Example
Federal Law, Regulation, or Instruction	U.S. Code, OMB Circular
Internationally Accredited and Treaty Based	International Standards Organization (ISO), International Electrotechnical Commission (IEC), United Nations/Economic Commission for Europe (UN/ECE), International Telecommunication Union (ITU), International Standardization Agreement
National	American National Standards Institute (ANSI)
Professional Society, Technology Consortia, Industry Association	Institute of Electrical and Electronics Engineers, Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), Organization for the Advancement of Structured Information Standards (OASIS), Object Management Group, Open Geospatial Consortium
Federal	Federal Information Processing Standard
Military	MIL-STD, standardization agreement

1. DoD Executive Agent for IT Standards

The DoD Directive (DoDD) 5105.19 designates the Director, Defense Information Systems Agency (DISA) as the DoD EA for IT Standards. In this capacity, the Director, DISA shall:

> [integrate], through standards, DoD information systems and networks serving both U.S. and authorized foreign partners…shall organize, chair, and participate in U.S. military IT standards bodies to develop, publish, and maintain established and developmental interoperability standards…[and] shall also represent [DoD] interests in Federal, nongovernmental, international, and allied IT standards bodies. (Director of Administration and Management, 2006, p. 6)

2. DoD Information Technology Standards Registry (DISR)

DISA maintains its list of standards via the DoD Information Technology Standards Registry (DISR). DISR is the unifying DoD registry for, "approved…IT and national security systems (NSS) standards and standards profiles" (Defense Standardization Program Office, 2020, p. 1). Once the DoD approves and adopts those standards, they are listed in the DISR. Mandated DISR standards are to be enforced above competing standards, while emerging DISR standards are authorized for use, but cannot be used in lieu of a Mandated Standard. Additionally, information/guidance standards are used to clarify standards but do not need to be used (Defense Standardization Program Office, 2020, p. 1). The DISR list contains myriads of standards, and the "Information sharing Cross Domain Solution (CDS) Standard" from 15 January 2017 is the sole CDS-related standard on the DISR listing (Defense Standardization Program Office, 2020, p. 1).

According to the Defense Standardization Program, mandated IT Standards on the DISR list are required to be used throughout the DoD Acquisition process and need to be included in Information Support Plans (ISPs). The ISP "identifies…[IT and NSS] information needs, dependencies, and interface requirements, focusing on interoperability, supportability, and sufficiency" (McCaskill, Hicks, & Kmorowski, 2020, p. 4). ISPs are used in the acquisition process and are mentioned in CDS-specific policies, to be discussed

in subsequent sections. Additionally, DISA's plan to fulfill its role in facilitating military IT standards bodies will be discussed.

C. IMPORTANT DOCUMENTS THAT GOVERN CDS REQUIREMENTS

1. Cross Domain Policy: DoDI 8540.01

The Department of Defense Cross Domain (CD) Instruction provides the policy, responsibilities, and procedures pertaining to the interconnection of different security domains using CDSs (DoD Chief Information Officer, 2017c, p. 1). This instruction applies to the OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD. These entities are referred to collectively as "DoD components" (DoD Chief Information Officer, 2017c, p. 1). Although this instruction encompasses a wide array of entities, it does not alter or supersede the policies that govern DoD ISs with CDSs connected to TS/SCI security domains. The policies that govern TS/SCI ISs specifically are established by the Director of National Intelligence (DNI), and will be detailed in subsequent paragraphs.

2. Risk Management Framework (RMF) for DoD Information Technology (IT): DoDI 8510.01

DoDI 8510.01 establishes the RMF process for DoD IT, establishes associated cybersecurity policy, and assigns responsibilities for executing and maintaining the RMF process (DoD Chief Information Officer, 2017a, p. 1). This instruction applies to all DoD components that were detailed in the previous section, as well as the U.S. Coast Guard and all DoD-controlled IT operated by a contractor or other entity on behalf of the DoD.

This instruction details generic actions that govern Steps 1–6 of the RMF process. Steps 1–6 of this process are: Categorize, Select, Implement Security Controls, Assess Security Controls, Authorize System, and Monitor Security Controls. These steps are broadly categorized in this instruction, but further detail is provided by DoDI 8540.01.

3. Cybersecurity: DoDI 8500.01

DoDI 8500.01 establishes the DoD cybersecurity program to protect and defend DoD information and IT (DoD Chief Information Officer, 2019b, p. 1). This instruction also establishes and defines the roles and positions of the DoD principal authorizing official (PAO) and the DoD Senior Information Security Officer (SISO) and continues the DoD Information Security Risk Management Committee (DoD ISRMC). These roles will be discussed throughout the DoD standards bodies discussion and approval process. It applies to the same DoD components detailed in DoDI 8540.01, all DoD IT, all DoD information in electronic format, and SAP IT (other than SCI).

4. The Defense Counterintelligence and Security Agency (DSCA) Assessment and Authorization Process Manual (DAAPM)

The DAAPM is a living document that governs CDS requirements for cleared contractors participating in the National Industrial Security Program (NISP), which includes but is not limited to the DoD, SAPs, and Intelligence Communities (National Industrial Security Program Authorization Office, 2020, p. 3). Under the DAAPM, cleared contractors must follow the Risk Management Framework (RMF) process to obtain system authorization to implement the technology.

The DAAPM focuses on the adoption of common guidelines to streamline and build reciprocity into the Assessment and Authorization (A&A) process. Reciprocity, as defined in CNSSI 4009, is a "[m]utual agreement among participating enterprises to accept each other's security assessments to reuse IS resources and/or to accept each other's assessed security posture to share information" (National Industrial Security Program Authorization Office, 2020, p. 1). Though reciprocity does not imply blind acceptance, it does offer the ability for organizations to accept approvals by other organizations to connect or reuse IT without the requirement to spend time, money, and other resources on retesting (National Industrial Security Program Authorization Office, 2020, p. 16).

5. Executive Order Number 12333, as amended

Though the DoDI 8540.01 Cross Domain Policy carries extensive authorities over DoD components, it does not alter or supersede existing authorities and policies of the

Director of National Intelligence (DNI) regarding the protection of SCI as directed by Executive Order Number 12333 (amended by Executive Order Number 13470) (Reagan, Ronald, 1981, p. 1). All DoD Information Systems that use CDSs to connect TS/SCI must comply with DNI Policy and guidance. This difference in authorities between the Intelligence Community (IC) and the rest of the DoD components causes variation in the CDS approval processes.

6. Intelligence Community Directive (ICD) Number 503

The Intelligence Community's IT system security risk management is covered by Intelligence Community Directive Number 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation" (Office of the Director of National Intelligence, 2008, p. 1). This ICD applies to:

> the IC, as defined by the National Security Act of 1947, as amended, and other departments or agencies that may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned as an element of the IC. (Office of the Director of National Intelligence, 2008, p. 1).

ICD 503 states that it, "focuses on a more holistic and strategic process for the risk management of [IT] systems, and on processes and procedures designed to develop trust across the intelligence community [IT] enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions" (Office of the Director of National Intelligence, 2008, p. 1). Reciprocity is certainly emphasized in this directive. In regard to reciprocity, it states that, "[a]n IC element shall accept the certification of a system or other item of [IT] by another IC element without requiring or requesting any additional validation or verification testing of the system or item of IT" (Office of the Director of National Intelligence, 2008, p. 7).

Though the DAAPM streamlines reciprocity for DoD components (governing non-TS/SCI systems), it never mandates that any DoD element *shall* accept the certification of a system completed by another DoD element. The IC's requirement for IC elements to

accept certification from other IC elements stands in stark contrast to the non-TS/SCI DoD component's guideline provided by the DAAPM.

7. Defense Information Systems Network (DISN) Connection Process Guide (CPG)

The CPG implements DISA's requirement to oversee and maintain the connection approval process, as detailed in DoDI 8500.01 (DoD Chief Information Officer, 2019b, p. 16). It governs DISN connection approvals for all DoD components.

D. MAJOR STANDARDS BODIES AND ENTITIES INVOLVED IN THE RMF PROCESS

At the end of each approval step, CDS documentation is reviewed by the Cross Domain Technical Advisory Board (CDTAB). The CDTAB feeds its recommendations at each step to the Defense Information Assurance (IA)/Security Accreditation Working Group (DSAWG). The DSAWG's stamp of approval between each step is required prior to entering the next step.

(1) Cross Domain Support Element (CDSE)

The CDSE is responsible for managing the DoD component's CD-related activities (DoD Chief Information Officer, 2017c, p. 46). The DoDI 8540.01 also states that the CDSE is responsible for knowing what CDSs are listed on the NCDSMO list, and what capabilities the CDSs provide. The CDSE will work closely with the DoD components throughout the entire RMF process to ensure they are aware of the documentation and guidance and procedures entailed with the RMF process (DoD Chief Information Officer, 2017a, p. 33).

(2) CDTAB

Under the authority, direction, and control of the DoD ISRMC and DSAWG, the CDTAB serves as a technical advisory board to the DSAWG and provides CDS selection recommendations, along with CDS security impact to the DoDIN, if applicable (DoD Chief Information Officer, 2017a, p. 45).

(3) DSAWG

Under the authority, direction, and control of the DoD ISRMC, the DSAWG is the first accreditation or accreditation review level for the transport, network management, and network segments of the Defense Information Systems Network (DISN) for the Department of Defense Information Networks (DoDIN) (Defense Information Systems Agency, 2020a, p. 1). The DSAWG makes connection approval recommendations to the DoD Information Security Risk Management Committee (ISRMC), and also oversees and provides guidance to the CDTAB (Defense Information Systems Agency, 2020a, p. 1).

The DSAWG is composed of representatives from the following organizations: a DSAWG Chair (non-voting, provided by DISA), Defense Intelligence Agency (DIA), Defense Information Systems Agency (DISA), Joint Staff (JS), National Security Agency (NSA)/Central Security Service (CSS), Service Representatives (U.S. Army, U.S. Navy, U.S. Marine Corps, U.S. Air Force), DoD Chief Information Officer (DoD CIO), U.S. Strategic Command (USSTRATCOM), National Cross Domain Services Management Office (NCDSMO), Under Secretary of Defense for Intelligence (USD(I)), Director of National Intelligence Chief Information Office (DNI CIO), and Deputy Chief Management Office (DCMO) (Defense Information Systems Agency, 2020b, p. 1).

(4) DoD ISRMC

The ISRMC holds the final risk decision authority for DISN connections, and it may choose to delegate that responsibility to DSAWG for an enterprise CD service or CDS (DoD Chief Information Officer, 2017a, p. 44). It oversees the CDS approval process and provides guidance to the DSAWG and CDTAB. Additionally, it receives recommendations from the DSAWG regarding disconnection or disapproval of a CDS (Defense Information Systems Agency, 2020a, p. 1).

(5) AO

The AO authorizes a CDS to operate based on agreed security controls and acceptance of risk. The AO’s authorization is required prior to final DoD ISRMC or DSAWG CDS approval (DoD Chief Information Officer, 2017a, p. 50).

THIS PAGE INTENTIONALLY LEFT BLANK

SUPPLEMENTAL. JOINT ALL DOMAIN COMMAND AND CONTROL CROSS FUNCTIONAL TEAM (JADC2 CFT) ESTABLISHMENT

This FOUO supplemental describes the memorandum released to govern the formation of the JADC2 CFT. It describes its purpose, mission, charter, involved entities, and organization. It also describes All Domain Operations.

Those interested in viewing the supplementary file should contact the NPS Dudley Knox Library Restricted Collections Librarian rresources@nps.edu.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

AFWIC. (2020, March 15). *Cross-functional teams.* Retrieved from AFWIC: https://www.afwic.af.mil/Cross-Functional-Teams/

Air Force Lessons Learned. (2018). *Doolittle Series 18: Multi-domain operations.* Retrieved from Air University: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/LP_0003_Multi_Domain_Operations.pdf

Air Force Research Laboratory. (2016, July 8). *SecureView overview.* Retrieved from Air Force Research Laboratory: https://www.fbcinc.com/e/cdse/presentations/day2/10-SecureView_Overview_-_Capt_Alex_Gwin_-_FINAL_-_Day_2.pdf

Amazon Web Services. (2016, December). *Cross-domain solutions on AWS.* Retrieved from Amazon Web Services: https://d0.awsstatic.com/whitepapers/Security/cross-domain-solutions-on-aws.pdf

American National Standards Institute. (2019, January). *ANSI procedures for U.S. participation in the International Standards activities of ISO.* Retrieved from ANSI.org: https://share.ansi.org/ISOT/ANSI%20and%20ISO%20Procedures/ANSI%20International%20Procedures%202019.pdf

Anderson. (2018, December). *Chapter 9: Multilevel security.* Retrieved from University of Cambridge: https://www.cl.cam.ac.uk/~rja14/Papers/SEv3-ch9-dec18.pdf

Anderson, R. J. (2008). *Security engineering: A guide to building dependable distributed systems* (2nd ed.). Wiley. Retrieved from https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c08.pdf

Arxan. (2013, April 10). *SDK and App wrapping for mobile application management.* Retrieved from Arxan: https://www.arxan.com/arxan-blog/sdk-and-app-wrapping-for-mobile-application-management

Ausanka-Crues, R. (2006). *Methods for access control: Advances and limitations.* Retrieved from Harvey Mudd College: https://www.cs.hmc.edu/~mike/public_html/courses/security/s06/projects/ryan.pdf

Barnett, J. (2020, March 3). *Air Force wants to lead on JADC2 system to connect military domains.* Retrieved from FedScoop: https://www.fedscoop.com/air-force-jadc2-funding/

Bell, D. E., & LaPadula, L. J. (1973, November). *Secure computer systems: Mathematical foundations.* Springfield: National Technical Information Service. Retrieved from National Technical Information Service: https://apps.dtic.mil/sti/pdfs/AD0770768.pdf

Bell, D. E., & LaPadula, L. J. (1996). *MITRE technical report 2547.* Springfield: National Technical Information Service. Retrieved from http://web.a.ebscohost.com.libproxy.nps.edu/ehost/detail/detail?vid=0&sid=8f93bda1-86a6-4255-ac28-84d5c6a8628f%40sdc-v-sessmgr02&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db=bth&AN=1427144

Bell, D. E. (2005, December 7). *Looking back at the Bell-La Padula model.* Retrieved from Applied Computer Security Associates: https://www.acsac.org/2005/papers/Bell.pdf

Best, R. A. (2011, June 6). *Intelligence information: Need-to-know vs. need-to-share.* Retrieved from Congressional Research Service: https://fas.org/sgp/crs/intel/R41848.pdf

Ceranowicz, A., & Smith, S. (2020, May 10). *An alternative approach for distributed cross domain simulation solutions* . Retrieved from Simulation Interoperability Standards Organization: https://www.sisostds.org/DesktopModules/Bring2mind/DMX/API/Entries/Download?Command=Core_Download&EntryId=41459&PortalId=0&TabId=105

Clark, C. (2020, February 18). *All-domain operations*. Retrieved from Breaking Defense: https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations/

Cohen, R.S. (2018, December 19). *MDC2 wargame spurs Air Force to shift budget, experimentation priorities.* Retrieved from Inside Defense: https://insidedefense.com/daily-news/mdc2-wargame-spurs-air-force-shift-budget-experimentation-priorities

Cohen, R. S. (2019, April 15). *Moving MDC2 from research to reality.* Retrieved from Air Force Magazine: https://www.airforcemag.com/article/Moving-MDC2-from-Research-to-Reality/

Committee on National Security Systems. (2015, April 6). *Committee on national security systems instruction 4009.* Retrieved from Committee on National Security Systems: www.cnss.gov/CNSS/issuances/Instructions.cfm

Committee on National Security Systems. (2016, May 6). *Committee on national security systems: Meeting current and future threats*. Retrieved from Committee on National Security Systems: https://www.cnss.gov/cnss/

Conrad, E., Misenar, S., & Feldman, J. (2010). *CISSP study guide.* Amsterdam: Elsevier. Retrieved from https://books.google.com/books?id=-smPM3SodNUC&q=computer#v=snippet&q=computer&f=false

Conrad, E., Misenar, S., & Feldman, J. (2016). *CISSP study guide.* Amsterdam: Elsevier. Retrieved from https://manpreetstorage.files.wordpress.com/2016/07/cissp-study-guide-3ed-2016-eric-conrad.pdf

Crabtree, M. S., & Ianni, J. D. (2014). *Survey of collaboration technologies in nulti-level security environments.* Wright-Patterson Air Force Base: Air Force Research Laboratory. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a604086.pdf

Cronk, T. M. (2019, February 12). *DoD unveils its artificial intelligence strategy.* Retrieved from U.S. Department of Defense: https://www.defense.gov/Explore/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/

Cyber Security and Information Systems Information Analysis Center. (2020, June 2). Retrieved from Cyber Security and Information Systems Information Analysis Center: https://www.csiac.org/reference-doc/?orderby=date&search=data&order=asc

Defense Information Systems Agency. (2020a, April 21). *DSAWG authority and responsibility*. Retrieved from Defense Information Systems Agency: https://www.disa.mil/Network-Services/Enterprise-Connections/DSAWG/Authority-and-Responsibility

Defense Information Systems Agency. (2020b, April 21). *Enterprise connections FAQ - DSAWG*. Retrieved from DoD Cyber Exchange Public: https://public.cyber.mil/connect/faq-dsawg/

Defense Standardization Program Office. (2020, March 28). *DoD information technology standards registry (DISR)*. Retrieved from Defense Standardization Program: https://www.dsp.dla.mil/Specs-Standards/List-of-DISR-documents/

Denning, D. E. (1976, May 01). A lattice model of secure information flow. *ACM Digital Library, 19*(5).

Deputy Secretary of Defense. (2018, June 22). *DoD cloud update.* Retrieved from Office of the Secretary of Defense: https://federalnewsnetwork.com/wp-content/uploads/2018/07/062218_shanahan_deasy_memo.pdf

Director of Administration and Management. (2006, July 25). *DoDD 5105.19.* Retrieved from Executive Services Directorate: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510519p.pdf

DoD Chief Information Officer. (2019, February 12). *Summary of the 2018 Department of Defense artificial intelligence strategy.* Retrieved from Executive Services Directorate: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DoD-AI-STRATEGY.PDF

DoD Chief Information Officer. (2017a, July 28). *Risk management framework (RMF) for DoD information technology (IT)* . Retrieved from Executive Services Directorate: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300

DoD Chief Information Officer. (2017b, July 31). *DoDI 8310.01: Information technology standards in the DoD, incorporating change 1.* Retrieved from Executive Services Directorate: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/831001p.pdf

DoD Chief Information Officer. (2017c, August 28). DoDI 8540.01: *Cross domain policy.* Retrieved from Executive Services Directorate: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/854001p.pdf

DoD Chief Information Officer. (2019a, August 12). *DoD enterprise DevSecOps reference design.* Retrieved from DoD Chief Information Officer: https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf?ver=2019-09-26-115824-583

DoD Chief Information Officer. (2019b, October 7). *DoDI 8500.01: Cybersecurity.* Retrieved from Executive Services Directorate: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

Erwin, S. I. (2013, March 1). *Defense, intelligence agencies struggle to unify data networks.* Retrieved from National Defense: https://www.nationaldefensemagazine.org/articles/2013/2/28/2013march-defense-intelligence-agencies-struggle-to-unify-data-networks-updated

Ford Aerospace and Communications Development. (1981, August). *Secure minicomputer operating system final report.* Retrieved from Defense Technical Information Centr: https://apps.dtic.mil/dtic/tr/fulltext/u2/a111566.pdf

Galbraith, J. R. (2020, May 16). *The star model.* Retrieved from Jay Galbraith: https://www.jaygalbraith.com/images/pdfs/StarModel.pdf

Gewirtz, D. (2019, April 8). *Windows, Mac, or Linux? We compare the pros and cons of these computing platforms.* Retrieved from ZD Net: https://www.zdnet.com/article/windows-mac-or-linux-we-compare-the-pros-and-cons-of-these-computing-platforms/

Greene, T. (2019, December 29). *Report: Palantir took over Project Maven, the military AI program too unethical for Google*. Retrieved from The Next Web: https://thenextweb.com/artificial-intelligence/2019/12/11/report-palantir-took-over-project-maven-the-military-ai-program-too-unethical-for-google/

Hitchens, T. (2020, February 11). *Air Force cuts aircraft to fund space, multi-domain.* Retrieved from Breaking Defense: https://breakingdefense.com/2020/02/air-force-cuts-aircraft-to-fund-space-multi-domain/

IBM. (2020, May 18). *Characteristics of a multilevel-secure environment*. Retrieved from IBM: https://www.ibm.com/support/knowledgecenter/SSLTBW_2.4.0/com.ibm.zos.v2r4.icha700/charmls.htm

Insinna, V. (2019, December 20). *The Air Force just conducted the first test of its Advanced Battle Management System.* Retrieved from C4ISRNet: https://www.c4isrnet.com/air/2019/12/21/the-air-force-just-conducted-the-first-test-of-its-advanced-battle-management-system/

Insinna, V. (2020, March 18). *Coronavirus pandemic (temporarily) derails the Air Force's Advanced Battle Management System program.* Retrieved from C4ISRNET: https://www.c4isrnet.com/c2-comms/2020/03/18/the-coronavirus-pandemic-has-temporarily-derailed-the-air-forces-advanced-battle-management-system-program/

International Committee of the Red Cross. (2011, January 1). *The relevance of IHL in the context of terrorism.* Retrieved from International Committee of the Red Cross: https://www.icrc.org/en/doc/resources/documents/faq/terrorism-ihl-210705.htm

International Electrotechnical Commission. (2020, April 23). *Publicly available specifications*. Retrieved from International Electrotechnical Commission: https://www.iec.ch/standardsdev/publications/pas.htm

International Organization for Standardization. (2020a, March 15). *ISO deliverables*. Retrieved from International Organization for Standardization: https://www.iso.org/deliverables-all.html

International Organization for Standardization. (2020b, April 5). *About us: Members*. Retrieved from International Organization for Standardization: https://www.iso.org/members.html?m=MB

International Organization for Standardization. (2020c, April 5). *About us: Structure and governance*. Retrieved from International Organization for Standardization: https://www.iso.org/structure.html

International Organization for Standardization. (2020d, April 5). *Member: ANSI United States*. Retrieved from International Organization for Standardization: https://www.iso.org/member/2188.html

International Organization for Standardization. (2020e, April 5). *New work item proposals*. Retrieved from International Organization for Standardization: https://isotc.iso.org/livelink/livelink?func=ll&objId=8913253&objAction=browse&viewType=1

International Organization for Standardization. (2020f, April 5). *Standards*. Retrieved from International Organization for Standardization: https://www.iso.org/standards.html

International Organization for Standardization. (2020g, April 5). *Who develops standards: Technical committees*. Retrieved from International Organization for Standardization: https://www.iso.org/technical-committees.html?s=INFORMATION_PROCESSING_GRAPHICS

International Organization for Standardization. (2020h, April 5). *Certification and conformity*. Retrieved from International Organization for Standardization: https://www.iso.org/certification.html

Irvine, C. E., & Nguyen, T. D. (2006, August). *An analysis of three kernel-based multilevel security architectures.* Retrieved from Calhoun: The NPS Institutional Archive: https://calhoun.nps.edu/bitstream/handle/10945/511/NPS-CS-06-001.pdf?sequence=1&isAllowed=y

Ismail, M. A., Senousy, M. B., & Aboelseoud, H. (2014, July). An investigation into access control in various types of operating systems. *International Journal of Computer Applications, 98*(10), p. 11.

ISO/ETC JTC 1. (2013, November). *JTC 1 strategic business plan*. Retrieved from International Organization for Standardization: https://isotc.iso.org/livelink/livelink?func=ll&objId=8913375&objAction=browse

ISO/IEC JTC 1 Subcommittees. (2019). *2019 business plans*. Retrieved from International Organization for Standardization: https://isotc.iso.org/livelink/livelink?func=ll&objId=20752181&objAction=browse&viewType=1

Jansen, E., Gallenson, A. C., & Higgins, S. L. (2015, March). *Integrating energy efficiency into Navy culture: an organizational design approach.* Retrieved from Calhoun: The NPS Institutional Archive: http://hdl.handle.net/10945/48170

KeySoft Systems. (2020, April 5). *JCDX*. Retrieved from KeySoft: www.keysoftsys.com/jcdx.html

Koelsch, B. (2013). *Solving the cross-domain conundrum.* Retrieved from Defense Technical Information Center: https://apps.dtic.mil/sti/pdfs/ADA589325.pdf

Konkel, F. (2018, June 21). *NSA 'systematically moving' all its data to the cloud.* Retrieved from Next Gov: https://www.nextgov.com/emerging-tech/2018/06/nsa-systematically-moving-all-its-data-cloud/149179/

Kundra, V. (2010, December 9). *25 point implementation plan to reform federal information tehnology management.* Retrieved from Department of Homeland Security: https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf

L3Harris. (2020, May 13). *Mission processing.* Retrieved from L3Harris: https://www.harris.com/solution/mission-processing

Levin, T. E., Irvine, C. E., & Nguyen, T. D. (2006, August). *An analysis of three kernel-based multilevel security architectures.* Retrieved from Calhoun: The NPS Institutional Archive Space Repository: https://calhoun.nps.edu/bitstream/handle/10945/511/NPS-CS-06-001.pdf?sequence=1&isAllowed=y

Lunt, T. F., Denning, D. E., Schell, R. R., Heckman, M., & Schockley, W. R. (1990). The SeaView security model. *IEEE Transactions on Software Engineering*, 593–607.

Mattis, J. (2018). *2018 national defense strategy.* Retrieved from Department of Defense: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Maucione, S. (2020, January 21). *Air Force using agile approach to connect systems for battle.* Retrieved from Federal News Network: https://federalnewsnetwork.com/air-force/2020/01/air-force-using-agile-approach-to-connect-systems-for-battle/

McCaskill, L., Hicks, R., & Kmorowski, I. (2020, June 1). *JCIDS DoDAF architecture primitives to assemble a repository for enterprise-wide analysis and decision-making*. Retrieved from DoD CCRP: http://www.dodccrp.org/events/12th_ICCRTS/CD/html/papers/100.pdf

Microsoft. (2020, May 4). *Learn about sensitivity labels.* Retrieved from Microsoft Documentation: https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

National Bureau of Standards. (1982, May 24). *Proceedings of the fifth seminar on the DoD computer security initiative.* Retrieved from National Institute for Standards and Technology: https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1982/05/24/proceedings-5th-seminar-dod-computer-security-initiative/documents/1982-5th-seminar-proceedings.pdf

National Cross Domain Strategy and Management Office. (2019, June 5). *Development & deployment timeline requirements for the cross domain solution (CDS) design and implementation requirements:*. Retrieved from National Cross Domain Strategy and Management Office: https://intelshare.intelink.gov/sites/ncdsmo/_layouts/15/WopiFrame.aspx?sourcedoc=/sites/ncdsmo/Shared%20Documents/CDS%20Development%20Guidance%20and%20Software/Raise%20the%20Bar%20(RTB)/NCDSMO-R-00012-001_00.pdf&action=default#

National Cross Domain Strategy and Management Office. (2020, April 7). *Cross domain solution (CDS) design and implementation requirements.* Retrieved from National Cross Domain Strategy and Management Office: https://intelshare.intelink.gov/sites/ncdsmo/_layouts/15/start.aspx#/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fncdsmo%2FShared%20Documents%2FCDS%20Development%20Guidance%20and%20Software%2FRaise%20the%20Bar%20%28RTB%29&FolderCTID=0x0120

National Industrial Security Program Authorization Office. (2020, March 9). *Defense counterintelligence and security agency assessment and authorization process manual.* Retrieved from Defense Counterintelligence and Security Agency: https://www.dcsa.mil/Portals/91/Documents/CTP/tools/DCSA_Assessment_and_%20Authorization_Process_Manual_Version_2.1.pdf

National Security Agency. (2020, May 18). *SELinux frequently asked questions (FAQ).* Retrieved from NSA.gov: https://www.nsa.gov/What-We-Do/Research/SELinux/FAQs/

Norquist, D. L. (2019, July 12). *DoD digital modernization strategy.* Retrieved from Department of Defense : https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DoD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF

NSWCDD Corporate Communications. (2019, November 26). *Microsoft tactical vehicle takes center stage at NSWC Dahlgren innovation day.* Retrieved from Naval Sea Systems Command: https://www.navsea.navy.mil/Media/News/SavedNewsModule/Article/2027626/microsoft-tactical-vehicle-takes-center-stage-at-nswc-dahlgren-innovation-day/

Office of the Chief of Naval Operations. (2018, July 18). *OPNAV Instruction 5239.1D: U.S. Navy cybersecurity program*. Retrieved from Office of the Chief of Naval Operations: https://fas.org/irp/doddir/navy/opnavinst/5239_1d.pdf

Office of the Director of National Intelligence. (2008, September 15). *Intelligence community directive number 503: Intelligence community information technology systems security risk management, certification and accrediation.* Retrieved from https://www.dni.gov/files/documents/ICD/ICD_503.pdf

Office of the Director of National Intelligence. (2020, March 15). *About the ISE*. Retrieved from DNI.Gov: https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/about-the-ise

Ong, K. L., Nguyen, T., & Irvine, C. (2008, April 1). *Implementation of a multilevel wiki for cross-domain collaboration.* Retrieved from Calhoun: The NPS Institutional Archive: https://calhoun.nps.edu/bitstream/handle/10945/7166/08paper_wiki_iciw.pdf?sequence=1&isAllowed=y

Phillips, C. E., Ting, T., & Demurjian, S. A. (2020, May). *Information sharing and security in dynamic coalitions.* Retrieved from Princeton website: http://www.princeton.edu/~rblee/ELE572Papers/p87-phillips.pdf

Raytheon. (2007). Raytheon secure systems and networks: Delivering mission assurance in a hostile cyberspace. *Technology Today*, 8.

Reagan, Ronald. (1981, December 4). *Executive order number 12333.* Retrieved from Central Intelligence Agency: https://www.archives.gov/federal-register/codification/executive-order/12333.html

Reed, N. (2004, September). *Security guards for the future web.* Retrieved from MITRE Technical Reports: https://www.mitre.org/sites/default/files/pdf/05_0166.pdf

Research, Development, Test & Evaluation, Navy. (2013, April). *PB 2014 Navy.* Retrieved from Tactical Command System - MIP Navy: https://www.globalsecurity.org/military/library/budget/fy2014/navy-peds/0304231n_5_pb_2014.pdf

Rjaibi, W., & Bird, P. (2004, August 31). A multi-purpose implementation of mandatory access control in relational database management systems. *Proceedings of the Thirtieth international conference on Very large data bases, 30*, 1010–1020. Retrieved from ACM Digital Library: https://dl.acm.org/doi/10.5555/1316689.1316776

Rome, J. A., & Tolliver, J. S. (2020, May 10). *Multilevel architectures for electronic document retrieval.* Retrieved from Oak Ridge National Library: https://web.ornl.gov/~romeja/baltsec.pdf

Saltzman, B. G. (2018). *MDC2 overview.* Retrieved from Mitre: https://www.mitre.org/sites/default/files/publications/Special-Presentation-Gen%20Chance-Saltzman%20MDC2%20Overview%20for%20MITRE-June-2018.pdf

Schmidt, E. (2018, April 17). *Statement of Dr. Eric Schmidt.* Retrieved from U.S. House of Representatives Document Repository: https://docs.house.gov/meetings/AS/AS00/20180417/108132/HHRG-115-AS00-Wstate-SchmidtE-20180417.pdf

Schneiderman, R. (2015). Modern standardization: Case studies at the crossroads of technology, economics, and politics. *The Institute of Electrical and Electronics Engineers, Inc*(First Edition), 253–267. Retrieved from Wiley Online Library: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119043492.oth#article__content

Secretary of the Air Force Public Affairs. (2019, December 23). *Air Force, Navy, Army conduct first 'real world' test of Advanced Battle Management System.* Retrieved from U.S. Air Force Webpage: https://www.af.mil/News/Article-Display/Article/2046531/air-force-navy-army-conduct-first-real-world-test-of-advanced-battle-management/

Senate and House of Representatives. (2020, January 30). *National security act of 1947.* Retrieved from Legal Counsel: https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947

Shanahan, P. (2018a, September 19). *Remarks By Deputy Secretary Shanahan at the Air Force Association's Air, Space and Cyber Conference.* Retrieved from U.S. Department of Defense : https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1639948/remarks-by-deputy-secretary-shanahan-at-the-air-force-associations-air-space-an/

Shanahan, P. (2018b, December). *DoD cloud strategy.* Retrieved from Department of Defense: https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DoD-CLOUD-STRATEGY.PDF

Sirota, S. (2020, February 7). *Norquist directs establishment of JADC2 cross functional team.* Retrieved from Inside Defense: https://insidedefense.com/daily-news/norquist-directs-establishment-jadc2-cross-functional-team

SPAWAR. (2016, April 20). *JCDX UCDSMO CDTF brief.* Retrieved from Intelink: https://intelshare.intelink.gov/sites/ucdsmo/_layouts/15/WopiFrame.aspx?sourcedoc=/sites/ucdsmo/SiteCollectionDocuments/Cross%20Domain%20Technical%20Forum%20(CDTF)%20Apr%202016/JCDX_UCDSMO_CDTF_Brief_APR_2016.pptx&action=default

Special Access Program Office. (2016, April 11). *Department of Defense joint special access program implementation guide*. Retrieved from Defense Security Cooperation Agency: https://www.dcsa.mil/portals/91/documents/ctp/nao/JSIG_2016April11_Final_(53Rev4).pdf

Taylor, D. (2018, February 6). *Why Linux is better than Windows or macOS for security.* Retrieved from Computer World: https://www.computerworld.com/article/3252823/why-linux-is-better-than-windows-or-macos-for-security.html

Tipton, H. F., & Nozaki, M. K. (2010). *Information security management handbook* (6 ed., Vol. 4). New York: Auerbach Publications.

Underwood, K. (2019, December 16). *Joint command and control comes out of the shadows.* Retrieved from AFCEA: https://www.afcea.org/content/joint-command-and-control-comes-out-shadows

Weissman, C. (1992). BLACKER: Security for the DDN examples of A1 security engineering trades. *Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy*, 286–292. Retrieved from IEEE: https://ieeexplore-ieee-org.libproxy.nps.edu/stamp/stamp.jsp?tp=&arnumber=213253

Wilson, B., Porche, I. R., Eisman, M., Nixon, M., Tierney, S., Yurchak, J., . . . Critelli, S. (2016). *Maritime tactical command and control analysis of alternatives.* Santa Monica: RAND Corporation.

World Standards Cooperation. (2020, April 5). *World standards cooperation: About*. Retrieved from World Standards Cooperation: https://www.worldstandardscooperation.org/about/

Yang, C.-Q. (2003, January). *Operating system security and secure operating systems.* Retrieved from Global Information Assurance Certification Papers: https://www.giac.org/paper/gsec/2776/operating-system-security-secure-operating-systems/104723

Yates, J., & Murphy, C. N. (2019). *Engineering rules: Global standard setting since 1880.* Baltimore: John Hopkins University Press.

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