NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

OFFICER DATA CARD (ODC) DISSEMINATION POLICY, MODEL, AND BLOCKCHAIN-BASED ACCOUNTABILITY MECHANISM

by

Brett Gentile

June 2018

Thesis Advisor: Cynthia E. Irvine
Second Reader: Theodore D. Huffmire

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 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE OFFICER DATA CARD (ODC) DISSEMINATION POLICY, MODEL, AND BLOCKCHAIN-BASED ACCOUNTABILITY MECHANISM	**5. FUNDING NUMBERS**
6. AUTHOR(S) Brett Gentile	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

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

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The Officer Data Card (ODC) is an automated record that provides up-to-date data about U.S. Navy officers for use in detailing and promotion boards. Policy regarding ODCs requires controlled access and dissemination of ODC information. A better understanding of the policies associated with ODCs could allow current technologies to be employed to support their use and management. This work builds a model for ODC dissemination based on current policies and practices. A process model is built to describe controlled dissemination of ODCs during specific promotion board processes. It is found that the dissemination policies and model for ODCs have a strong similarity to those applied to ORCON-labeled information handled by the intelligence community. With the threat of unauthorized dissemination of ODCs in mind, a blockchain solution is proposed for auditing the access to and modification of ODCs. The proposed solution is a distributed auditing mechanism that does not rely on a central auditing server. The proposed blockchain solution is analyzed and determined to be able to provide accountability for record handling processes and ODC dissemination but does not provide enough new functionality or efficiency beyond that possible through intensive central audit logging.

14. SUBJECT TERMS personnel records, ODC, originator control, ORCON, dissemination control, access control, integrity, accountability, audit, OMPF, blockchain, distributed ledger	**15. NUMBER OF PAGES** 91
	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.

OFFICER DATA CARD (ODC) DISSEMINATION POLICY, MODEL, AND BLOCKCHAIN-BASED ACCOUNTABILITY MECHANISM

Brett Gentile
Ensign, United States Navy
BS, United States Naval Academy, 2017

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 2018

Approved by: Cynthia E. Irvine
Advisor

Theodore D. Huffmire
Second Reader

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Officer Data Card (ODC) is an automated record that provides up-to-date data about U.S. Navy officers for use in detailing and promotion boards. Policy regarding ODCs requires controlled access and dissemination of ODC information. A better understanding of the policies associated with ODCs could allow current technologies to be employed to support their use and management. This work builds a model for ODC dissemination based on current policies and practices. A process model is built to describe controlled dissemination of ODCs during specific promotion board processes. It is found that the dissemination policies and model for ODCs have a strong similarity to those applied to ORCON-labeled information handled by the intelligence community. With the threat of unauthorized dissemination of ODCs in mind, a blockchain solution is proposed for auditing the access to and modification of ODCs. The proposed solution is a distributed auditing mechanism that does not rely on a central auditing server. The proposed blockchain solution is analyzed and determined to be able to provide accountability for record handling processes and ODC dissemination but does not provide enough new functionality or efficiency beyond that possible through intensive central audit logging.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. OBJECTIVES....1
B. RELEVANCE TO THE DEPARTMENT OF DEFENSE....2
C. THESIS ORGANIZATION....2

II. BACKGROUND AND EXISTING WORK....5
A. NAVY PERSONNEL RECORDS....5
1. Record Types....5
2. Construction of Underlying Database....6
3. Digital Record Storage....7
4. Record Access and Maintenance....7
5. Record Usage....7
6. Record Privacy....8
B. ORIGINATOR CONTROLLED INFORMATION DISSEMINATION....8
1. History of ORCON Models....9
2. ORCON Usage Example....10
C. BLOCKCHAIN TECHNOLOGY....11
1. History and Origin....12
2. Blockchain Characteristics and Features....14
D. SUMMARY....18

III. PERSONNEL RECORD MANAGEMENT SCENARIOS....19
A. OVERVIEW OF PROMOTION BOARD PROCESS....19
B. RECORD HANDLING IN STATUTORY PROMOTION BOARDS....22
C. STEPS FOR CORRECTING ODC INFORMATION....25
1. Determination....25
2. Request....25
3. Admittance....26
4. Resolution....26
D. CONSTRUCTING THE SCENARIOS....27
1. Scenarios....27
2. Variables....27
3. Desired Outcomes....28
E. SUMMARY....28

IV. THREAT MODEL....31
A. ASSET EVALUATION....31
1. Confidentiality....31
2. Integrity....32
3. Availability....32
B. ADVERSARY EVALUATION....32
1. Intentional Outsider....33
2. Unintentional Outsider....33
3. Intentional Insider....33
4. Unintentional Insider....34
C. MOST RELEVANT THREAT....34

V. ODC ORCON PROCESS MODEL....37
A. OVERVIEW AND DEFINITIONS....37
1. Access Control Overview....38
2. Rules and Terminology....38
B. ODC OBJECT CREATION....42
C. CREATION OF COPIES OF ODC FOR PROMOTION BOARD USE....44
D. MODIFICATION OF ODC WHILE IN USE BY PROMOTION BOARD....46
1. Determination of Missing or Incorrect Information....46
2. Request for Records....47
3. Admittance of Records....50
4. Resolution....51
E. SUMMARY....51

VI. BLOCKCHAIN USE CASE ANALYSIS....53
A. THE VALUE OF AUDITING....53
B. BLOCKCHAIN AUDIT MECHANISM....54
1. Type of Blockchain Used....55
2. Transactions....56
3. Consensus....56
4. Software Suite....58
C. ANALYSIS OF BLOCKCHAIN APPLICABILITY....58
1. Desired Outcome Analysis....58
2. Scalability and Throughput....60
3. Comparison....61
4. Recommendation....63
D. SUMMARY....64

VII. CONCLUSION 67
A. SUMMARY 67
B. RECOMMENDATIONS FOR FUTURE WORK 68
1. Implementation of Proposed Solution 68
2. Additional Use Case Studies 68

LIST OF REFERENCES 69

INITIAL DISTRIBUTION LIST 73

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Example ODC 6

Figure 2. ORCON Usage Example Diagram. Source: [15]. 10

Figure 3. Hype Cycle for Emerging Technologies (August 2017): Source: [20]. 12

Figure 4. Example Merkle Tree. Source: [22] 13

Figure 5. Blockchain Hash Pointer Usage. Source: [22] 14

Figure 6. Distributed Nature of Blockchain 16

Figure 7. Immutable Nature of Blockchain. Source: [16]. 17

Figure 8. Example Board Membership Memorandum. Source: [32]. 21

Figure 9. Physical and Network Segmentation of Promotion Board Spaces 23

Figure 10. Abstract Object Construction 39

Figure 11. Example ACL for ODC Object 41

Figure 12. Creation of ODC Object 43

Figure 13. ODC Object Setup for Board 45

Figure 14. State of ODC at Determination of Need for Modification 47

Figure 15. Orcon Process for Request for Record from Office 48

Figure 16. Orcon Process for Request of Record from Officer 49

Figure 17. Corrected State of ODC 50

Figure 18. Example Blockchain Audit Mechanism Usage 59

Figure 19. ODC vs. Bitcoin Throughput Comparison [38] 61

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACL	Access Control List
BUPERS	Bureau of Naval Personnel
CAC	Common Access Card
CNPC	Commander Naval Personnel Command
DAC	Discretionary Access Control
DoD	Department of Defense
DOPMA	Defense Officer Personnel Management Act
e-Sub	Electronic Submission
EMPRS	Electronic Military Personnel Record System
FOUO	For Official Use Only
MAC	Mandatory Access Control
NMCI	Navy Marine Corps Intranet
NPDB	Navy Personnel Database
NPRC	National Military Personnel Records Center
NSIPS	Navy Standard Integrated Personnel System
O-4	Lieutenant Commander
ODC	Officer Data Card
OMPF	Official Military Personnel File
OOD	Officer of the Deck
ORAC	Originator Controlled Access Control
Orcon	Originator-Controlled (not to be confused with the intelligence community term: ORCON)
OSR	Officer Summary Record
PERS	Navy Personnel Command
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
SAAR-N	System Authorization Access Request Navy
SF-180	Standard Form 180
SOP	Standard Operating Procedures
TDY	Temporary Duty

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my advisor, Dr. Cynthia Irvine, for her guidance and support in making this research meaningful and insightful. Your mentorship was vital in the journey through the thesis research and writing process. I would also like to thank my second reader, Dr. Ted Huffmire, for his insight and assistance in the editing of this thesis.

I would like to express thanks and gratitude to CAPT Good for supporting this research. The hours spent in your office and the conversations through email and in passing aided tremendously in shaping the research. Your dedication to the success of others and encouraging spirit are traits I hope to emulate in my leadership.

I would like to thank the U.S. Naval Academy for the appointment as a Bowman Scholar and the opportunity to complete a master's degree at the Naval Postgraduate School. The program has enabled me to continue in the educational foundation laid in Annapolis and build lasting friendships and professional networks for the future.

Finally, and most importantly, I would like to thank my family and friends for their unwavering support throughout this process. Your constant words of encouragement and patience inspire and motivate me to work hard and be a better man, son, brother, and friend.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The Officer Data Card (ODC) is an automated record that provides up-to-date data about U.S. Navy officers for use in detailing and promotion boards. Policy regarding ODCs requires controlled access and dissemination to ODC information. Because ODCs are used in various U.S. Navy personnel processes and contain the personal data of the officer, they should reflect the most current and accurate data of the officer. While there are overarching policies regarding the use and handling of personnel record information in general, ODCs are handled and used in unique ways for promotion boards and other specific processes.

Blockchain technology has gathered the immense interest of cybersecurity researchers, companies and organizations seeking new, potentially disruptive technologies to improve their cybersecurity posture. A possible application of blockchain technology is in the handling of U.S. Navy personnel records. This work explores the policies related to ODCs and investigates the merit of blockchain technology in the context of promotion boards and discusses how blockchain technology could be used as part of an audit mechanism to support policies related to ODC dissemination.

A. OBJECTIVES

There are two primary objectives of this work. The first is to build a model for ODC dissemination during the process of statutory promotion boards for U.S. Navy officers. No model describing the access control policy for this process exists. This work aims to take governing guidelines, policies, procedures, and best practices and create a technical model for access control for personnel records during the process of statutory promotion boards when records need to be corrected.

The second objective is to provide a useful case study of a possible application blockchain technology. Given the lack of proven use cases for blockchain technology, this work aims to build a blockchain solution as an auditing mechanism in support of policy enforcement of ODC access and dissemination. Building a blockchain solution

will permit critical analysis of the use of blockchain technology within the context of record keeping and audit logging in support of ODC access and dissemination policies.

B. RELEVANCE TO THE DEPARTMENT OF DEFENSE

The Department of Defense (DoD) strives to maintain a critical military advantage and stay on the cutting edge of technologies. Information assurance and cybersecurity are two categories of research and development that the DoD is interested in and provides funding for the research and development. Personnel record information, including the ODC, is required by governing authorities and policies to have access and dissemination control [1]. In 2017, the National Defense Authorization Act for Fiscal Year 2018 was passed and included funding for the cyber application of blockchain technology [2]. Accountability policies pertain to the linkage between individuals or groups of individuals and the processes that act on their behalf. An essential requirement for accountability is a reliable audit mechanism. One potential avenue for blockchain applications within the DoD is to use blockchain technology as an audit mechanism to support accountability policy enforcement of personnel record information. Blockchain technology can provide integrity to an audit mechanism which can be used to hold users accountable while handling and maintaining ODCs and other personnel record information.

C. THESIS ORGANIZATION

This work consists of five chapters: Introduction (Chapter I), Background and Existing Work (Chapter II), Personnel Record Management Scenarios (Chapter III), Threat Model (Chapter IV), ODC Orcon Process Model (Chapter V), Blockchain Use Case Analysis (Chapter VI), and Conclusion (Chapter VII).

Chapter I outlines the problem and states the objectives of this work. It provides an overview of the motivation, objectives, and benefits to DoD of the research conducted. Finally, it describes the overall flow of the work and its organization.

Chapter II briefly covers three topics: U.S. Navy personnel records, originator controlled access control, and blockchain technology. The personnel record system

section provides a brief overview of the record management process within the DoD and introduces the ODC, a record of specific interest to this work. The Orcon section gives a brief history of originator control over information distribution and provides a small example of its usage. The blockchain section gives a brief history of the new technology and defines characteristics of blockchain technology as they relate to this work.

Chapter III discusses the processes used in promotion boards for active duty officers in the U.S. Navy. We discuss the specifics of record handling within the context of statutory promotion boards. Finally, we construct two scenarios for the handling and modification of ODCs within the context of statutory promotion boards. The intent of the chapter is to reduce the problem space to working scenarios for use in subsequent chapters.

Chapter IV defines a threat model to ODC usage during the promotion board process defined in Chapter III. We evaluate the critical security aspects, i.e., confidentiality, integrity, and availability, of ODCs during the board process, and evaluate the ability of adversaries to degrade those assets. The intent of the chapter is to determine a most relevant threat to ODC policy and processes for use in subsequent chapters.

Chapter V builds a model for originator controlled access control for the scenarios constructed in Chapter III. The model tracks user and group access to specific records through the process of admitting new records into a promotion board as a result of incorrect or incomplete information provided at the beginning of the process. The intent of the chapter is to document the process for access control for ODCs within the promotion board process.

Chapter VI builds a blockchain solution to act as an audit mechanism model and attempts to counter an aspect of the defined threat modeled in Chapter IV. We conclude with an analysis of the blockchain solution and give recommendations for implementation and testing. The intent of the chapter is to explore the utility of blockchain technology within the context of controlled distribution of information.

Chapter VII concludes and summarizes the entirety of the work, and provides recommendations for future research to advance the knowledge and development of blockchain technology further.

II. BACKGROUND AND EXISTING WORK

The purpose of this chapter is to provide an overview of three topics that serve as the basis for this work. We start with a discussion on the personnel record management system for officers in the United States Navy. An introduction, history, and brief discussion of blockchain technology will then follow. Finally, an introduction to Originator Controlled (Orcon) dissemination is provided.

A. NAVY PERSONNEL RECORDS

All active duty U.S. Navy officers carry official records of their military careers. An ODC summarizes these records. The ODC serves as a single document that is the collection of the records of the U.S. Navy officer.

The ODC is generated by querying the Bureau of Naval Personnel (BUPERS) web interface [3]. BUPERS is an organization that serves to provide administrative leadership, policy planning, and general oversight of the Navy Personnel Command (PERS) [4]. Multiple databases that store individual records for a U.S. Navy officer connect to the BUPERS web interface. Querying these databases generates the ODC, extracting information necessary to fill all blocks in the ODC. There are a total of five offices in three locations where all subsidiary information is stored. Appendix E of NAVPERS 15839I details the specific offices that have ownership of, and are queried for information, of all blocks in the ODC [5]. The Navy Standard Integrated Personnel System (NSIPS) aggregates the necessary data from these offices to create an ODC. Figure 1 shows a portion of an ODC, as generated by the BUPERS web interface.

1. Record Types

There are a total of 110 blocks of information in the ODC. Examples of the information contained in the ODC for each U.S. Navy officer are personally identifiable information, education records, and information about dependents associated with the officer. The Manual of Navy Officer Manpower and Personnel Classifications, Volume II, The Officer Data Card details the exact information for all blocks in the ODC [5]. The

ODC does not contain all of the involved records in their entirety. Instead, only the necessary information is aggregated from the required records to generate the block of the ODC.

General Data

Name	YG	Date Processed	SSN	Designator	Date of Birth	Age	Prof. Serv. Date
DUFF DAVID GAVIN	95	090314	[redacted]	1310	[redacted]	35	

Promotion History

CAPT	CDR	LCDR	LT	LTJG	ENS	W-2
		041201	990601	970531	950531	

Current Duty

Present Duty Station Title	Present Billet Title
CNAVPERSCOM MILL	PERS DIST OFF/

Education - Formal (College)

College	Year	Level	Major	Minor
USNA	95	BACH/1PRO	NAV ARCH	

Sub-Specialty
5403Q

Figure 1. Example ODC

2. Construction of Underlying Database

ODCs are generated online through the BUPERS website [3]. Records are kept as original physical documents, scanned electronic copies, or digitally signed electronic copies, depending on the record. It is the responsibility of the officer, who acts as a trusted agent, to keep either the original or a copy of all records. This redundancy allows the officer to generate a new copy of a record, should it be missing from the database of each record holding office, or if the information reported by the office is incorrect. Verification of records is described in the Navy Personnel Command Electronic Submission Standard Operating Procedures (e-Sub SOP), Version 2.0 [6]. If the officer is not a trusted agent for a particular document, the officer must contact the trusted agent for the document and have the trusted agent provide a copy of the record on the officer's

behalf [6]. Complete details of the assignment of trusted agents are designated in the Navy Personnel Database (NPDB).

3. Digital Record Storage

Records are kept in multiple places and exist as either an original hard copy or an authentic, replicated digital copy. A single record is held by the originator of the record, the office that stores the record for use in a Navy officer's ODC, and may optionally be held personally by the Navy officer. Each record is stored in the Electronic Military Personnel Record System (EMPRS) at its designated digital storage location. Appendix E of NAVPERS 15839I [5] associates a record to the office that owns the record [7].

4. Record Access and Maintenance

ODCs are generated by BUPERS and are viewed by the U.S. Navy Officer, as well as personnel involved in detailing and selection boards for that officer. A Navy officer's ODC is available to view at any time online, and hard copies of an ODC can be generated, downloaded, and printed as well. Some of the ODC fields do not change throughout the officer's career, some are changed or appended to, and some fields are generated in the ODC at specific milestones in the officer's career. Examples of the last are rank, qualifications, and milestones during the officer's career.

Once the officer is discharged from military service, the records are retained in an archival database. Current U.S. Navy officers have their records transferred to the National Military Personnel Records Center (NPRC), in St. Louis, Missouri [8]. Access to these records by the veteran or next-of-kin at this point can only be obtained by filling out a Standard Form 180 (SF-180). The general public can also view redacted records under rules and guidelines of the Freedom of Information Act [9].

5. Record Usage

Personnel records are used for promotion, selection boards, billeting, pay, and benefits, and are run through the offices of the Navy Personnel Command and NSIPS. The Commander of Navy Personnel Command (CNPC) owns the ODC. A U.S. Navy officer can view his or her ODC and can request updates to the ODC. Detailers who work

for CNPC can view ODCs and make restricted updates to ODCs. The Privacy Act of 1974 and SECNAVINST 5211.5E are the policies that prohibit the unauthorized use or disclosure of official record information, including ODCs [1].

6. Record Privacy

Personnel records are protected under the Privacy Act of 1974 [10] because they contain personally identifiable information (PII). Records containing PII are marked For Official Use Only (FOUO) and therefore fall under the dissemination controls described in the *Department of Defense Manual 5200.01*, Volume 2 [11]. The safeguards surrounding the FOUO records involve a heightened measure of access control, requiring the use of public key infrastructure (PKI) with a common access card (CAC) for access to documents. Specific protocols for the transfer and movement of documents include cover sheets for hard copies and encrypted email transmissions. This also includes a model for restricted access to the specific records. In addition, policies, procedures, and practices dictate robust dissemination controls on ODCs.

B. ORIGINATOR CONTROLLED INFORMATION DISSEMINATION

Access controls on computer systems enforce policies to protect information so that it is accessible only to those for whom access is authorized. In a computer system, an entity will be granted or denied access to an object in the system, based upon rules set in place in the system. In many cases, these determinations are made based upon access control lists (ACLs) associated with an object in the system. The ACL describes who is allowed to have access to the object. There are various categories for access control, each describing the unique nature in which the system builds, reads, and interacts with ACLs on an object. Originator Controlled (Orcon) Access Control is an information dissemination control that is defined as the "dissemination and extraction of information controlled by the originator" [12]. Information, in this context, refers to data and data objects that have an originator of that specific data. The originator, as referred to in this context, is the entity who has ownership of certain information, and has originated a document or item such that the originator has control over the handling of the information in all capacities, including documents created by others that contain this controlled

information. The Orcon dissemination control represents a stringent form of access control where minimal information sharing is needed, and a tight chain of information flow can be established. ORCON (capitalized) is used by the DoD and intelligence communities to "mark information that requires the originator's consent for further dissemination or extraction of information when the classification level and other controls alone are insufficient to control dissemination" [11]. ORCON is a special dissemination marking on highly classified intelligence information. ODCs do not fall into this category, so "Orcon" in the context of this work describes originator-controlled information in ODCs. In discussing ODCs, Orcon will be defined simply as the dissemination and extraction of information controlled by the originator.

1. History of ORCON Models

In 1989, Graubart was one of the first people to think about how ORCON might be implemented in a system. The motivation for the implementation of ORCON was the insufficient mapping of existing access controls to specific DoD/Intelligence information. The two significant access control policies are Mandatory Access Control (MAC) and Discretionary Access Control (DAC). MAC policies restrict access to information based on the sensitivity of the information and the formal authorizations of people. In DoD and the U.S. Government, it is enforced by applying sensitivity labels to the information and checking a user's clearance to access information of such sensitivity [13]. DAC is used to restrict access to objects based on the identity of subjects or groups to which they belong [13]. DAC policies allow for the policy to be modified. DAC utilizes a runtime interface for policy modification: changing ACLs or permissions. Often, DAC policies are implemented so that UIDs or roles are checked against an ACL. ORCON exists as a way to fill a gap needed in access control that could not be adequately solved by MAC, DAC, or a combination of the two [14]. McCollum et al. expanded upon this work in 1990, developing a policy model for ORCON which would be a strictly enforced control of access and specific access modes at an individual user level [15]. ORCON is a unique type of access control. MAC and DAC do not satisfy the conditions needed for ORCON [14]. This form of access control allows original owners of data to retain control of the

data, even after it is propagated, copied, merged, and written by other users who obtained access to the data [15].

2. ORCON Usage Example

Figure 2 illustrates the access control that ORCON provides. In Figure 2, part (a), Alice creates an object with information that will follow the rules of ORCON. Alice can create an access list containing who is able to view the particular object, and who can create new objects that contain the ORCON information contained within the object. Alice allows Bob to read from and write to OBJ-1. In Figure 2, part (b), Bob creates a copy of OBJ-1 and calls it OBJ-2. Bob, instead, could have retyped the contents of OBJ-1 into a new object OBJ-2, and have complete control over that object; however, he is still required to obey the dissemination controls originally applied by Alice. The retyping of information is a limitation of computer controls, since it is a process that the system can do nothing about. For the purpose of this work, this limitation is not considered.

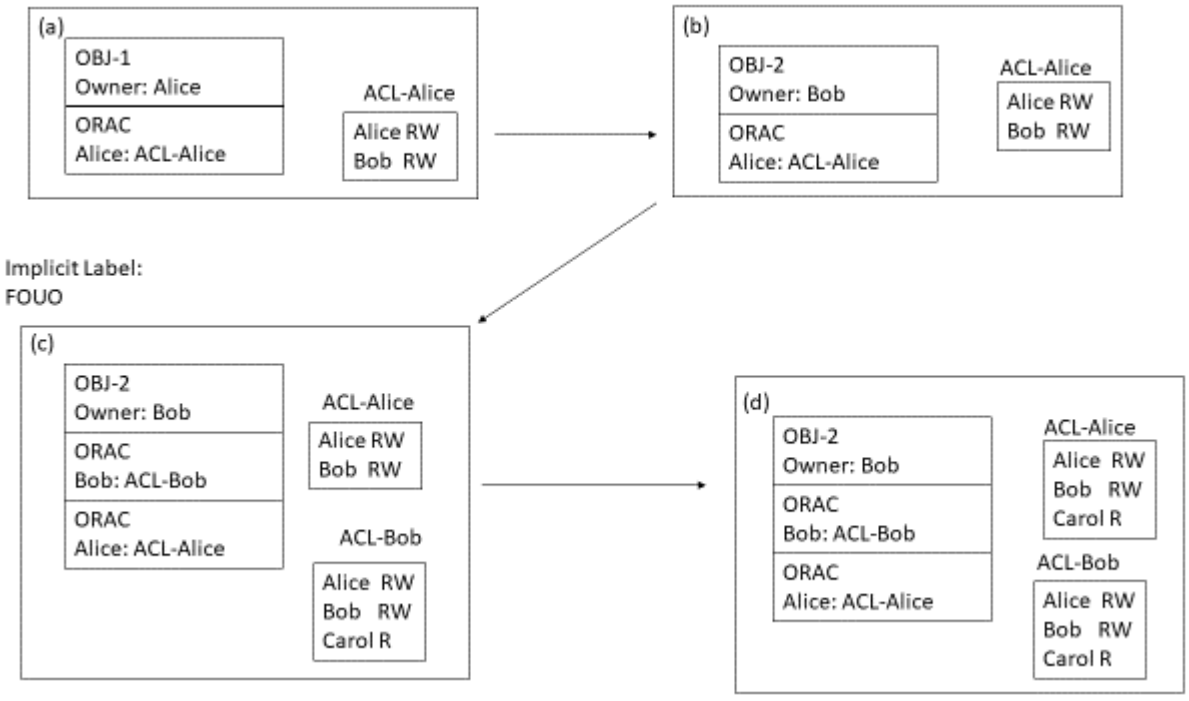


Figure 2. ORCON Usage Example Diagram. Source: [15].

Bob is the owner of OBJ-2, but this new object is still subject to the access control list created by Alice. Bob can create his own access list for his object. In Figure 2, part (c), Bob gives Carol read permission for OBJ-2. Under the rules of ORCON, Alice still retains ownership of the information in OBJ-2, and her access control still applies to the object. Because Carol does not have read access according to Alice's access control list, Carol is not allowed to read the document. In order for Carol to read the document, Alice must grant Carol read access to the document. Because Alice controls her access list, only she can update it. Bob can update and change his access list, but not Alice's, so he must ask Alice to update her access list to allow Carol to have read access to the object. In Figure 2, part (d), Alice updates her access control list for the object, which now gives Carol read access to the document.

C. BLOCKCHAIN TECHNOLOGY

Although the concept of blockchains evolved from work starting in 1980, the first well-known instance of its use was by Bitcoin in 2008 [16]. The term *blockchain* has "no standard technical definition but is a loose umbrella term used by various parties to refer to systems that bear varying levels of resemblance to Bitcoin and its ledger" [17]. Given this, researchers and industry leaders tailor the definition of blockchain to their given implementations of the technology.

For the purposes of this work, blockchain will be defined as a distributed, immutable* ledger. Many industry leaders have invested in research on the use of blockchain technology because of its potential to solve issues associated with centralized systems and bureaucracy [18], [19]. Gartner's chart in Figure 3 illustrates the emergence of new and developing technologies. The figure includes technologies that show promise in delivering a competitive advantage to organizations who leverage the technologies [20]. Each of these technologies is categorized by their maturity in terms of research done to applications built in the industry. Blockchain technology is being considered by

* Blockchains are immutable when all parties participating in a blockchain act in a non-malicious way. Blockchains are difficult to change, but are vulnerable to attacks that can change the contents, breaking its immutable nature. For the purposes of this work, this vulnerability will not be considered, and all participants are assumed to be non-malicious. Immutable, used from this point on, is defined as "essentially immutable," taking into account this vulnerability.

organizations as a potential solution for streamlining processes burdened by centralized and intermediary organizations, even outside of the financial realm [20]. However, Figure 3 shows blockchain technology at the peak of inflated expectations because many proposed applications have been theorized, but few have been implemented.

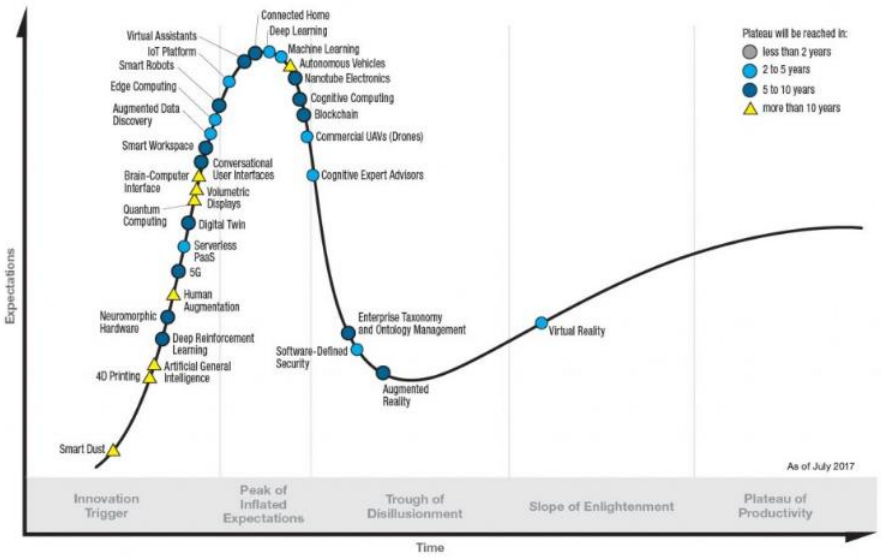


Figure 3. Hype Cycle for Emerging Technologies (August 2017): Source: [20].

1. History and Origin

"Bitcoin, A Peer-to-Peer Electronic Cash System" was publicly released in 2008 [16]. Bitcoin was designed to be a trustless, distributed system that supported currency transactions. Bitcoin takes out the financial institution as a middleman for financial transactions and is trusted through the application of cryptographic techniques. This innovative system, widely known as a cryptocurrency, allows mutually suspicious participants to engage in transactions through the use of blockchain technology. The Bitcoin whitepaper does not use the term "blockchain," eluding to the fact that blockchain does not have a standard definition, but was a new way to combine distinct cryptographic elements to accomplish something new [17].

Blockchain technology combines the ideas of linked timestamping and verifiable logs, verifiable proofs (e.g., proof-of-work or Byzantine fault tolerance), PKI, and smart

contracts [17]. Each implementation of a blockchain is unique but draws upon a collection of research advancements and technologies of the last 35 years. Merkle trees, first introduced by Ralph Merkle in 1980 [21], are used to create a digest of all of the data items that make up each block that will be added to the blockchain. Figure 4 illustrates a Merkle Tree.

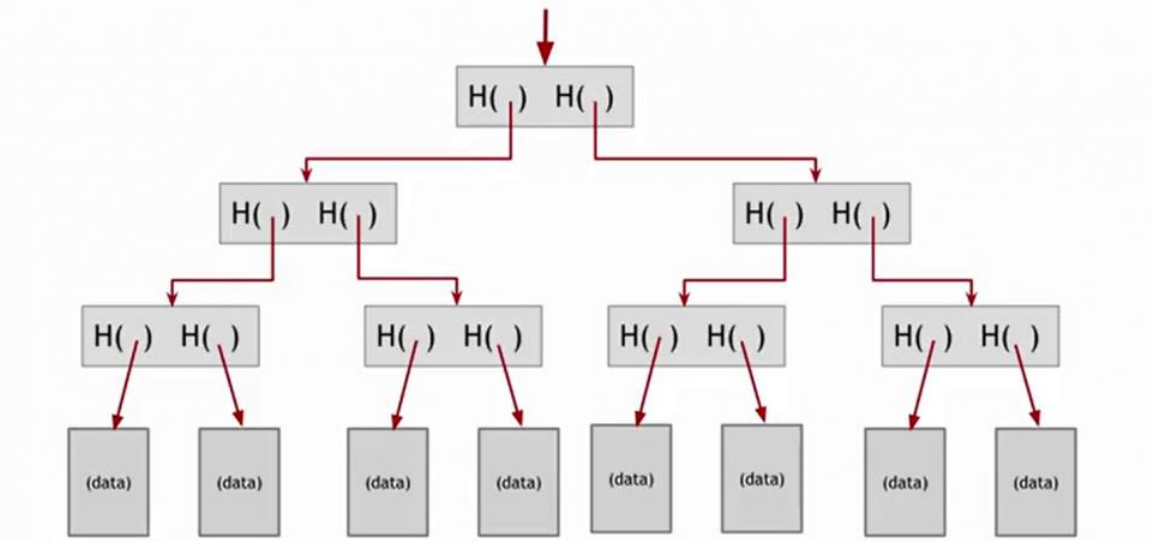


Figure 4. Example Merkle Tree. Source: [22].

Merkle Trees add only a small footprint to the original data and provide a quick method to verify the integrity of each item within the block. Integrity in this context means that the value of an item within the block cannot be changed once it has been incorporated into the blockchain. Figure 5 illustrates how this forced integrity is achieved.

Work done by Stuart Haber and Scott Sornetta in the 1990s produced linked timestamping as a digital notary service that is used as the foundation for the ledgers used in blockchain implementations [23], [24]. Research done by Leslie Lamport, Robert Shostak, Marshall Pease, Miguel Castro, and Barbara Liskov in the field of state replication and fault tolerance in distributed computing allowed for the introduction of consensus models for the addition of new blocks appended to a blockchain [25], [26]. Blockchain technology has combined these diverse concepts in order to provide a mechanism that is new and unique.

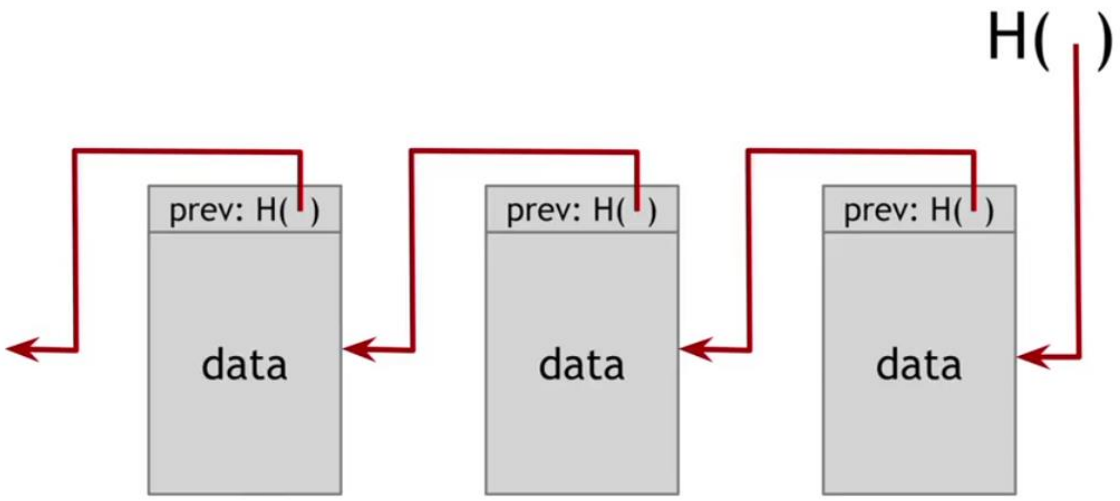


Figure 5. Blockchain Hash Pointer Usage. Source: [22].

2. Blockchain Characteristics and Features

A definition for blockchain is an "immutable ledger for recording transactions, maintained within a distributed network of mutually untrusting peers," [27]. A record of all previous transactions that have ever taken place within the system is recorded on the blockchain. Every blockchain has two distinct characteristics. The first reflects its availability to new participants. A *public* blockchain is open to the public and can any user can gain access to the blockchain and its ledger to participate in the blockchain in some manner. In contrast, a *private* blockchain requires explicit authorization to participate in the blockchain and associated ledger. The second blockchain characteristic relates to its permissions.

A *permission-less* blockchain grants all users who have access to the blockchain authorization to read the blockchain and the ledger, write transactions and build blocks, and participate in consensus. A *permissioned* blockchain can restrict the authorization of users to read, write, and participate in consensus. The work presented in this document will, from this point forward, use the word "blockchain" to refer to a private permissioned blockchain, which will be the type of blockchain used for the case study. Three blockchain features are relevant for this work: its distributed nature, its immutable nature, and its permissioned access control.

a. Distributed Nature

A benefit of distributed systems is the ability to eliminate single points of failure with respect to the execution of a process or the storage of data. Blockchains achieve a distributed nature in both of these regards. First, nodes that participate in a blockchain use a specific software suite to comply with blockchain's specific protocols. Each participant in a blockchain runs the software based on their permissions to be able to read, write, and verify data on that blockchain. Second, redundant copies of the blockchain are maintained by each end node in the peer-to-peer network. Each user has an up-to-date copy of the history of all previously recorded transactions tied to the particular blockchain. This history of transactions is called a *ledger*. The ledger contains all transactions that are recorded on the blockchain. When a person decides to append a new transaction to the blockchain, his or her addition is sent to peer nodes that will verify the addition as valid, i.e., one that obeys the protocol and does not violate the integrity of any previous transaction. These peer nodes then send the transaction to their own peer nodes. For each transaction, this process continues until all users have the new changes to the blockchain and their ledgers are updated. The changes can also be rejected, at which point the transaction is not added to the blockchain and is not reflected in any user's copy of the blockchain.

Figure 6 shows this distributed nature. Each node participating in the blockchain has its own copy of the blockchain. The blockchain is a structured collection of all transactions. The contents of the blockchain can be verified and reproduced from the contents of the ledger. Nodes communicate with each other in a peer-to-peer network to communicate any updates to or verifications of a copy of the blockchain, and edits are then reflected in each copy of the blockchain. This is how blockchain technology achieves its distributed nature.

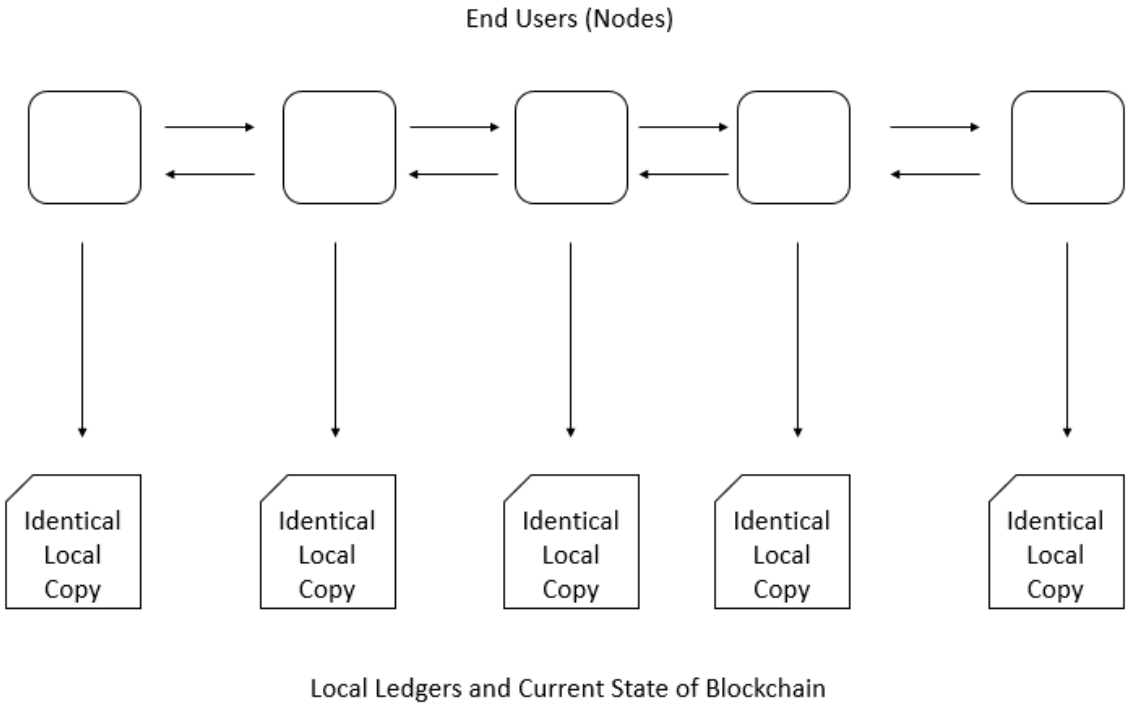


Figure 6. Distributed Nature of Blockchain

b. Immutable Nature

Immutability is a property of an object in which the state of the object cannot be modified after it is created. Immutability is achieved in blockchains through the use of cryptographic hashes. Using a method to condense a group of items into a single value, usually through the use of a Merkle Tree, a series of transactions or items are grouped to make a block that is added to the end of the existing blockchain. Blocks can only be added to the end of a blockchain, and once added and verified, they should not be modified. The new block is cryptographically secured from subsequent modification because the state of the current blockchain is used as an ingredient for creating the cryptographic hash of the next block. This means that every block contains evidence of the state of the blockchain at the time of the new block's creation. When this effect compounds and a block's position in the blockchain deepens, it becomes very difficult to change an already existing transaction [17]. Changing an existing transaction would make the block the transaction is a part of, and every block afterward, inconsistent with the

cryptographic hash that represents the state of the blockchain, thus invalidating the integrity of the blockchain. This is an attribute that can be easily checked.

Figure 7 illustrates how this chain of cryptographic hashes results in the immutability of the blockchain. The state of each block contains not only the content of each item (transaction) for the current block but also the hash of the most current block that has been established in the blockchain, to create a new hash that will be used by future blocks to build upon.

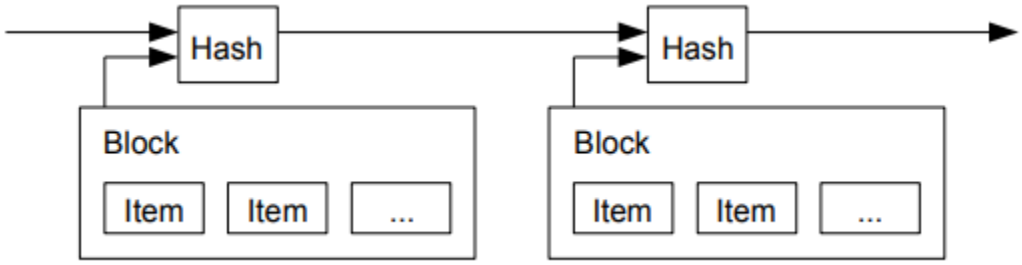


Figure 7. Immutable Nature of Blockchain. Source: [16].

c. Permissions

A permissioned blockchain has a specific mechanism for achieving access controls on users' interactions with the blockchain. This can be accomplished through the use of public-key cryptography. This is a simple solution because public key cryptography is already a part of blockchain technology as it represents the identity of the user participating in the blockchain. Blockchain implementations like Bitcoin that are anonymous still use public-key cryptography to link a Bitcoin wallet to transactions. Public key cryptography is accomplished through the use of shared public keys and secret private keys for authentication and encryption purposes [28]. Permissioned blockchains require this authentication at end nodes to permit or deny access to specific features of the software managing the blockchain. The software retains the public key for a user and his or her associated permissions. When a user authenticates with a private key, he or she is allowed to interact with the blockchain as specified by his or her permission level. This mechanism allows for access control and privacy of data stored on a blockchain, which is

necessary for applications surrounding the use of sensitive information such as personnel records. The Department of Defense already has a public key cryptography implementation through the use of Common Access Cards (CAC).

D. SUMMARY

This chapter provided an overview of Navy Personnel Record Management with regard to the Officer Data Card, an introduction to Orcon, and a brief explanation of blockchain technology. These three subject areas will intersect by creating Officer Data Card Orcon dissemination procedures for which blockchain can provide an immutable timeline of records with verifiable integrity. This use case is relevant to the study of the utility of blockchain technology within the U.S. Navy. The use case will focus on the feasibility, usability, benefits, and risks of blockchain solutions to an existing system for handling personnel records for U.S. Navy officers.

III. PERSONNEL RECORD MANAGEMENT SCENARIOS

This chapter will focus on scoping Navy personnel record management as a whole into specific technical processes involving U.S. Navy officer ODCs and Orcon dissemination restrictions. The scenarios are constructed by defining all of their requirements, variables and desired outcomes.

The breadth of record handling processes within the U.S. Navy is vast. In order to create meaningful and detailed scenarios, several records were initially considered. Of the candidate records, the ODC was the specific record chosen for use in record handling situations. When researching dissemination procedures and practices for ODCs, it was determined that Orcon was used to control dissemination of ODC information. One specific procedure that uses Orcon to control dissemination of ODC information is U.S. Navy officer promotion boards. We will first introduce scenarios for recordkeeping within the context of promotion boards, including the records, the members who interact with the records, and the access controls associated with each member in the process. We will then define the scope and boundaries of the specific scenarios. The following chapters will develop a technical model to represent the scenarios for record-keeping and maintaining Orcon for ODCs during promotion board processes.

A. OVERVIEW OF PROMOTION BOARD PROCESS

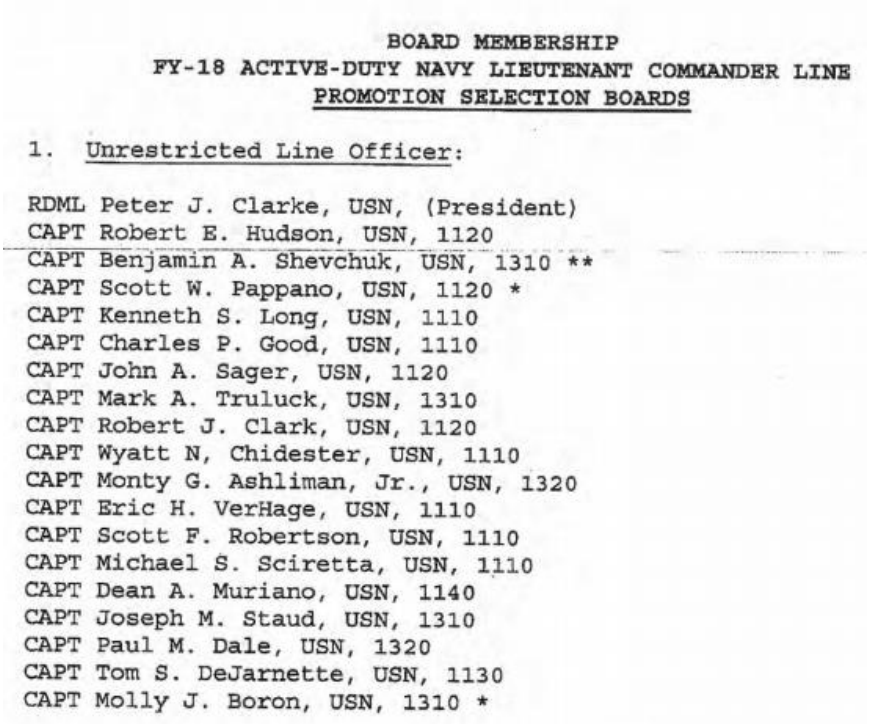
Navy Personnel Command is responsible for overseeing and conducting numerous promotion boards every year. The office responsible for U.S. Navy officer promotions is PERS-801, a subset of the Navy Personnel Command, located in Millington, TN [29]. Promotion boards are held both for U.S. Navy officers and enlisted service members. This work will focus only on U.S. Navy officer promotion boards. There are multiple types of promotion boards, each with its own specific governing authorities and set of rules, regulations, and guidelines. These guidelines include the makeup of board members, eligibility of board candidates, and the criteria for selection. However, these boards can generally be divided into two categories. The first category is *statutory boards*. These boards are required by law and governed by the Defense Officer

Personnel Management Act (DOPMA) [30]. Statutory boards are held for U.S. Navy officers who are being considered for promotion to the rank of Lieutenant Commander (O-4) and higher. DOPMA controls the total number of U.S. Navy officers who can hold a specific rank [30]. DOPMA is held to a strict standard of procedure and compliance and are constrained by governing legislation regarding retention, availability, and budget [30]. The second category of boards is an *administrative board*. These boards are not governed by DOPMA and are specific to a warfare community, e.g., surface warfare or aviation, based upon the needs and requests of that community. Examples of an administrative board are a surface warfare department-head board, an O-5 command board, and a major command board. These boards are governed by leaders within their respective communities, and their standards and procedures meet specific community requirements [31].

A U.S. Navy officer is assigned a detailer who is in charge of billeting and who manages the officer's career path, goals, and plans for military service. Detailers are a set of people who are able to view the service records of other personnel. Detailers are only permitted this special access by nature of their position and must be granted access to the BUPERS database by completing a System Authorization Access Request (SAAR-N). An individual officer's service record is viewable by name in a query-based system. This permissioned viewing access is given to an individual while serving in the role of detailer and is revoked when an individual is no longer a detailer. Even though they have read access to personnel records, including PII and HIPAA information, detailers have limited ability to modify records. An example of a record modification a detailer may perform is the addition of career milestones, e.g., an Officer of the Deck (OOD) Letter. Because of the detailers' permissioned read access to the records and assignment to specific officers, they are excluded from the promotion board process. The promotion board must make an unbiased evaluation of each U.S. Navy officer.

Members of a promotion board are selected based upon rank and service community and are brought to Millington, TN on Temporary Duty (TDY) orders to serve as board members. Figure 8 is a sample memorandum that lists board members who have been called upon to sit as members of a board [32]. Because being a board member

requires viewing PII or HIPAA information, board members, upon initiation of orders, must complete a SAAR-N form, elevating their permission to view records for the duration of their orders.



BOARD MEMBERSHIP
FY-18 ACTIVE-DUTY NAVY LIEUTENANT COMMANDER LINE
PROMOTION SELECTION BOARDS

1. Unrestricted Line Officer:

RDML Peter J. Clarke, USN, (President)
CAPT Robert E. Hudson, USN, 1120
CAPT Benjamin A. Shevchuk, USN, 1310 **
CAPT Scott W. Pappano, USN, 1120 *
CAPT Kenneth S. Long, USN, 1110
CAPT Charles P. Good, USN, 1110
CAPT John A. Sager, USN, 1120
CAPT Mark A. Truluck, USN, 1310
CAPT Robert J. Clark, USN, 1120
CAPT Wyatt N, Chidester, USN, 1110
CAPT Monty G. Ashliman, Jr., USN, 1320
CAPT Eric H. VerHage, USN, 1110
CAPT Scott F. Robertson, USN, 1110
CAPT Michael S. Sciretta, USN, 1110
CAPT Dean A. Muriano, USN, 1140
CAPT Joseph M. Staud, USN, 1310
CAPT Paul M. Dale, USN, 1320
CAPT Tom S. DeJarnette, USN, 1130
CAPT Molly J. Boron, USN, 1310 *

Figure 8. Example Board Membership Memorandum. Source: [32].

For a statutory board, there is no contact between detailers and board members. This applies to detailers who are assigned to the evaluated officers as well as the board member's own detailer. This restriction is not only a digital restriction, by means of electronic communications, but a physical one as well. Detailers reside in the Whitten Building on the Navy Personnel Command in Millington, TN and the building for promotion boards is adjacent to it. While serving under orders on a promotion board, its members are prohibited from entering the Whitten Building for the duration of the TDY orders and are prohibited from contact with all detailers for the duration of the orders. Likewise, detailers are prohibited from entering promotion board spaces and communicating by any means with board members. Board members, in addition to this restriction, are prohibited from disclosing the fact that they have been selected as board

members until the results of the board have been released. These restrictions on board members exist to eliminate outside bias, which could affect the case of a candidate for promotion.

Administrative boards differ from statutory boards in that at specific points within the board process, communication among detailers and board members is permitted. For an administrative board, detailers are allowed to do a pre-board "record scrub" for candidate officers. A record scrub provides an opportunity for communication between board members and detailers to give guidance regarding the particular records of interest to the board, and for the detailers to reach out to candidate officers to resolve any discrepancies in a candidate's record package [33]. For the purposes of this work, only statutory boards will be considered due to their heightened strictness and enforceability of procedures for board meetings and board conduct.

B. RECORD HANDLING IN STATUTORY PROMOTION BOARDS

Personnel records, as described in detail in Chapter II, are divided into three distinct categories: the OMPF, the ODC, and the Officer Summary Record (OSR). These three types of military records are stored in separate databases and are accessed through separate mainframes and user interfaces. The BUPERS database contains all scanned documents associated with a U.S. Navy officer's personnel file and provides interfaces to access and change these documents [33]. Users can access this database of information through the use of a CAC, once they have been granted access to the database by means of a SAAR-N authorization. Access control is handled by associating an identity via a CAC and enforcing access control rules on that identity. A specific set of access control rules is determined based on a user's role within the system, and are stored on database systems. A user's access is associated with those documents he or she is allowed to read, append, and edit within the BUPERS database.

Before a statutory promotion board convenes, personnel records are copied for all U.S. Navy officers who are being evaluated in a particular promotion board. This typically takes place two weeks before the convening of the board. The copying of data is initiated by administrators and IT members who work in the promotion board building.

While multiple records are used for each U.S. Navy officer promotion candidate, this work will only focus on the use of ODCs during the promotion board process. In the case of copying ODCs from the BUPERS database, the ODC copy is in the form of a PDF document that represents the most up-to-date ODC that was generated by the BUPERS database.

The promotion board building is segmented into three distinct sections. Figure 9 shows the segmentation, information flow, and physical access restrictions of the board spaces within the building.

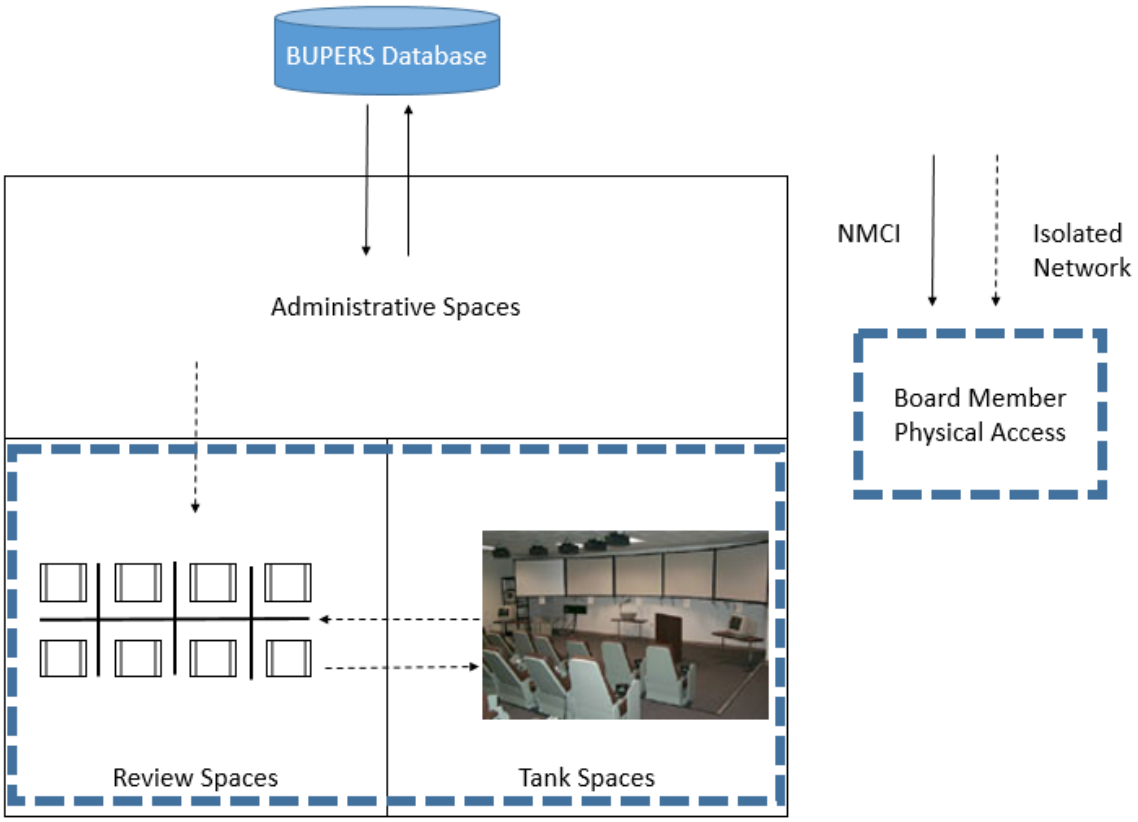


Figure 9. Physical and Network Segmentation of Promotion Board Spaces

The promotion board spaces consist of two networks: an externally-facing network, and an internal, isolated network. The administrative spaces are the only portion of the building connected to the external-facing network. Administrators have Navy

Marine Corps Intranet (NMCI) access and can access all necessary databases for records from administrative space systems. The copied personnel record information from the BUPERS database is stored in the administrative spaces and then distributed to workstations in the review spaces. Review spaces are used for individual work where board members markup records for each promotion candidate. The tank space is used for group work where all board members congregate and deliberate over candidates and make decisions to promote or not promote each candidate. The review spaces and tank spaces house workstations equipped with consoles that are only connected to the internal, isolated network. Personal devices with Internet connectivity are not allowed into the building.

The administrative systems can be connected to the internal network to transfer records to the internal network. This process takes place while the review space systems are not being used. Any request for additional information during the promotion board must be made to an administrator via email or paper request. The administrator will retrieve the information via the external network connection. These measures ensure the data held in the internal network has limited means for being leaked and that there is no use of information other than for the strict purposes of the statutory promotion board. It creates a soft air-gap from outside the building to the inside of the building where board members operate [33].

When the board takes place, the record copies have already been loaded onto the workstations in the review spaces. Each board member is assigned a group of candidate officers whose records are to be evaluated. When board members evaluate records, they use markup language software to add notes and comments to records, appending the markup to the underlying records. Because the markup of the records overlays the officer's actual records, the actual contents of the records are not changed by the markup process. Even if a record were somehow changed, the records, once in the promotion board building, are considered separate and unique from the actual records stored in the records databases. The board members may only work with copies of records that never go back into the BUPERS database. The marked records are stored locally until the board results are announced, at which point they are discarded.

After markup of the records has been completed, the marked-up records are moved into the tank spaces. Here they are deliberated upon by board members. The records are displayed for all board members to see, but records are never edited or marked up in tank spaces. After the deliberations in the tank-spaces have concluded, specific candidates' records are discarded because they have been selected or not selected for promotion. Only a portion of the eligible candidates is selected for promotion during an iteration of deliberations. Board members then return to the review spaces and review records of those candidates who were neither selected nor rejected during the iteration. They markup records that they previously did not markup, but that a different board member had already marked-up. The records are then sent back to the tank spaces for deliberation and voting. This process iterates until a sufficient number of officers have been selected for promotion as mandated by DOPMA.

C. STEPS FOR CORRECTING ODC INFORMATION

1. Determination

On occasion, when ODCs are initially copied for a given promotion board, there are situations in which an ODC may have missing information or may contain incorrect information. Under normal circumstances, the two situations are handled differently. However, the processes to handle these two situations are the same from the perspective of the promotion board process and will be discussed below.

2. Request

Both the process of adding missing ODC information and correcting incorrect ODC information can be initiated by a member of the promotion board or by the U.S. Navy officer being considered for promotion. The process presented here does not apply outside the context of promotion boards. The only difference in procedure between the two scenarios is in who first requests missing or corrected information. If a board member requests the information in question, there is additional overhead at the beginning of the process. A request must first be made in order for any new information to be admitted into the board. Board members must request the missing information from administrative personnel working within the board spaces. The administrative member

assigned the task of retrieving the missing information will query the permanent databases to ensure no previous error was made. If the queries yield no results, the administrative member will then reach out to the officer to attempt to retrieve the appropriate information.

3. Admittance

At this point, the rest of the procedure for the two scenarios is the same whether the admittance of new ODC information is initiated by a board member or by the U.S. Navy officer being considered for promotion. The new record to be admitted will be provided by the officer. This submission is made by sending an encrypted email containing the record that contains the requested information.

4. Resolution

The email is sent to the administrative personnel who work within the board spaces. The administrative third party is necessary because of the strict prohibition between board members and candidates during the promotion board process. The ODC information is added to the respective officer's records housed in the board spaces and is used for the duration of the board deliberations.

In both scenarios, there is a crucial point with regard to record management. When the new ODC information is admitted into the board spaces for review during a promotion board, regardless of how or why it was admitted, it is only added to the U.S. Navy officer's ODC for the duration of the board, and will not be reflected in the officer's permanent ODC. Because of the nature of record handling during promotion boards, information only flows into board spaces. No ODC information leaves the board spaces. When new information is admitted to the board, it is only for use in that board and is visible only to the members of the board. Additions or corrections to permanent ODCs must be routed using conventional processes for adding or correcting ODCs, as mentioned in Chapter II.

D. CONSTRUCTING THE SCENARIOS

The two scenarios mentioned in Section C, the addition of missing ODC information or the correction of ODC information, represent two useful case studies for information flow. This section will explain the scenarios of adding missing ODC information and admitting corrected ODC information within the context of U.S. Navy officer statutory promotion boards by defining variables and desired outcomes.

1. Scenarios

The ODC of a U.S. Navy officer being considered for promotion in a statutory promotion board is copied and admitted for the purposes of the board. The ODC accurately reflects the contents of underlying the subsidiary information. However, assume that a line item within a U.S. Navy officer's ODC is missing information or has incorrect information in it. The associated record from which the ODC line item derives is either missing or results in the incorrect information shown on the ODC. This only applies to line items that should have previously been correctly documented and does not include line items that are intentionally left blank or are not applicable to the officer.

2. Variables

- ODC Line Item W – A field within an ODC record for Officer Y that reflects Record Information Z.
- ODC X_{NEW} – A corrected X_{OLD} document. This document houses Record Information Z and is reflected in W.
- ODC X_{OLD} – A document that contains incorrect information or missing information. This document either houses an incorrect Record Information Z or is missing Record Information Z altogether.
- U.S. Navy Officer Y – Officer being considered for promotion in a statutory promotion board.

- Record Information Z – An item of information stored in a record that is reflected in Line Item W.

3. Desired Outcomes

In both scenarios, ODC X_{NEW} is inserted into officer Y's OMPF, reflecting the current date of addition to the OMPF. Record Information Z_i, which is contained within X_{OLD} and associated with Y's ODC Line Item W, is updated reflecting Z_{i+1}, resulting in ODC X_{NEW}. In the scenario for the missing record, the OMPF notes that the X_{NEW} was added on this date. In the scenario of the incorrect record, the OMPF notes that X_{NEW} was admitted with the correct information, replacing ODC X_{OLD}. In both scenarios, the ODC X_{NEW} is updated reflecting new information in W, and the underlying records support why the ODC X_{OLD} was updated.

Two additional desired outcomes are also given. Neither are implemented in the current process. The first additional desired outcome is that once Z_{i+1} has been updated in W within the board spaces, it should not be necessary for Z_{i+1} to be updated in W within the official database system for Officer Y. This additional desired outcome extends the process of adding or correcting records for promotion boards and results in a more streamlined process for updating and correcting records. The second additional desired outcome is to add a revision number to ODCs. When an update to an ODC X_{OLD} is made, a revision number is assigned to Y's ODC X_{NEW}. This allows for ODC changes to be tracked from the original ODC X_0, and a forensic chain can be made to reflect all changes ever made to Y's ODC. This would provide greater tracking of the progression and change of an ODC throughout a U.S. Navy officer's career and if needed, would support recovery and tracking of the time that a line item may have been corrupted or not correctly updated.

E. SUMMARY

This chapter defined two specific scenarios within the vast space of U.S. Navy officer record management. The promotion board process is a critical function within the U.S. Navy and the U.S. military as a whole. Because governing legislation outlines how

its results should be tailored and how it should be conducted, strict adherence to the implementation of policy and legislation is needed. Personnel records contain and include PII and HIPAA information, both of which must be safeguarded and require access control checks in order to be viewed. The records are owned by the CNPC throughout the entire process, and the results of a statutory promotion board are also owned by CNPC. The information flow process is regulated in a way that maximizes security and privacy of information in personnel records. Through the use of the one-way flow of information and restricting access to information as ODCs are being created from existing information, CNPC maintains the proper ownership and control of information and new ODCs created throughout the process of statutory promotion boards.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THREAT MODEL

Threat modeling is an approach for analyzing the security of an application [34]. Building a threat model is the process by which security risks associated with a system or process can be identified, quantified, and addressed from the perspective of an adversary to the system or process [34]. Threat modeling allows the owners of systems and processes a systematic and pre-emptive way to identify vulnerabilities and weaknesses in order to develop mitigations to harden their systems and processes. A threat model for the process of admitting missing or incorrect ODC information in statutory promotion boards must be defined. Formal threat model construction involves the steps of decomposing applications, determining and ranking threats, and determining countermeasures and mitigations [34]. We will only construct an informal threat model by defining assets to the record handling process for statutory promotion boards and determining threats to the assets.

A. ASSET EVALUATION

The first step in threat modeling is to identify assets, in this case, those used in supporting the process of admitting missing or corrected ODC information during a statutory promotion board for U.S. Navy officers. For the purpose of this work, assets will be defined as records, systems, and processes associated with the scenarios of Chapter III. The protection required for assets will be associated with one or more of three security policies: confidentiality, integrity, and availability (CIA). Each of these three policies and the associated assets is assessed in terms of its value to the organization.

1. Confidentiality

Chapter II outlines the contents of ODCs, and the associated privacy policies and restrictions to access. Policies govern the processes for which privacy is maintained for record handling. Conservation of the confidentiality of PII, in particular, is of the utmost importance, as mandated by HIPAA. Record usage and policy governance outlined in Chapter II.A.5 set forth restrictions for safeguarding confidentiality of official record

information. These governing policies, therefore, make confidentiality of the board process and record handling very important. The OPM data breach is an example of a breach of record confidentiality and should act as a warning of the fallout of an attack on record confidentiality [35].

2. Integrity

Ensuring the integrity of information in the ODCs of U.S. Navy officers in promotion boards is a critical aspect of this thesis. The processes constructed in Chapter III are processes that reinstate the integrity of U.S. Navy officers' ODCs that have lost their integrity at some point prior to the convening of the statutory promotion board. Integrity is lost when information within ODCs is incorrect or incomplete. The integrity of these ODCs has real consequences with regard to manpower and retention of the best officers for the U.S. Navy. Manpower is a critical asset of the DoD; therefore, maintenance of the integrity of material used in the board process and record handling process is critical.

3. Availability

For ODCs, availability is not as critical as confidentiality and integrity. The availability of records with respect to the promotion board process in an electronic sense deals with being able to access records for use in consideration of U.S. Navy officers for promotion. While an attack on availability would result in the delay of the overall process, physical measures can be taken to mitigate attacks on availability. Thus, it is determined that the availability of assets used in the board process and record handling is of less concern that confidentiality and integrity.

B. ADVERSARY EVALUATION

With the determination of critical assets and the most applicable policies, adversaries can be evaluated to determine the most relevant threats to ODCs. Two traits will be considered when defining a type of adversary. The first is the adversary's intentions. An adversary is defined as either being *intentional* or *unintentional*. An intentional adversary is an adversary who acts with the purpose of attacking or tampering

with ODCs and the processes used to manage them. An unintentional adversary is one who accidentally degrades the integrity or confidentiality of the ODC. While an unintentional adversary does not have malicious intent, the unintentional actions can result in the degradation of originator control of ODCs.

The second trait is the adversary's access point. An adversary is defined as either an *insider* or an *outsider*. An outsider is an adversary who acts against ODCs by penetrating the network space and obtaining access to enterprise systems or data that the outsider does not have permission to access. For the purpose of this work, the network space is defined as the databases polled for the creation of the ODC, the BUPERS database that stores the ODC, and the machines in the board spaces. An insider is an adversary who acts against ODCs from inside the network space, and already has permissions to access enterprise systems and data. With these traits defined, the four types of adversaries can be considered:

1. Intentional Outsider

This adversary knowingly acts against the ODC or promotion process from outside the defined network space. It is reasonable to assume a highly capable adversary is required to obtain access to the databases where subsidiary information for the ODC is stored. Therefore, the intentional outsider adversary is considered a threat candidate.

2. Unintentional Outsider

This adversary unknowingly acts against the ODC or the promotion process from outside the defined network space. Due to the security measures taken on NMCI and the internal board spaces network, it is improbable that an adversary could unintentionally access the ODCs or the network spaces. Therefore, the unintentional outsider adversary is not considered a threat candidate.

3. Intentional Insider

This adversary knowingly acts against the ODC or the promotion process from inside the defined network space. Even though the defined network space is segmented

with restricted access, this adversary has the potential to cause considerable damage. Therefore, the intentional insider adversary is considered a threat candidate.

4. Unintentional Insider

This adversary unknowingly acts against the ODC or the promotion process from inside the defined network space. Record-handling processes are inherently human processes that require users to update and maintain record information. It is reasonable to assume that mistakes are made in these processes unknowingly. Therefore, the unintentional insider adversary is considered a threat candidate.

C. MOST RELEVANT THREAT

, Threats are analyzed considering assets critical to the promotion process and ODC and the potential adversaries. With regard to the confidentiality of the board process, current processes to safeguard confidentiality are already in place. Enforcement of confidentiality of information in the ODC system is achieved through safeguards and by applying punitive pressure to personnel to ensure the confidentiality of records. Networks with no external communications limit the loss of confidentiality. Confidentiality with regard to the scenarios described in Chapter III deals with physical processes more than digital processes. Because of the need to enforce policy for ODC dissemination control, the confidentiality of ODCs for statutory promotion boards is considered.

We also consider the integrity of the promotion board process and the ODC. On a macro level, the promotion board process adheres to the highest standards as it is governed by DOPMA, so its integrity is intended to be high. On a micro level, the integrity of the ODC is essential to accurately reflect the U.S. Navy officer. The ODC represents the work of the U.S. Navy officer, his or her career timeline, and significant accomplishments. In order for the promotion board to act with a high level of integrity, the ODC must be of high integrity. Therefore, an attack on the integrity is a highly relevant threat to the promotion process and ODC.

The three types of adversaries are now considered as vectors for carrying out attacks on the integrity of the promotion process or ODC. The intentional outsider is an adversary who is assumed to be a technically capable and perhaps a nation-state actor. The nature of this adversary's capabilities may allow him or her to covertly corrupt ODC documents. Although this is possible, it is unlikely for an adversary to target personnel records amidst the large target space within the DoD. This adversary is considered dangerous and sophisticated, but because of the unlikely nature of an attack against the promotion process and ODCs, the intentional outsider is not considered part of the most likely threat.

The intentional insider is considered the most dangerous adversary with regards to the confidentiality, integrity, and availability of the ODC. The vetting process for personnel who can access records at any given time provides mitigation for this type of adversary. Thus, the likelihood of this adversary is very low. However, because of the combination of permissioned access and malicious intent, the intentional insider is still considered a highly relevant threat.

The unintentional insider has network access but acts in a way that inadvertently leaves the ODC in an incorrect state. Because the policy and procedures for statutory promotion boards are not openly documented [33], the discretion given to insiders regarding procedures can lead to a breach of the integrity of the promotion process or ODC. Given the full range of personnel who can act as unintentional adversaries and the access permissions they have, we believe that the unintentional adversary is the most likely to corrupt or disclose an ODC.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ODC ORCON PROCESS MODEL

The purpose of this chapter is to construct an Orcon process model for the two scenarios introduced in Chapter III. Because BUPERS controls both the contents and dissemination of the underlying datastores and the ODC itself, this is an originator control problem. The objective is to ensure that there is a log of the reads and writes to ODC records starting when they are copied and put into board spaces, through potential record correction, and ending at the conclusion of the promotion board. Although it is expected that most records do not require correction, the logging system could support the correction of any ODC. The methodology used to build the Orcon process model was to step through the scenarios constructed in Chapter III and follow the handling of ODCs, adhering to the rules necessary to satisfy Orcon conditions. An explanation of the model at the critical steps of determination, request, admittance, and resolution is given. These steps are defined in detail in Chapter III.

Following its construction, the Orcon process model can be used as the basis for examining how technical mechanisms could be used to support the enforcement of policies pertaining to ODCs. The Orcon process model describes the interactions between individual users and systems that interact with the records for promotion boards and describes how these users will act on the records and derivative objects created from these records. Derivative objects are defined as objects that originate from another object and include the marked-up documents created by the board members in the reviewing spaces.

A. OVERVIEW AND DEFINITIONS

This section provides an overview of the rules and definitions used in this chapter for modeling ODC Orcon dissemination control. We first define categories of actors and information for the Orcon process model from the perspective of computer access control. We then set the rules and define the terms that will be used throughout the creation and discussion of the ODC Orcon process model.

1. Access Control Overview

The Orcon process model contains three main constructs: objects, subjects, and access modes. Objects are defined as documents or records which are controlled according to policy. Objects are created by subjects and can convey access to other subjects. Subjects are defined as the execution entities, such as processes, that act on behalf of people or organizations. Subjects create, read, write, and delete objects. (Other modes of access are combinations of these basic actions.) A subject may control access rights of other subjects to objects and may convey control, read, and write access to other subjects. ACLs are associated with objects and define the rules for which subjects may interact with an object [15]. Because of the compiled nature of documents where originator control is in effect, it is possible for multiple subjects to control or have differing rights to various information elements contained in an object. Therefore, ACLs may reflect a variety of control and access rights. When an object is created, the underlying protection system creates its default ACL. The ACL has fields to support originator control over dissemination. Originators of objects must maintain control when objects are copied, and metadata associated with originator controls must be applied to new objects. This allows for originator control over objects created and owned by other users. Note that for the purposes of this work, the ACLs created and used are hypothesized. We are abstracting the processes of Chapter III and superimposing dissemination ACLs based on current practices and procedures.

2. Rules and Terminology

Figure 10 illustrates the construction of an object and its metadata, which is the foundational building block for the Orcon model for this work. For illustrative purposes, the metadata in Figure 10 is partitioned into distinct components. Component A contains two elements. The first is the name of the object. The name of the object container identifies information and its associated metadata, allowing for the object to be found, e.g., via a pathname in a file system. The second element is the owner of the object. Each object has exactly one owner. Component B is the usage ACL, which is filled with permissions for user interaction with the object. Component C defines the originator

retained access control (ORAC) metadata container for the object. Each ORAC metadata container defines an originator, and the associated ORAC ACLs created and maintained by the originator.

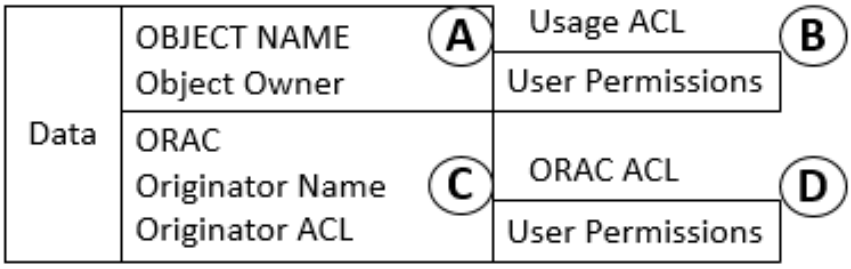


Figure 10. Abstract Object Construction

Component D shows the ORAC ACLs associated with an object. ORAC ACLs have a name, which is associated with an ORAC metadata container (Figure 10, Component C), and a list of permissions. ORAC ACLs may be updated, but only by the owner of the ORAC ACL subsection. Because the ODC object is a composite object containing information from various datastores, the object will use a structured ACL. A structured ACL contains the usage ACL and at least one ORAC ACL subsection. Any user who has originator control over an entire object or a portion of an object must have a subsection of the structured ACL associated with the object. Thus, it is possible for multiple ORAC ACL subsections to be associated with an object. The object is then limited by the intersection of all ACL subsections, which leads to the most restrictive access permission.

ORAC ACLs consist of access permissions to the object for the subjects acting on behalf of users. Usernames are presented in this high-level model to represent users or user-groups; however, implementations often choose other representations. Each username within an ORAC ACL is assigned up to four distinct modes of access. These operation permissions are assigned to specific users, as determined by the originator associated with the object's ORAC ACLs. The four types of operations for ACLs for this work are read (R), write (W), append (A), and ownership (O). For the purpose of this

work, execution is not considered because the objects involved do not contain executable data. Reading allows a subject to view the contents of an object. Reading also allows a subject to create a copy of the entire object or a portion of the object. When an object is copied, the ORAC ACL subsections are also copied to derivative objects. Writing allows a subject to write to an object, and can include additions, deletions, and modifications to the contents of an object. Appending allows a subject to add additional content to an object. Appending is similar to writing, but it does not allow for deletion or modification of the contents of an object.

The ownership operation allows for the originator of the object to transfer ownership to another specified user. Only the originator of an object may assign another user or user-group with the ownership mode of access, and does so in the originator's ORAC ACL subsection (Figure 10, Component D). Ownership change occurs when the specified user or user-group creates a copy of the object. The copied object's owner (Figure 10, Component A) is the new user or user-group, and the old owner's ORAC ACLs are now owned by the new user or user-group. Ownership of ORAC ACLs can only be transferred through the use of the ownership change operation.

Figure 11 illustrates an example ODC object within the context of the scenarios built in Chapter III. Neither the data contained in the object nor the usage ACL are relevant to the originator control discussion, so, from this point forward they will not be shown in this chapter's figures.

In order to accurately read the contents of Figure 11 and future figures, definitions are given.

- Officer is the user ID for the active duty U.S. Navy officer whose ODC object is represented in Figure 11.
- OFFICER ODC is the ODC document associated with user Officer.
- CNPC is the user ID for the Commander of Navy Personnel Command.

- ACL-CNPC is the set of access control rules associated with the OFFICER ODC object that reflect the desired access control set forth by CNPC.
- Detail is the user-group ID for the detailers who work under CNPC.
- Board Member is the user-group ID for the Board Members participating in the statutory promotion board process.

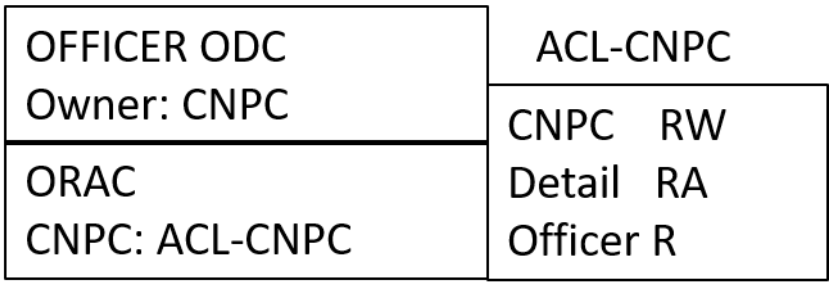


Figure 11. Example ACL for ODC Object

When looking at Figure 11, in combination with the definitions given, the reader should gather the following information:

- The object's name is OFFICER ODC.
- User ID CNPC owns OFFICER ODC.
- CNPC owns an ORAC metadata container on OFFICER ODC with one ACL named ACL-CNPC that encompasses the entirety of OFFICER ODC.
- According to ACL-CNPC, user CNPC may read and write to OFFICER ODC.
- According to ACL-CNPC, user Detail may read and append OFFICER ODC.

- According to ACL-CNPC, user Officer may read OFFICER ODC.

B. ODC OBJECT CREATION

CNPC is the authoritative owner of all information within BUPERS databases, which includes the ODC. Therefore, CNPC is the owner of OFFICER ODC. To maintain the requirements for Orcon, CNPC requires a SAAR-N request to explicitly authorize all other users' accesses to the ODC. Thus, CNPC will either need to explicitly authorize access to read, write, or append to the material or will need to grant ownership of the file object to another subject in order to maintain the requirements of Orcon.

As mentioned in Chapter II, an ODC is a data structure comprised of information derived from other existing records. The ODC is a snapshot of the most recent records maintained by BUPERS. ODCs are generated approximately once per month, and the snapshot of the generated ODC is stored until a new ODC is generated the following month. Figure 12 illustrates the creation of an ODC through an Orcon process. Figure 12, part (a) illustrates the various records that contain information relevant to a U.S. Navy officer's ODC. Each of these records is stored in a database owned by one of the offices outlined in Appendix E of NAVPERS 15839I [5]. Each of these various offices is the owner of the record before the construction of the ODC. Some of these offices work directly for BUPERS, while other Naval offices only report to BUPERS for the purpose of supplying necessary records needed to construct ODCs. The ACLs described by these records allow the office to read and write to the particular record, but also allow CNPC to read, write and own a document. The U.S. Navy officer has read permission for each of these records.

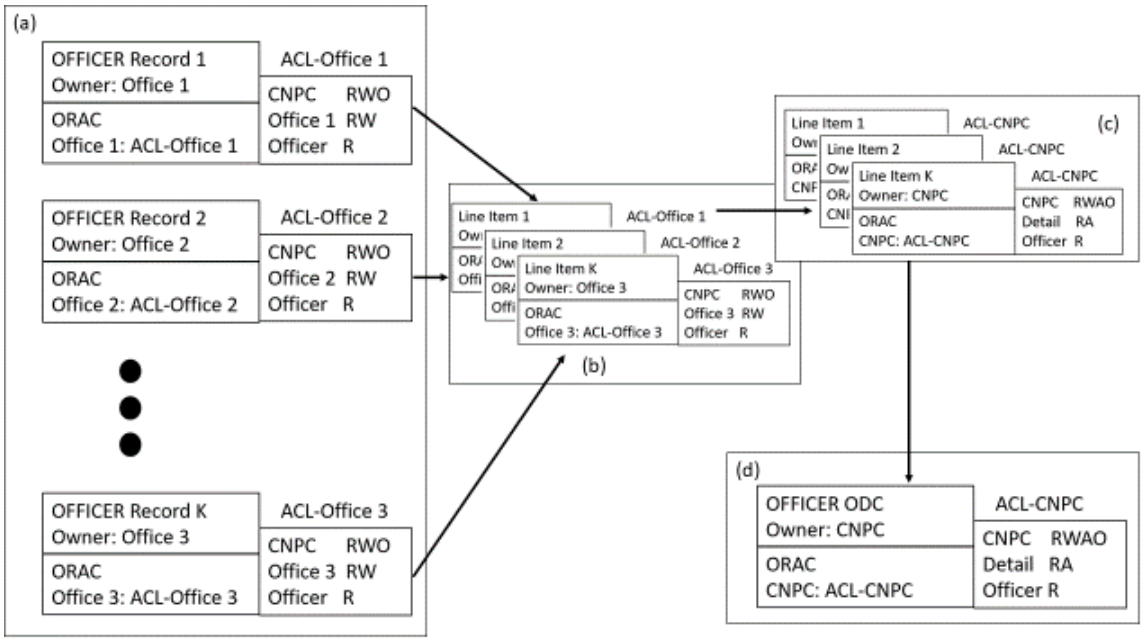


Figure 12. Creation of ODC Object

The ODC does not incorporate all of the information contained in the subsidiary records. Instead, it retrieves and stores only portions of original records. This process is illustrated in Figure 12, part (b) and results in the creation of line items. Only the line items necessary for the compilation of an ODC are kept. Line items are owned by the individual offices, and the ACLs remain unchanged from Figure 12, part (a).

Figure 12, part (c) shows an ODC created by BUPERS, which is represented by UID CNPC. The structural shell of the ODC document is created by CNPC, and the contents of the document are filled according to NAVPERS 15839I [5] and illustrated in Figure 1. CNPC creates object OFFICER ODC and is determined to be the originator of the object. Information associated with ODC line items is first owned by the various offices. In order for CNPC to have complete ownership of the OFFICER ODC object, CNPC must obtain ownership of all line items contained in the OFFICER ODC. This step is accomplished through CNPC having ownership permission of all LINE ITEM objects. When CNPC takes ownership of a LINE ITEM object, ownership changes to CNPC, and the ACLs associated with the original owner are also transferred to CNPC. This step is

illustrated in Figure 12, part (c) by keeping all ACLs associated with line items attached to OFFICER ODC, but reflecting the change of ownership.

The final step shown in Figure 12 eliminates the redundancy in all of the ACLs associated with OFFICER ODC. Since CNPC owns all ACLs associated with the object, there is no need for more than one ACL-CNPC. Note that the amount of consolidation will be less for documents constructed from information from several Orcon sources. Our ODC construction process creates one ACL for all of the information in the object. CNPC has read and write permission, and Officer retains the read permission. Detail is added to the ACL, since Detail subjects work for CNPC. Detail subjects have read and append permission to OFFICER ODC. Figure 12, part (d) shows the final ACL for object OFFICER ODC as it would exist under normal conditions in the BUPERS database.

C. CREATION OF COPIES OF ODC FOR PROMOTION BOARD USE

The object OFFICER ODC is an object used for statutory promotion boards and is used in the scenarios discussed in Chapter III. Figure 13 illustrates the steps taken to make object OFFICER ODC suitable for use within the context of statutory promotion boards.

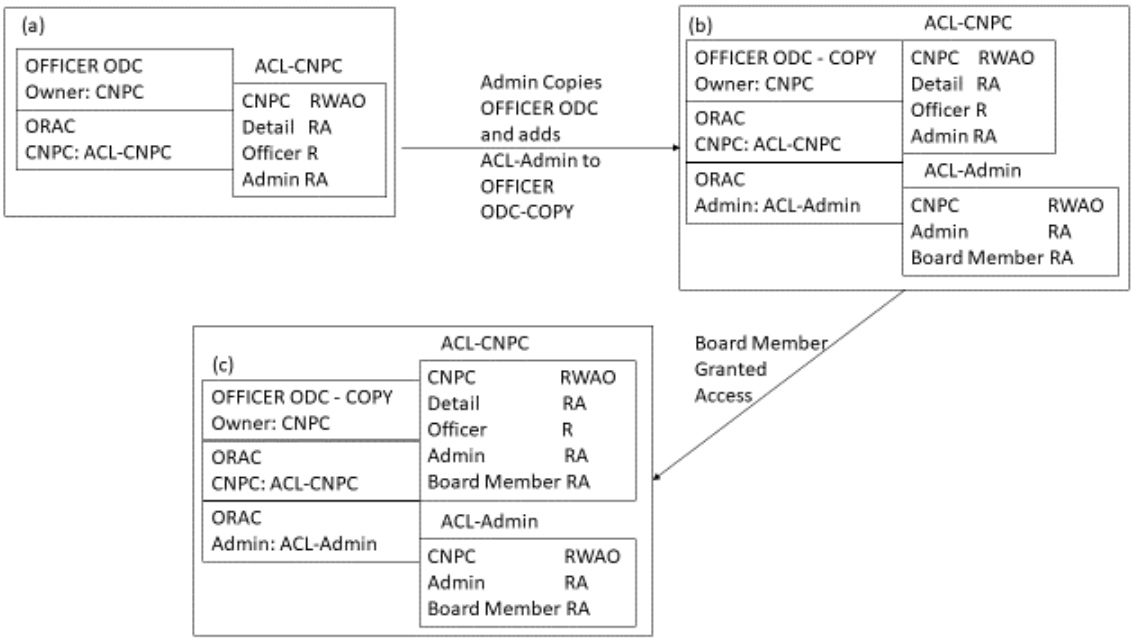


Figure 13. ODC Object Setup for Board

The first step in the process of preparing the OFFICER ODC object for use in statutory promotion boards is creating a copy of the OFFICER ODC object. This is the physical act of copying the ODC object from the BUPERS database and storing it on systems in board spaces. Note that the underlying physical process for copying the object to board spaces is generating a static PDF file of the most current ODC and putting the PDF into the board spaces. It is critical to note that in this step the object is a copy. The original object remains in the BUPERS database, while the copy of the object made by subject Admin is stored on systems in the board spaces. The result of this step is the creation of the copied object, called OFFICER ODC-COPY, for use in board spaces. All of the subsequent steps are performed on OFFICER ODC-COPY in the board spaces.

Subject Admin now adds an ACL to the OFFICER ODC-COPY object. The ACL allows CNPC, the owner of the object, read and write permissions. Admin's ACL also gives Admin read and append permission. The unique permission on ACL-Admin that does not exist on ACL-CNPC is the read and append permission granted to subject Board Member. Figure 13, part (b) illustrates the OFFICER ODC-COPY object after the update to ACL-Admin. This is the state of object OFFICER ODC-COPY in the model when

Admin has loaded copies of the ODCs from the administrative spaces to the review spaces in the promotion board building. This step takes place roughly two weeks before the date the statutory promotion board begins its work.

The final step necessary to prepare the OFFICER ODC-COPY object for use in statutory promotion boards is to grant user-group ID Board Member access to the object. ACL-Admin gives the necessary permissions to user-group ID Board Member in Figure 13, part (b), but due to the nature of Orcon, ACL-CNPC must also give permission to user-group Board Member. Then user group Admin, on behalf of user CNPC, grants read and append permission to user-group Board Member for the purpose of the statutory promotion board. ACL-CNPC associated with OFFICER ODC-COPY object is updated to reflect this change. This step models approval of a SAAR-N form submitted by each board member. Figure 13, part (c) illustrates the state of the ACL for OFFICER ODC-COPY object when the statutory promotion board convenes. This represents the initial state of the object for use in the scenarios built in Chapter III.

D. MODIFICATION OF ODC WHILE IN USE BY PROMOTION BOARD

This section describes in detail the steps defined in Chapter III for correcting ODC information. Each step is modeled using the rules and terminology defined in this chapter to create a detailed ODC Orcon process for the steps required to correct ODC information while in use by statutory promotion boards.

1. Determination of Missing or Incorrect Information

As mentioned in Chapter III, the two scenarios deal with the requirement that new ODC information is submitted for consideration by the statutory promotion board. In this section, the problem of missing or incorrect information will be addressed.

Either a board member or the U.S. Navy officer will determine that ODC information is missing or is incorrect, and will initiate the process of admitting new information into consideration for the statutory promotion board. Figure 14 illustrates the state of the Orcon process model at the point at which this determination is made. Figure 14 shows the elements required to correct OFFICER ODC-COPY: the record containing

the requested ODC information to be added, the current OFFICER ODC-COPY, and the corrected OFFICER ODC-COPY.

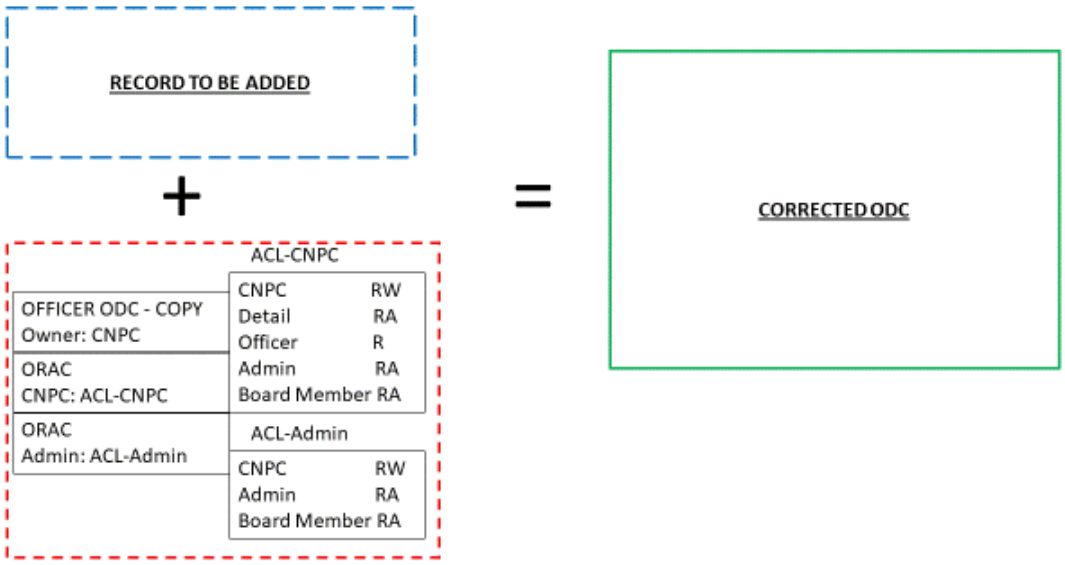


Figure 14. State of ODC at Determination of Need for Modification

At this point, OFFICER ODC-COPY is in one of two states: unmodified, or previously modified, where modification means a change to or addition of a line item in the ODC. In addition, the record could either contain no markups or have markups by board members. Recall that the ODC as admitted to the promotion board spaces is a PDF. It is not modified. Both markups and modifications are appended to the object. Board Members cannot modify the original information in OFFICER ODC-COPY. The steps in the ODC modification process are now described in detail.

2. Request for Records

In all cases, the requester is the same user who determined that OFFICER ODC-COPY was incorrect in the determination step. The process for requesting a record for admittance in a statutory promotion board starts differently depending on the initiator, but the two processes end with the same result. The two request processes are illustrated in Figure 15 and 16. The result of the request is an object ready for the admittance step.

The physical process for the request of a new record to fill a gap in information or replace an incorrect record is given in Chapter III. Figure 15 illustrates the process in which Office 1 holds a record to be added to an existing ODC. This flow will represent the case where the Administrator copies a record from a database. Figure 16 illustrates the process for which an Officer holds information to be admitted. This flow will represent the case given in Chapter III, Section C where the officer electronically delivers a record to the administrator for admission.

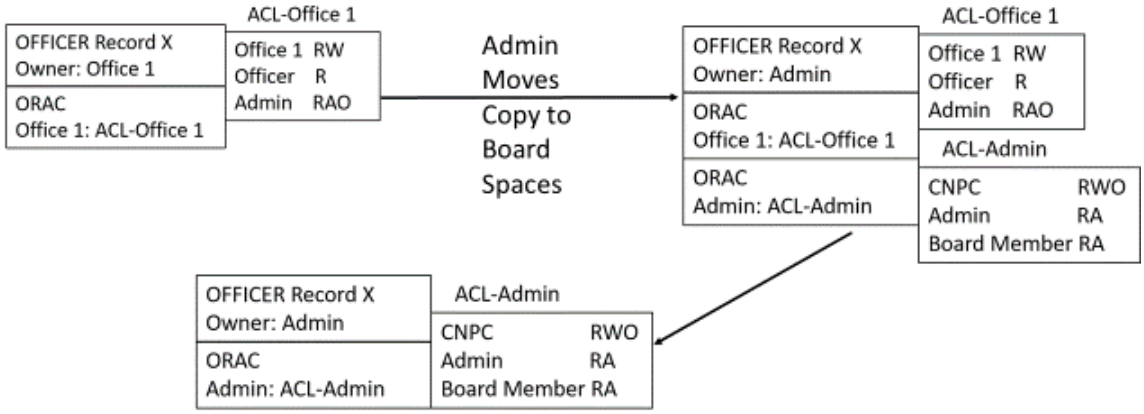


Figure 15. Orcon Process for Request for Record from Office

In Figure 15, the OFFICER Record X is in a database owned by Office 1. The object's ACLs give Office 1 read and write permissions and Officer read permissions. Subject Admin is given read, write, and ownership permission to this object by means of subject CNPC, and subject Admin is acting on behalf of subject CNPC when this record is copied. This permission escalation is provided as a way for user-group Admin to conduct a permissioned action that is pre-approved by user CNPC. This copy of the object is stored within the board spaces. User-group Admin adds an ACL to the OFFICER Record X object, giving user CNPC read, write, and ownership permissions, Admin read and append permissions, and Board Member read and append permissions. Admin then exercises the ownership change permission in ACL-Office 1 to take control of ACL-Office 1 from Office 1. Admin then removes the original ACL-Office 1 from the object, leaving it with only the new ACL-Admin that user group Admin had added to the

OFFICER Record X object. Now the record is ready for admittance to the statutory promotion board.

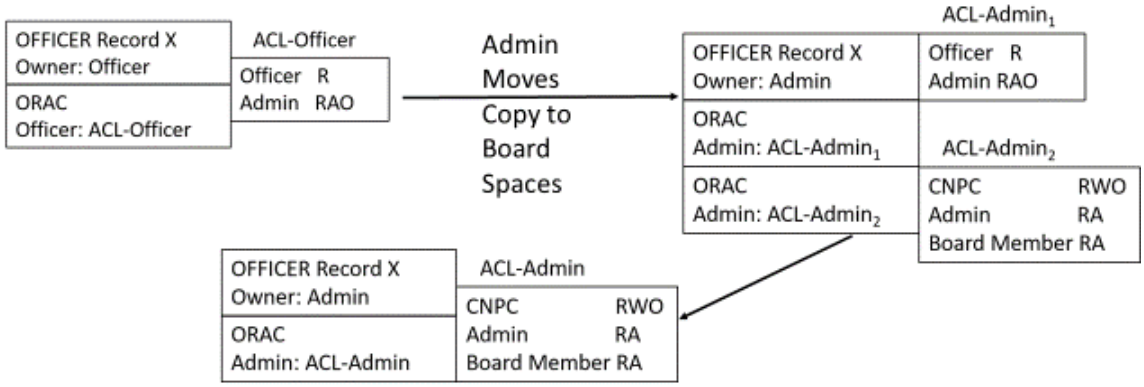


Figure 16. Orcon Process for Request of Record from Officer

Now consider Figure 16. Officer electronically submits a record object for admittance. The object's ACLs give the Officer read permissions, and Admin read, write and ownership permissions. Note that this object exists to represent the officer's electronic submission of a copy of the record to the administrators working in the board spaces. Admin then exercises the ownership change permission in ACL-Officer to take control of ACL-Officer. Then Admin adds an ACL to the OFFICER Record X object, giving CNPC read, write, and ownership permissions, Admin read and append permissions, and Board Member read and append permissions. Admin then removes the original ACL from the OFFICER Record X object, leaving it with only the new ACL that Admin had added to the OFFICER Record X object. The record object at this point is ready to be admitted to the statutory promotion board.

The result of the operations in Figure 15 and 16 is a record object that is allowed to be admitted into the statutory promotion board. An important distinction to make at this point between OFFICER Record X and OFFICER ODC-COPY is that the owner of OFFICER Record X is Admin and not CNPC. This distinction establishes the scope for which the new record object can be used and reflects its impermanence in the BUPERS

record system. This distinction will be further clarified in the resolution step of the model.

3. Admittance of Records

Figure 17 illustrates the end-state of the metadata after the request and admittance steps have been completed.

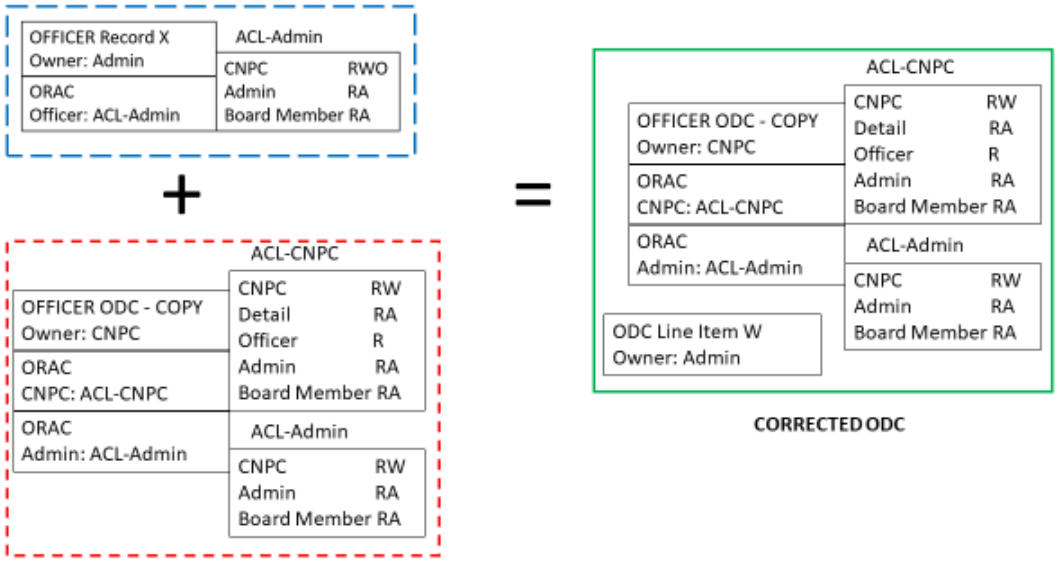


Figure 17. Corrected State of ODC

The upper left corner of Figure 17 is the admitted record object that was built during the request step. The entire record object is not needed to be admitted to the promotion board. Looking back to Figure 12, remember that only the necessary line items from the corresponding records are used. The admitted records added to the original board ODC object will follow this same principle. The necessary line item is extracted from the record object by user-group Admin and appended to the ODC object for use for the remainder of the promotion board. When an ODC is corrected during the promotion board process, the same admittance steps are used. The newly admitted line item exists in parallel with the incorrect line item in OFFICER ODC-COPY, but the newly admitted line item is considered valid while the original, incorrect line item is considered invalid. The newly admitted line item inherits the ACL associated with the container the ODC exists in.

4. Resolution

The resolution step involves the post-board procedures regarding the ODC object for which a line item has been appended as a result of information that was missing or incorrect in the original OFFICER ODC object at the time the board convened.

The OFFICER ODC object was only used in this entire model to act as the point of origination for the copy to be made for use in the promotion board. All operations in the model are on the OFFICER ODC-COPY object. This results in a corrected OFFICER ODC-COPY object, but not in the correction of the original OFFICER ODC object.

The OFFICER ODC-COPY object is stored locally in the board spaces until the results of the board have been disclosed. At this point, OFFICER ODC-COPY is deleted. Corrections to OFFICER ODC-COPY will also be lost. For the OFFICER ODC object to be updated, the record containing the line item of previously missing or corrected information must be submitted for correction through standard processes.

E. SUMMARY

This chapter built an Orcon process model based upon two scenarios constructed in Chapter III. Existing physical processes for the admittance of records to statutory promotion boards due to missing or incorrect information were described in a logical access control model so that computers can be used to support those processes. This model reflects a use case with actors who are compliant with all rules and act accordingly. Tools, such as blockchain, which are used to build integrity and security in an application, may be useful when the threats from Chapter IV are introduced to this Orcon process model. This will be the topic of the next chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. BLOCKCHAIN USE CASE ANALYSIS

The purpose of this chapter is to define and analyze a blockchain-based audit mechanism to act as a deterrent to the threat modeled in Chapter IV. We believe that an audit mechanism for accountability of ODC accesses and modifications would help mitigate threats described in Chapter IV. The proposed blockchain audit mechanism is based on the underlying transactions being built from access and modification transactions on ODC objects. A functional and security analysis will examine the efficacy of using a blockchain mechanism to provide auditing to support the ODC Orcon dissemination restrictions. The analysis will discuss the strengths and weaknesses of the proposed solution for the defined scenarios from a technical point of view and will assess whether a blockchain solution would be beneficial within the context of the scenarios and Orcon model presented here.

A. THE VALUE OF AUDITING

We propose auditing to address the threats introduced by insiders. The threat model for this scenario was defined as an insider acting against an ODC, altering its state to a state that does not accurately reflect the correct state of the ODC or violating the dissemination policies for the ODC. Because the threat is an insider, it is assumed that they have authenticated access to the systems on which unauthorized actions are carried out. There could be a single incorrect action amidst thousands of correct actions, which translates to one incorrect transaction amidst thousands of legitimate transactions. Note that the audit mechanism described here only supports audit logging, not audit analysis, and an incorrect action is not identified as unauthorized and will not be flagged as invalid. The execution of the unauthorized action cannot be prevented.

A benefit of an audit mechanism is that it is able to deter the insider threat by keeping track of all accesses and modifications to ODCs. A central audit server and a blockchain audit mechanism are able to create a timestamped and signed audit trail. Audit mechanisms offer a forensic audit trail of accesses and modifications to an ODC, from the time of its initial creation to the current time. Therefore, the one improper transaction

logged can be traced back to the exact time when the action took place, and a user can be associated with the specific transaction. Hence, evidence will be available that could be used to identify and possibly prosecute the insider.

Invalid transactions cannot be discovered by audit mechanisms, so the transaction must first be discovered by other means. Once it has been discovered, audit mechanisms offer enough information to recreate a valid ODC. Compare this to the existing system that only stores the current state of the ODC, and does not store previous transactions performed on ODCs. The current system is vulnerable to the threat of unauthorized modification of the ODC and does not provide a method for restoring the correct state of the ODC, other than attempting to piece together a new, correct ODC by hand. Audit mechanisms offer a way to restore a previous version of the ODC that the current process cannot effectively achieve

B. BLOCKCHAIN AUDIT MECHANISM

In this section, the implementation of the audit application will rely on blockchain technology. When considering blockchain as an audit mechanism within the context of the scenarios defined in Chapter III, multiple approaches can be considered. The mechanism can audit who accessed the information, the mode of access to the information, the time of access, and the state of an ODC. A blockchain can be used to create an audit trail of accesses and modifications to an ODC. It able to store a log of all transactions in its associated ledger, and the integrity of the logs can be verified as the blockchain grows. Storing the state through modification transactions creates the benefit of being able to track all iterations of an ODC object and the users associated with individual modifications.

Revision numbers are an additional desired outcome of Chapter III and can be accomplished by binding timestamps with ODC state in the audit trail. The revision number desired outcome was determined to benefit in the tracking of ODC state over time. By binding timestamps with ODC state in a blockchain audit mechanism, all ODC modifications can be tracked sequentially without the need to change the structure or

contents of an ODC by including revision numbers, yet still satisfying the outcome of the addition of revision numbers.

Using blockchain technology as an audit mechanism would make it possible to provide integrity to the access and modification logs associated with ODCs. If an ODC had been disseminated in violation of policy, the blockchain could provide evidence as to who may have performed the unauthorized action. The proposed blockchain audit mechanism will provide this capability, which can act as a deterrent to the insider threats modeled in Chapter IV. The main blockchain components to be used are described below.

1. Type of Blockchain Used

We must determine if the blockchain should be public or private. The systems in use for the Orcon process model have specific access controls and are located in physical spaces that require specific authorization for access. In addition, privacy controls protect the material being accessed. Thus, a private blockchain appears to be most appropriate. The private blockchain for this use case will be owned by CNPC and would give explicit permission to users and user-groups to view the blockchain and its contents in accordance with privacy rights and ODC policies.

Next, we must determine whether the proposed blockchain should be permissioned or not. The physical process for access to PII held within systems used for statutory promotion boards is handled through a SAAR-N, as described in Chapter III. This vetting process for access to information is best translated to the proposed blockchain application using a permissioned blockchain. For this use case, CNPC gives permissions to a user-group of employees who will participate in consensus and create blocks. Users and user-groups who wish to create transactions will be granted permission by means of official orders or via authenticated access to ODCs or digital ODC resources through web interfaces.

2. Transactions

Transactions comprise the data that is recorded in the blocks of a blockchain. Thus, an ODC-handling audit transaction must first be defined. In accordance with the Orcon process model of Chapter V, users or user-groups will access or modify ODC objects. These actions can be translated into one of two transaction types for use in the blockchain audit mechanism.

The first transaction type is an access transaction. This transaction will record the users who access an ODC. Not all ODC accesses will be recorded in the ledger, as this would clutter the ledger with redundant actions. Instead, access transactions will be added to the ledger with a level of granularity that will make each transaction meaningful within the context of auditing, while accurately reflecting the ODC access patterns of specific users. An access transaction will consist of the user accessing the ODC, the time of the access action, and the name of the ODC object being accessed.

The second transaction type is an ODC modification transaction. All modification transactions will be recorded in the ledger. ODC modification transactions consist of the time of the modification, the user who performed the modification action, and a snapshot of the ODC object after the modification action. These transactions allow tracking of changes to ODCs over time and can attribute all modifications to ODCs to specific users. This will create an accountability record of users who have modified ODC objects.

Other special actions to an ODC, such as its creation and its retirement, will also be considered transactions that will be recorded in the ledger and blockchain. Users are vetted prior to being able to access or modify ODCs, either through a SAAR-N or CAC authentication on web interfaces.

3. Consensus

The second key feature of a blockchain application is its consensus method. This requires two choices. The first is the type of consensus method to be used. The second is who can participate in consensus. The second consideration is essential for permissioned blockchains.

All consensus models require a tradeoff between security and cost. Consider proof-of-work. With fewer nodes participating in proof-of-work, the blockchain is less secure. The blockchain loses security because malicious nodes may dominate or collude to gain control over consensus when fewer total nodes participate in consensus. If malicious nodes were able to gain control of consensus, they would be able to determine the creation of new blocks and could modify previous blocks, breaking the immutability of the blockchain. When many nodes are participating in proof-of-work, the blockchain becomes more secure, because malicious nodes have less total influence in consensus. However, proof-of-work is expensive at large scales [18] because in proof-of-work, many nodes compete to solve a proof puzzle for a block, which results in redundant, computationally intensive work. Other blockchain consensus models exist, such as practical Byzantine fault tolerance [36]. Each consensus method has its own advantages and disadvantages and requires tradeoffs. Determining a consensus model requires familiarity with systems and users participating in consensus.

For the purpose of this work, the actual consensus model will not be discussed, because it is not a critical factor in determining the applicability of a blockchain for ODC auditing. The decision for a consensus model is left to the implementation of the proposed application.

Not all users generating transactions in a blockchain application must also participate in the consensus mechanism required to construct new blocks. This is a critical feature in a permissioned blockchain. For the Orcon process model, there are regular users and permissioned users within the context of statutory promotion boards. CNPC owns the ODC, and would also own the blockchain audit mechanism. CNPC must determine a group of users who on its behalf, will participate in consensus for block creation. The number of users can be small since the number of transactions in the blockchain is small in comparison to popular cryptocurrency applications. The users selected to participate in consensus should not have regular access to ODCs, and should not be creating transactions. This will allow for the audit mechanism to better act as an accountability tool because the users participating in consensus are distinct from those who are generating transactions as a result of ODC accesses and modifications.

4. Software Suite

Blockchain technology relies on a software suite to manage the ledger, transactions, and consensus. The software suite interacts with the system, the user, and the peer-to-peer network that constructs and maintains the blockchain. All systems used that fall under the jurisdiction of the Orcon process model of Chapter V will run the software and participate in the peer-to-peer network. This software can be interposed between user interfaces and software that interacts with ODCs to generate transactions from associated actions.

The Orcon process model built in Chapter V defined specific users and user-groups who interact with ODC objects during the process of statutory promotion boards. For the purpose of statutory promotion boards, user-group Admin can act on behalf of user Officer and user-group Board Member for all actions that take place within the board spaces.

C. ANALYSIS OF BLOCKCHAIN APPLICABILITY

This section will discuss the applicability of the proposed blockchain solution. While a blockchain solution cannot ensure the integrity or confidentiality of ODCs, it can allow for the recovery from modification errors and can help ensure the integrity of the audit record. There are several points in an ODC's history when auditing is recommended. This helps detect and deter unauthorized actions by insiders. The analysis examines how the blockchain mechanism meets the desired outcomes of Chapter III and the scalability and throughput of a blockchain approach. A comparison of the proposed blockchain audit mechanism to traditional auditing performed by a central audit server is made, and a recommendation is given regarding the implementation of an audit mechanism for use in auditing ODC accesses and modifications.

1. Desired Outcome Analysis

Chapter III defined the desired outcomes for the scenarios revolving around the ODC. The primary desired outcome from the scenarios was to have the ODC correctly updated with corrected information from supporting documents, and for the overarching

BUPERS database to reflect the time and detail of the ODC update. Modification transactions also include a snapshot of the current ODC. The transaction would contain the ODC snapshot post modification. The blockchain audit mechanism is not able to verify that the admitted records are correct but does provide the user associated with every transaction. Should an ODC be discovered to be incorrect or unauthorized disclosure of an ODC occur, this audit mechanism can provide a subset of users who accessed or modified a specific ODC as a list of potential suspects who performed the unauthorized Action. In the case of Figure 18, Action C shows an error inserted in the ODC, and Action E shows unauthorized dissemination. Action E is not recorded in the audit trail. The audit mechanism can be used to determine that user Y made the incorrect modification, and at least one of the group of users Z who performed Action D disseminated the ODC without authorization.

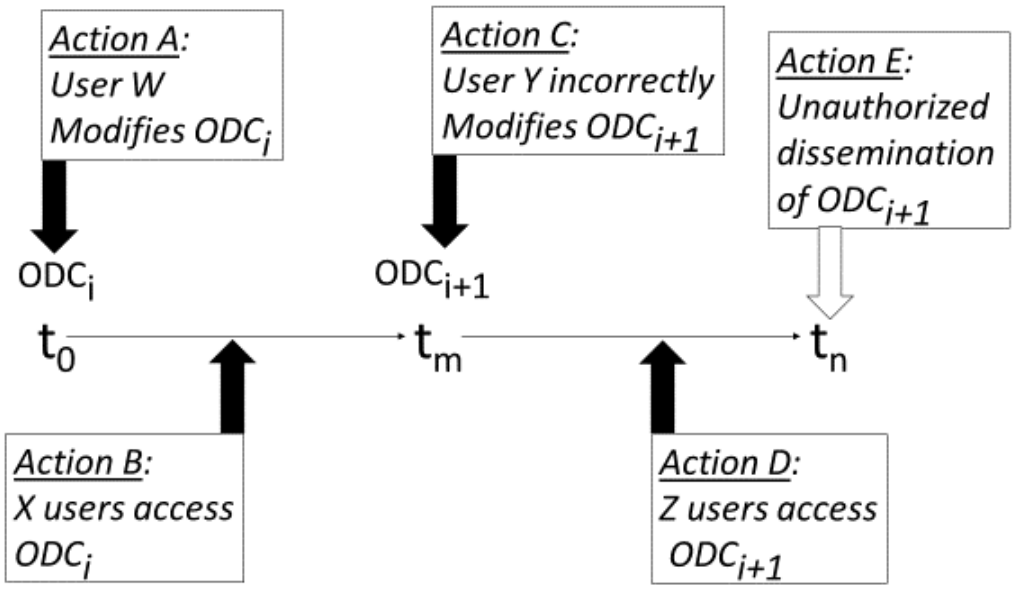


Figure 18. Example Blockchain Audit Mechanism Usage

Chapter III also defined two additional desired outcomes that are not reflected by current processes in the defined scenarios. The first is to have revision numbers added to ODC documents, providing a sequential number for an officer's ODC. The proposed

blockchain solution is able to satisfy this additional desired outcome by linking timestamps with ODC states, without having to add an actual revision number to the ODC document. Whenever a modification is made to an ODC, a modification transaction would incorporate a timestamp for the transaction. This can be seen in Figure 18 where ODC_i is associated with Action A, and ODC_{i+1} is associated with Action C. This feature of the proposed solution creates an additional benefit to the overall ODC management process.

The second additional desired outcome is to allow for modification to the ODC to be made during the promotion board process, and have it reflected in both the ODC used during the promotion board and the ODC for permanent use within the BUPERS database. Recording modifications made during a promotion board as transactions in the ledger would allow the local change in the board spaces to be stored in the ledger for the ODC. Because transactions only log modifications, the BUPERS database still needs to be updated to reflect the change made during the promotion board logged in the audit mechanism. The blockchain audit mechanism cannot implement this additional desired outcome.

2. Scalability and Throughput

The proposed blockchain solution has nodes set up in the peer-to-peer network on multiple systems within Naval Personnel Command in Millington, TN. These nodes are in communication with each other, sending transactions and blocks between those participating in consensus and block creation across the network. This requires a specific throughput of information on a consistent basis in order to be able to use the proposed solution reliably. One limitation of blockchain solutions is scalability [36]. According to the Navy Fact File, there are approximately 54,000 active duty U.S. Navy officers [37]. ODCs are updated a minimum of once a month per officer, and the average size of an ODC PDF document is assumed to be 90KB. Figure 19 calculates and compares the number of transactions and amount of data required for the proposed solution as compared to the Bitcoin blockchain.

The Bitcoin blockchain stores 93.5 times the number of transactions in half of the space as the proposed ODC solution. While this inefficiency would seem to indicate a disadvantage in the proposed solution, these are performance estimates, and analysis and comparison testing will be needed to assess them for a real system.

	ODC	Bitcoin	
Bytes in PDF of ODC	90KB		
Transactions per Officer	* 15	0.72 MB	Size of Block
Number of Officers	* 54000	* 52560	Blocks per year
Data Size per year	72.90 GB	37.8 GB	

	ODC	Bitcoin	
Transactions per Officer	* 15	207500	Transactions per Day
Number of Officers	* 54000	* 365	Days per Year
Transactions per year	810000	75737500	

	ODC	Bitcoin	
Data Size per year	72.90 GB	37.8 GB	Data Size per year
Transactions per year	/ 810000	/ 75737500	Transactions per year
Data per Transaction	90 KB	0.50 KB	

Figure 19. ODC versus Bitcoin Throughput Comparison [38]

3. Comparison

Finally, the blockchain audit mechanism is compared to a central audit server. One of the main benefits of the proposed solution is the handling of concurrent usage of systems and creation of transactions. Rather than having all transactions sent to a central authority for verification, the proposed solution distributes the transactions across nodes, and the permissioned users who participate in consensus have the responsibility of

verification. The proposed solution solves the problem of a single point of failure for the system of auditing ODC documents. The proposed solution requires information to be passed within the peer-to-peer network for transactions, consensus and block formation. Testing is needed in order to assess the impact of peer-to-peer communication on network performance accurately. The blockchain is also able to provide integrity to the logs. When transactions deepen in the blockchain, it becomes increasingly difficult to change the transaction. An adversary would have to gain control over enough systems to control consensus to change a transaction. With the distributed verification and consensus of transactions added by means of a blockchain audit mechanism, a single point of failure is eliminated, and the overall system for tracking changes to ODCs becomes more resilient and secure.

A disadvantage of the blockchain approach is the increase in the total amount of data stored, as the entire audit log ledger has to be stored on all systems participating in consensus and block creation. The blockchain approach would also require acquisition of multiple systems to handle the auditing, consensus, and block creation. The cost of acquisition and implementation of these systems with respect to time and money would have to be analyzed to determine the feasibility of implementation.

A central server authority solution would handle all transactions to ODC documents and record the time-stamped, digitally signed transactions into a single log. The central solution would congregate all ODC accesses and modifications into a single log stored on the central audit server or stored on another system. The benefits of a centralized solution are its ease of implementation and the localization of all audit log information. The total storage needed for the central approach would be less than the blockchain approach, and cost and time to implement the solution would be less. A disadvantage of a central audit server is that if it were to go down, all auditing may be lost or halted for the duration of the server downtime. A backup server would be needed to provide resiliency. Therefore, the central solution is less costly and simpler, but potentially less resilient and secure.

4. Recommendation

The value of auditing has been discussed, and a possible blockchain audit mechanism has been described. The proposed blockchain audit has been analyzed against the desired outcomes defined in Chapter III, analyzed in its effectiveness in deterring the insider threats for ODC accesses and modifications, and compared to the current system to which a central audit server is added. This section provides a recommendation for existing U.S. Navy personnel record management systems based on the analysis.

The proposed solution is able to satisfy the required outcomes defined in Chapter III and is able to satisfy one of the two additional desired outcomes for managing ODCs. Timestamping ODC states in the blockchain helps show the progress of the record as it is updated through an officer's career. The path towards the reduction of redundancy in updating incorrect records during statutory promotion boards is also discussed.

The main advantages of the proposed blockchain audit mechanism are that it provides a way to account for insider threats, and it allows for the inclusion of the additional desired outcomes defined in Chapter III. Within the context of personnel record management of an organization of 54,000 employees, it is reasonable to assume the prospect of the mishandling of information from time to time. The proposed solution accounts for this happening and provides a way to recover the integrity of an incorrect record, and hold accountable users who mishandle sensitive personal record information. It does not assure that mistakes will not fall through the cracks but ensures that all errors can be associated with a time and a specific subset of users.

The main disadvantages of the proposed blockchain solution are the scalability of the solution and the overhead in implementing the solution on existing systems. Testing of implementation of the proposed solution would determine how large the peer-to-peer network can get before throughput is affected. No matter the size of the network, however, the proposed solution does increase the overall network traffic on the networks where the systems reside. Another disadvantage is the time and manpower required to implement the proposed solution. It requires that a software suite be installed on all participating systems. Any new system in the peer-to-peer network would be required to

install the software and download the ledger associated with the blockchain. Another disadvantage of the proposed solution is the size of ledger and blockchain over time. The ledger will grow over time and is stored locally on systems participating. The ledger and blockchain can be archived and reduced in size once deemed too large, keeping the memory usage for the online peer-to-peer systems low.

When considering the advantages and disadvantages of the proposed blockchain solution in the broader context of the U.S. Navy personnel record management system, the proposed solution appears to be overly complicated and impractical at this time, due to the need for implementation and testing of the entire system, the increase in data storage across all systems storing the blockchain, and the increase in network congestion from the peer-to-peer node traffic. Further research is needed to determine if the disadvantages of the solution can be mitigated or eliminated. A more practical immediate alternative would be to enable timestamped, digitally signed audit logging on a central server authority. This would be less cumbersome to implement compared to the blockchain solution and would require that only a single system be monitored and updated. The alternate method would support the desired outcomes and would integrate into existing systems.

D. SUMMARY

We discussed the value of auditing in addressing the issues posed by insiders, and determined that a blockchain or a central server can be used to audit ODC modifications and dissemination control. Using the Orcon process model built in Chapter V, a blockchain solution was analyzed as a deterrent to partially mitigate insider threats to the confidentiality and integrity of ODCs. While the proposed solution cannot prevent the alteration of the ODC, it provides an immutable audit trail of accesses and modifications to the ODC and should support the proper recreation of a correct ODC. Advantages and disadvantages of the proposed blockchain solution were analyzed, and a recommendation regarding its pursuit was given: a blockchain is not the best immediate solution to the threat posed to the ODC Orcon process model. Advances in blockchain technology could

make it a more viable option in the future. A recommended alternative is to enable timestamped, digitally signed audit logging on a central server authority.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION

The purpose of this chapter is to provide a summary of this work and to provide recommendations for future work based on the findings of this work.

A. SUMMARY

This work investigated the policy for accesses, modification and dissemination of ODCs, built a model for ODC dissemination during the process of statutory promotion boards and provided a potential blockchain audit mechanism that can be used to support accountability policy enforcement for personnel record handling within the U.S. Navy. This work built a model for ODC dissemination that has not been modeled before. This work also demonstrated the criticality of use case studies when researching the usability of new technologies. The analysis of the blockchain audit mechanism determined that blockchain might be an effective tool to deter potential insider threats. However, we also determined that the proposed blockchain solution introduced unnecessary redundancy and complexity relative to alternative solutions.

The ODC Orcon model provides a technical access control model for the dissemination control of ODCs during the statutory promotion board process. The ODC Orcon process model was based on the compilation of sources and authorities. The model also identified improvements to the process of handling the access control of ODCs and streamlining the process for record correction. This model can be used in future work on ODC dissemination control, record correction procedures, or statutory promotion board processes.

The threat model associated with the Orcon process model was not entirely countered by any proposed solutions in this work. The proposed audit mechanism is able to account for and act as a tool for assistance in recovery from attacks by insider threats, so their implementation to help mitigate the overall threat from this and other adversaries should be assessed.

This work considered the use of blockchain technology for a single use case. Even though blockchain technology is not deemed to be the best solution here, it may be well-

suited for other situations. Blockchain technology is evolving, and its underlying processes are still being improved. New developments in blockchain technology could mitigate the main disadvantages associated with the use case presented here, and re-examination of in the future may be prudent.

B. RECOMMENDATIONS FOR FUTURE WORK

This section describes the recommendations for possible future work. The two recommendations are: further testing of the proposed blockchain solution and future blockchain use case studies.

1. Implementation of Proposed Solution

This work proposed a blockchain solution for auditing a personnel record management process and analyzed it based on the principles of the technology, the current processes and systems. The next step in the research of this particular use case would be to implement the use case and study the real effects of the solution. The implementation could be compared to the findings of this work to determine how the solution actually behaves on the discussed systems and networks. This implementation would also provide a real use of blockchain technology as an audit mechanism for personnel record management.

2. Additional Use Case Studies

In the process of building and analyzing the use case presented here, new information on processes was learned, technologies were better understood, and recommendations could be made to improve processes. A systematic method for creating and analyzing use cases for blockchain technology is critical for thoughtful and accurate analysis of its value for specific situations. Use case studies should be constructed for other scenarios in order to determine critical system or process weaknesses and to further our application of the potential uses of blockchain technology within the DoD.

LIST OF REFERENCES

[1] *Department of the Navy Privacy Program*, SECNAVINST 5211.5E, Department of the Navy, Washington, DC, USA, 2005.

[2] U.S. House. 115th Congress. (2017, Jun. 7). H.R.2810, *National Defense Authorization Act for Fiscal Year 2018*, 2017. [Online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/2810/

[3] "BUPERS Online," United States Navy. Accessed February 2018. [Online]. Available: bol.navy.mil

[4] "About BUPERS," United States Navy. Accessed February 2018. [Online]. Available: http://www.public.navy.mil/bupers-npc/organization/bupers/ Pages/ default.aspx

[5] *The Manual of the Navy Officer Manpower and Personnel Classifications, Volume II, The Officer Data Card*, NAVPERS 15839I, Department of the Navy, Washington, DC, USA, 2017.

[6] "Electronic Submission (e-Submission) Standard Operating Procedures," United States Navy. Accessed February 2018. [Online]. Available: http://www.public.navy.mil/bupers-npc/career/recordsmanagement/Documents/ eSubmission%20SOP%20(V2).pdf

[7] "Records Management and Policy (PERS-313)," United States Navy. Accessed February 2018. [Online]. Available: http://www.public.navy.mil/bupers-npc/career/recordsmanagement/militarypersonnelrecords/pages/default2.aspx

[8] "Research in Military Records," National Archives. Accessed February 2018. [Online]. Available: https://www.archives.gov/research/military

[9] "Freedom of Information Act (FOIA) and The Privacy Act," National Archives. Accessed February 2018. [Online]. Available: https://www.archives.gov/st-louis/military-personnel/foia-info.html

[10] "Overview of the Privacy Act of 1947," United States Department of Justice. Accessed February 2018. [Online]. Available: https://www.justice.gov/opcl/ overview- privacy-act-1974-2015-edition

[11] *DoD Information Security Program: Marking of Classified Information*, Department of Defense Manual 5200.01, vol. 2, Department of Defense, Washington, DC, USA, 2013.

[12] *Intelligence Community Policy Guidance 710.1, Application of Dissemination Controls: Originator Control*, Office of the Director of National Intelligence, July 25, 2012. [Online]. Available: https://fas.org/irp/dni/icd/icpg710-1.pdf

[13] *Department of Defense Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, Department of Defense, Washington, DC, USA, 1985.

[14] R. Graubart, "On the need for a third form of access control," *Proceedings of the 12th National Computer Security Conference*, pp. 296–303, Baltimore, MD, USA, 1989.

[15] C. J. McCollum, J. R. Messing and L. Notargiacomo, "Beyond the pale of MAC and DAC—defining new forms of access control," *IEEE Computer Society Symposium on Research in Security and Privacy*, 1990.

[16] S. Nakamoto, "Bitcoin: A Peer-to-peer electronic cash system," 2008. [Online] Available: https://bitcoin.org/bitcoin.pdf

[17] A. Narayan and J. Clark, "Bitcoin's academic pedigree," *Communications of the ACM*, vol. 60, no. 12, pp. 36–45, 2017.

[18] T. Smith, "The blockchain litmus test," *IEEE Conference on Big Data*, Boston, 2017.

[19] A. Kaushik, "Blockchain - literature survey," *IEEE International Conference on Recent Trends in Electronics, Information, & Communication Technology*, Bengaluru, 2017.

[20] K. Panetta, "Top trends in the Gartner Hype Cycle for emerging technologies, 2017," Gartner, August 15, 2017. [Online]. Available: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

[21] R. C. Merkle, "Protocols for public key cryptosystems," *1980 IEEE Symposium on Security and Privacy (SP)*, Oakland, CA, 1980, pp. 122. [Online]. doi:10.1109/SP.1980.10006

[22] "Hash Pointers and Data Structures," E-Learning Spot, November 28, 2016. [Online]. Available: http://learningspot.altervista.org/hash-pointers-and-data-structures/?doing_wp_cron=1526257314.3044140338897705078125

[23] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *Conference on the Theory and Application of Cryptography*, 1990.

[24] S. Haber and W. S. Stornetta, "Secure names for bit-strings," *ACM Conference on Computer and Communications Security*, Zurich, 1997.

[25] L. Lamport, R. Shostak and M. Pease, "The Byzantine general's problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.

[26] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," *Third Symposium on Operating Systems Design and Implementation*, New Orleans, 1999.

[27] C. Cachin et al., "Hyperledger Fabric: a distributed operating system for permissioned blockchains," *Proceedings of EuroSys 2018 Conference*, January 30, 2018. [Online]. doi:10.1145/3190508.3190538

[28] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Upper Saddle River, NJ, USA: Prentice Hall, 1999.

[29] "Active Duty Officer Promotions," U.S. Navy, April 24, 2018. [Online]. Available: http://www.public.navy.mil/bupers-npc/boards/activedutyofficer/Pages/default.aspx

[30] B. Rostker, H. Thie, J. Lacy, J. Kawata and S. Purnell, "The Defense Officer Personnel Management Act of 1980: a retrospective assessment," Santa Monica, CA, USA, 1993.

[31] "Administrative Boards," U.S. Navy, May 25, 2017. [Online]. Available: http://www.public.navy.mil/bupers-npc/boards/administrative/Pages/default.aspx

[32] "Board membership: FY-18 active duty Navy Lieutenant Commander line promotion selection boards," November 29, 2017. [Online]. Available: http://www.public.navy.mil/bupers-npc/boards/activedutyofficer/04line/Documents/FY-18%20AO4L%20MEMBERSHIP.pdf

[33] C. Good, interview, Mar. 2018.

[34] "Application threat modeling," OWASP, May 31, 2017. [Online]. Available: https://www.owasp.org/index.php/Application_Threat_Modeling#Threat_Model_Information

[35] "Cybersecurity incidents," Office of Personnel Management, 2015. [Online]. Available: https://www.opm.gov/cybersecurity/cybersecurity-incidents/

[36] M. Vukolic, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," *Open Problems in Network Security*, 2015.

[37] "Status of the U.S. Navy," U.S. Navy Accessed May 10, 2018. [Online]. Available: http://www.navy.mil/navydata/nav_legacy.asp?id=146

[38] "Bitcoin Charts & Graphs," Blockchain Luxembourg S.A. Accessed May 10, 2018. [Online]. Available: https://blockchain.info/charts

[39] V. L. Lemieux, “A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation,” *IEEE International Conference on Big Data*, Boston, MA, USA, 2017.

[40] J. Park and R. Sandhu, “Originator control in usage control,” *Proceedings Third International Workshop on Policies for Distributed Systems and Networks*, Monterey, CA, USA, 2002.

[41] Z. Zheng, S. Xie, H.-N. Dai, X. Chen and H. Wang, “Blockchain challenges and opportunities: a survey,” *International Journal of Web and Grid Services*, 2017.

[42] G. Zyskind, “Decentralizing privacy: using blockchain to protect personal data,” *IEEE Security and Privacy Workshops*, 2015.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California