



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

CAPSTONE APPLIED PROJECT REPORT

SOFTWARE BILL OF MATERIALS: A CATALYST TO A MORE SECURE SOFTWARE SUPPLY CHAIN

December 2023

By: **Phillip Q. Nguyen**
 Madison A. Tikalsky
 Samantha M. Durlauf

Advisor: **Daniel J. Finkenstadt**
Co-Advisor: **Jamie M. Porchia**

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE December 2023	3. REPORT TYPE AND DATES COVERED Capstone Applied Project Report	
4. TITLE AND SUBTITLE SOFTWARE BILL OF MATERIALS: A CATALYST TO A MORE SECURE SOFTWARE SUPPLY CHAIN			5. FUNDING NUMBERS	
6. AUTHOR(S) Phillip Q. Nguyen, Madison A. Tikalsky, and Samantha M. Durlauf				
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) This MBA innovation capstone project investigates cyber supply chain security, emphasizing targeted incidents within the United States. It encompasses Hacking for Defense (H4D), innovation capstone initiatives, and system dynamics modeling, culminating in Minimum Viable Product (MVP) development. Aligned with the “Back-to-Basics” restructuring initiative and Executive Order 14028, the research aims to enhance cyber supply chain security in line with three core objectives: validating the EITaaS Program Office’s problem statement, identifying potential solutions, and offering informed recommendations. Methodologies include the Lean Launchpad, working groups, the goals-decisions-signals-data model, and system dynamics. Findings present advanced tools for EITaaS Supply Chain Risk Management, with implications for national security. The study underscores the importance of Software Bills of Materials (SBOM) in DOD’s software supply chain risk management. Effective SBOM implementation is crucial for strengthening the nation’s cyber defense infrastructure. The research outlines a roadmap for improving cyber supply chain security, reducing cyberattacks, and minimizing economic losses, advocating for the implementation of an SBOM policy. It concludes with actionable recommendations for SBOM implementation, covering education, collaboration, best practices, process framework development, and DOD-specific SBOM standards.				
14. SUBJECT TERMS SBOM, cyber supply chain, cyber risk management, CDRL, DID, data visualization, visualization tools, H4D, software supply chain, software risk, system dynamics model, cyberattacks			15. NUMBER OF PAGES 131	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**SOFTWARE BILL OF MATERIALS: A CATALYST TO A MORE SECURE
SOFTWARE SUPPLY CHAIN**

Phillip Q. Nguyen, Captain, United States Air Force
Madison A. Tikalsky, Captain, United States Air Force
Samantha M. Durlauf, Captain, United States Air Force

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

**NAVAL POSTGRADUATE SCHOOL
December 2023**

Approved by: Daniel J. Finkenstadt
Advisor

Jamie M. Porchia
Co-Advisor

Rene G. Rendon
Academic Associate
Department of Defense Management

THIS PAGE INTENTIONALLY LEFT BLANK

SOFTWARE BILL OF MATERIALS: A CATALYST TO A MORE SECURE SOFTWARE SUPPLY CHAIN

ABSTRACT

This MBA innovation capstone project investigates cyber supply chain security, emphasizing targeted incidents within the United States. It encompasses Hacking for Defense (H4D), innovation capstone initiatives, and system dynamics modeling, culminating in Minimum Viable Product (MVP) development. Aligned with the “Back-to-Basics” restructuring initiative and Executive Order 14028, the research aims to enhance cyber supply chain security in line with three core objectives: validating the EITaaS Program Office’s problem statement, identifying potential solutions, and offering informed recommendations. Methodologies include the Lean Launchpad, working groups, the goals-decisions-signals-data model, and system dynamics. Findings present advanced tools for EITaaS Supply Chain Risk Management, with implications for national security. The study underscores the importance of Software Bills of Materials (SBOM) in DOD’s software supply chain risk management. Effective SBOM implementation is crucial for strengthening the nation’s cyber defense infrastructure. The research outlines a roadmap for improving cyber supply chain security, reducing cyberattacks, and minimizing economic losses, advocating for the implementation of an SBOM policy. It concludes with actionable recommendations for SBOM implementation, covering education, collaboration, best practices, process framework development, and DOD-specific SBOM standards.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	BACKGROUND	1
B.	MOTIVATION	2
C.	WHAT IS H4D?	3
D.	THE SPONSORED PROBLEM	3
E.	CYBER SUPPLY CHAIN RISK.....	4
F.	WHAT IS AN SBOM?.....	4
G.	PROJECT OBJECTIVES.....	5
H.	CAPSTONE HYPOTHESIS.....	5
I.	SUMMARY	6
II.	SUMMARY OF STAKEHOLDERS.....	7
A.	ENTERPRISE INFORMATION TECHNOLOGY AS A SERVICE PROGRAM OFFICE.....	7
B.	DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER.....	8
C.	DEPARTMENT OF THE AIR FORCE CHIEF INFORMATION OFFICER.....	8
D.	FEDERAL AND DEFENSE AGENCIES	9
	1. Department of Homeland Security.....	9
	2. Cybersecurity and Infrastructure Security Agency	10
	3. National Institute of Standards and Technology	11
E.	WARFIGHTER	11
F.	CONTRACTORS	11
G.	SUMMARY	12
III.	SUMMARY OF METHODOLOGY.....	13
A.	HACKING 4 DEFENSE.....	13
B.	WORKING GROUPS	14
C.	GOALS, DECISIONS, SIGNALS, AND DATA	16
D.	SYSTEMS DYNAMICS.....	18
IV.	H4D PROJECT	19
A.	PROBLEM DISCOVERY	19
B.	FIRST MVP ITERATION.....	21
C.	SECOND MVP ITERATION.....	23

D.	H4D FINAL MVP	24
E.	VALIDATED PROBLEM STATEMENT	28
V.	SBOM DISCOVERY POST H4D	31
A.	UNDERSTANDING SBOMS	31
B.	EXISTING SBOM FORMATS	32
C.	IDENTIFYING VULNERABILITIES	35
D.	MAPPING VULNERABILITIES TO SOFTWARE RISK CATEGORIES.....	36
E.	WORKING GROUPS	39
F.	SUMMARY	40
VI.	FINAL MVP: SBOM DASHBOARD PROTOTYPE	43
A.	FINAL MVP HYPOTHESIS	43
B.	NPS SBOM DASHBOARD MVP	43
1.	SBOM Development	43
2.	SBOM Repository	44
3.	SBOM Digestion.....	45
4.	SBOM Dashboard.....	49
5.	MVP Results.....	52
6.	Final MVP Summary.....	53
VII.	SYSTEM DYNAMICS SBOM POLICY MODEL.....	55
A.	SBOM CAUSAL LOOP DIAGRAM	56
1.	AF IT Acquisition Loop.....	58
2.	AF Security Loop	59
3.	Contractor Software Security Loop	60
4.	AF Supply Chain Risk Management Loop.....	60
5.	AF Contracts Loop	61
6.	AF IT Manpower Loop	61
B.	SBOM SIMPLE SYSTEM DYNAMICS MODEL	61
1.	U.S. Economy and DOD Budget Model Section.....	63
2.	AF Defense Budget Model Section	65
3.	AF Cybersecurity Manpower Budget Model Section.....	67
4.	AF IT Procurement Budget Model Section	70
5.	Cyberattacks and Economic Damage Model Section	72
6.	AF Total IT Expenditure Model Section	75
7.	Model Interface	76
C.	FINDINGS AND ANALYSIS	77

D.	MODEL LIMITATIONS AND FUTURE RESEARCH.....	83
VIII.	ROADMAP AND RECOMMENDATIONS FOR THE DOD	85
A.	EDUCATION OF INTERNAL STAKEHOLDERS	85
B.	COLLABORATION AMONG STAKEHOLDERS.....	87
C.	COLLECTION, ADOPTION AND IMPLEMENTATION OF BEST PRACTICES	89
D.	DEVELOP A SOFTWARE RISK MANAGEMENT FRAMEWORK.....	90
E.	CREATION OF AN INCLUSIVE SBOM STANDARD	91
IX.	LIMITATIONS AND FUTURE RESEARCH.....	93
A.	INFORMATION DISSEMINATION AND SBOM TRAINING PROGRAMS	93
B.	SBOM RETENTION AND REPOSITORY PROCEDURES	94
C.	SBOM FORMAT DEVELOPMENT.....	95
D.	ADVANCEMENT OF DASHBOARDING CAPABILITIES	96
E.	OPTIMIZATION OF DATA VISUALIZATION	97
X.	CONCLUSION	99
	APPENDIX. H4D MISSION MODEL CANVAS.....	101
	LIST OF REFERENCES.....	103
	INITIAL DISTRIBUTION LIST	109

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Analysis of CISA. Source: GAO (2023).....	10
Figure 2.	Build-Measure-Learn Feedback Loop. Source: Ries (2011)	14
Figure 3.	GDSD Model. Source: Finkenstadt et al. (2022).....	16
Figure 4.	SCRM Process Flowchart. Adapted from AFLCMC/LG-LZ (2021).....	22
Figure 5.	Final H4D MVP SBOM Standardization Collaboration	26
Figure 6.	Final H4D MVP Vision: SCBI Collaboration Hub.	27
Figure 7.	FY22 AFLCMC Annual Logistics Functional Team Award Presentation.....	29
Figure 8.	NTIA required SBOM elements. Source: NTIA (2021b).....	32
Figure 9.	Title of attributes for each SBOM type. Source: NTIA (2021c)	34
Figure 10.	SBOM GDSD	36
Figure 11.	Syft Mac Terminal Commands Adapted from Apple Inc., (2022b)	44
Figure 12.	Zotero Generated SBOM in File Folder Repository. Adapted from Apple Inc. (2022a)	45
Figure 13.	Zotero in CycloneDX Version 1.4 SBOM Format as .json File Type. Source: Apple Inc (2022c)	46
Figure 14.	ChatGPT Sample Prompt for Python Coding Assistance. Adapted from OpenAI (2023)	47
Figure 15.	SBOM Extraction Python Code. Adapted from Python Software Foundation (2023).....	48
Figure 16.	NPS SBOM Dashboard V1.0 (CycloneDX) Interface.....	49
Figure 17.	NPS SBOM Dashboard Filter Feature.....	50
Figure 18.	Component HikariCP Version 4.0.3. Source: Rodriguez Olivera (2023).....	51
Figure 19.	Component Search Feature	52
Figure 20.	NPS: Full SBOM Demo with Dialogue. Source: Nguyen (2023b)	53

Figure 21.	SBOM CLD. Adapted from ISEE Systems (2023)	57
Figure 22.	AF IT Acquisition CLD Section. Adapted from ISEE Systems (2023).....	58
Figure 23.	AF Software Security CLD Section. Adapted from ISEE Systems (2023).....	59
Figure 24.	SBOM System Dynamics Model. Adapted from ISEE Systems (2023).....	63
Figure 25.	U.S. Economy and DOD Budget Model Section. Adapted from ISEE Systems (2023).....	64
Figure 26.	U.S. AF Budget Model Section Adapted from ISEE Systems (2023).....	66
Figure 27.	AF Cybersecurity Manpower Budget Section. Adapted from ISEE Systems (2023).....	67
Figure 28.	AF IT Procurement Budget Section. Adapted from ISEE Systems (2023).....	70
Figure 29.	Cyberattacks and Economic Damage Model. Adapted from ISEE Systems (2023).....	72
Figure 30.	AF Total IT Expenditure Section. Adapted from ISEE Systems (2023).....	75
Figure 31.	Software Bill of Material System Dynamics Model Interface. Adapted from ISEE Systems (2023).....	77
Figure 32.	U.S. Economy, DOD Budget, AF Budget Sector Results. Adapted from ISEE Systems (2023)	78
Figure 33.	AF Cybersecurity Procurement and Manpower Budget Sector Results. Adapted from ISEE Systems (2023).....	79
Figure 34.	With and Without SBOM Policy Run Results. Adapted from ISEE Systems (2023).....	80
Figure 35.	With SBOM Policy Run Results. Adapted from ISEE Systems (2023).....	81
Figure 36.	Without SBOM Policy Run Results. Adapted from ISEE Systems (2023).....	82

LIST OF TABLES

Table 1.	H4D Interviews and Main Takeaways.....	20
Table 2.	Crosswalk for MITRE Risk Categories to DOD Risk Categories.....	37
Table 3.	U.S. Economy and DOD Budget Elements	64
Table 4.	AF Defense Budget Elements.....	66
Table 5.	AF Cybersecurity Manpower Budget Elements	68
Table 6.	AF IT Procurement Budget Elements.....	71
Table 7.	Cyberattacks and Economic Damage Elements	73
Table 8.	AF Total IT Expenditure Elements.....	76

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AFLCMC	Air Force Life Cycle Management Center
AFSC	Air Force Specialty Code
BPA	blanket purchase agreement
CDX	CycloneDX
CIO	chief information officer
CISA	Cybersecurity and Infrastructure Security Agency
CLD	causal loop diagram
DAF	Department of the Air Force
DOD	Department of Defense
EITaaS	enterprise information technology as a service
FY	fiscal year
GAO	Government Accountability Office
GDP	Gross Domestic Product
GDSD	goals, decisions, signals, and data
H4D	Hacking for Defense
HBOM	hardware bill of materials
IT	information technology
MBA	Master of Business Administration
MVP	minimum viable product
NAVAIR	Naval Air Systems Command
NIST	National Institute of Standards and Technology
NPS	Naval Postgraduate School
NTIA	National Telecommunications and Information Administration
SBOM	software bill of materials
SCBI	supply chain business intelligence
SCRM	supply chain risk management
SPDX	Software Package Data Exchange

SWID

Software Identification

USD (A&S)

Under Secretary of Defense for Acquisition and Sustainment

ABOUT THE AUTHORS

Capt Phillip Nguyen is an officer working in the U.S. Air Force contracting career field. He graduated from Wingate University, NC, with a Bachelor of Science in Business Finance and commissioned in the Air Force in 2016 through Officer Training School. Upon graduating in December 2023, he has follow-on orders to the Space Force's Space Systems Command located in Los Angeles, CA.

Capt Madison Tikalsky is an officer working in the U.S. Air Force contracting career field. She graduated from Clarkson University, NY, with a Bachelor of Science in Engineering and Management and was commissioned in the Air Force in 2019 through Reserve Officer Training Corps. Upon graduating in December 2023, she has follow-on orders to the 763rd Enterprise Sourcing Squadron located at Scott AFB, IL.

Capt Samantha Durlauf is an officer working in the U.S. Air Force contracting career field. She was commissioned after serving five years as an enlisted Air Force member specializing in contracting. Prior to that, she graduated from the University of West Florida with a Bachelor of Science in Interdisciplinary Social Sciences. Upon graduating in December 2023, she has follow-on orders to Wright-Patterson Air Force Base in Dayton, Ohio, where she will be working with the 771st Enterprise Sourcing Squadron.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

We would like to express our profound gratitude to our spouses, Nektarios and Cindy, as well as Samantha's son, Grayson, and Madison's dog, Midas, for their unwavering support throughout the research and development phases of this project. Our heartfelt thanks go to our advisors, Lt Col Daniel Finkenstadt and Lt Col Jamie Porchia; their guidance and encouragement were indispensable to the realization of this work. Our appreciation also extends to the EITaaS Program Office for their collaboration and sustained backing. We are professionally indebted to the commands that contributed data and insights. Lastly, we are grateful to NPS, its faculty, and fellow students for the enriching journey during our MBA program.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In this chapter, we shed light on a series of significant cyber supply chain incidents that have specifically targeted the United States. These incidents underscore the severe consequences of such attacks, spanning from their detrimental impacts on national security to economic stability and technological infrastructure. These adverse effects, coupled with our professional responsibilities and academic insights, provide the foundation for addressing this intricate issue. Throughout the upcoming sections of this paper, we delve into the findings stemming from our Hacking for Defense (H4D) project, the subsequent innovation capstone project, and our system dynamics modeling project. Our exploration encompasses the development of a minimum viable product (MVP), a system dynamics model and strategic initiatives aimed at fostering collaboration between the enterprise information technology as a service (EITaaS) program and the Department of Defense (DOD) Chief Information Officer (CIO), ultimately leading to recommendations centered on software bills of materials (SBOMs). Our overarching objective is to drive innovation and enhance the available mechanisms for safeguarding the cyber supply chain, thereby contributing to the resilience of our national defense framework.

A. BACKGROUND

The United States persistently grapples with detrimental cyber campaigns, infiltrating both public and private sectors, posing threats to personal privacy, economic stability, and national security. A report from the Government Accountability Office (GAO) revealed that the DOD was subjected to over 12,000 cyber incidents between 2015 and 2021 (Kirschbaum & Franks, 2022). That same report found an alarming 97.7% of these incidents were classified as malicious logic attacks. This form of cyberattack involves the deployment of adversary-designed software aimed at unauthorized access to resources or confidential information, unbeknownst to the user (Kirschbaum & Franks, 2022).

In 2021, a significant cybersecurity breach hit the Colonial Pipeline, the largest U.S. pipeline system for refined oil products. A crippling ransomware attack led to a 5-day disruption of the nation's oil supply, compelling the company to pay \$4.4 million in Bitcoin

to restore their systems (PBS NewsHour, 2021). That same year, cybersecurity specialists discovered a vulnerability in Log4j, a universally used open-source code for software applications and online services. This vulnerability created opportunities for attackers to steal passwords and login credentials, exfiltrate data, and infiltrate networks with malicious software (National Cyber Security Centre, 2021).

In response to the escalating cyber threat landscape, President Joseph R. Biden Jr. enacted Executive Order 14028, titled *Improving the Nation's Cybersecurity*, on May 12, 2021 (White House, 2021). This directive compels the federal government to embark on significant investments and implement substantial transformations aimed at fortifying and improving the nation's information technology (IT) infrastructure. Among its various lines of effort to augment cybersecurity, this paper concentrates on Section 4 of the executive order, titled "Enhancing Software Supply Chain Security."

B. MOTIVATION

The intent of this comprehensive report and innovation capstone project, an integral part of the Master of Business Administration (MBA) program at the Naval Postgraduate School (NPS), lies in the increasing relevance of supply chains to our professional path in the United States Department of Air Force (DAF).

This project is a continuation of NPS's Enterprise Innovation Design course, MN3307. During this course, students were grouped into H4D teams and tasked with addressing real-world DOD issues. The report documents the outcomes of the H4D endeavor and the students' voluntary decision to develop the project further, culminating in an extensive MBA innovation capstone project.

Our motivation is anchored by the 2020 restructuring initiative, known as "Back-to-Basics," by the Office of the Under Secretary of Defense for Acquisition and Sustainment (2021). This initiative emphasized the importance of supply chain management as a key knowledge area for contracting officers (Office of the Under Secretary of Defense for Acquisition and Sustainment [USD(A&S)], 2021).

Finally, in this project we shine a light on the cyber supply chain as a crucial, yet often overlooked, subset of the overall DOD acquisition supply chain. By focusing our project on this aspect, we bring attention to the pressing need for increased care and focus in managing and safeguarding our cyber supply chains.

C. WHAT IS H4D?

H4D is a university course that connects academia and the private sector with the DOD and intelligence communities to solve real-world national security problems and emerging threats (BMNT, n.d.). These problems are submitted by various DOD and intelligence organizations. The course encourages students to engage in rapid research and discussions to validate their problem statement. This is achieved through extensive interviews with end users and key stakeholders. Students are expected to rapidly introduce a solution, termed a MVP (BMNT, n.d.). The MVP is intended to be a bare-bones solution designed with the purpose of eliciting swift end-user feedback, thereby enhancing learning and paving the way for future solution refinement. H4D is taught in 44 universities across the United States, including NPS; Stanford University; Columbia University; University of California, Berkeley; and Duke University (BMNT, n.d.).

D. THE SPONSORED PROBLEM

This research is sponsored by the EITaaS Program Office, a DAF program initiative based in Hanscom Air Force Base under Air Force Life Cycle Management Center (AFLCMC), in alignment with Executive Order 14028. Their goal is to develop strategies to reinforce their cyber supply chain as part of DAF's software and hardware modernization campaign.

As reported by DefenseScoop, "The EITaaS program intends to delegate basic IT services, enabling the Air Force to repurpose airmen for more specialized, cyber-focused network defense and mission assurance" (Harper, 2023). This strategic outsourcing of basic IT services necessitates the EITaaS supply chain risk management (SCRM) team to thoroughly evaluate if the existing and upcoming IT products are aligned with cybersecurity standards and are safeguarded against malicious activity and cyber threats.

E. CYBER SUPPLY CHAIN RISK

According to the National Institute of Standards and Technology (NIST), cyber SCRM involves

the process of identifying, assessing, and mitigating risks associated with the distributed and interconnected nature of ICT [information and communication technology]/OT [operational technology] product and service supply chains. It encompasses the entire life cycle of a system, including its design, development, distribution, deployment, acquisition, maintenance, and disposal (Computer Security Resource Center, 2016, para. 3)

Analogous to physical product supply chains, cyber supply chains operate on a complex, global, and interconnected ecosystem to deliver widely accepted, reusable, and cost-efficient IT capabilities. This intricate ecosystem comprises numerous “components,” including multiple contributors, distribution channels, technologies, and practices.

The EITaaS Program Office approached NPS seeking greater visibility into the complex cyber supply chain. The problem statement they presented, henceforth referred to as the original problem statement in this paper, reads,

Enterprise IT program managers require an efficient method to manage the supply chain risk for their vendors to prevent cyberattacks and supply chain disruptions. An effective solution would expedite the vetting process for vendors and subcontractors and prevent costly and potentially hazardous disruptions to strategic operations within the U.S. Air Force.

F. WHAT IS AN SBOM?

An SBOM is like an ingredient list for software, detailing its components. It records information such as supplier, component name, version, dependencies, author of the SBOM data, and timestamp. This inventory traces the relationships and origins of components in the software supply chain. SBOMs provide clarity on these components, enabling users to understand their supply chain better (Cybersecurity and Infrastructure Security Agency, n.d.).

G. PROJECT OBJECTIVES

Safeguarding the cyber supply chain is paramount to uphold the national security interests of the United States. There are three main objectives of this MBA project. First and foremost, we validate the problem statement proposed by the EITaaS Program Office and ascertain its relevance in the current scenario, while also cultivating an independent understanding and interpretation of the problem through our research findings and interviews with stakeholders. The second objective involves pinpointing potential solutions to the issue, accompanied by a thorough assessment of each solution's merits and drawbacks. Lastly, based on our comprehensive analysis and insights, we offer informed recommendations to the EITaaS Program Office, ensuring the security of their cyber supply chain.

The benefits of this project are multifold. By augmenting the tools and processes available to the EITaaS SCRM team, we enhance their ability to effectively manage risks within their cyber supply chain. The improved security protocols resulting from our project will help protect sensitive national security information and mitigate the risk of cyber threats. Ultimately, our work contributes to strengthening the nation's defense against increasingly sophisticated cyberattacks, enhancing the protection of our nation's IT systems, and upholding the country's economic stability.

H. CAPSTONE HYPOTHESIS

It is imperative for the DOD to promptly investigate and comprehend the potential use cases for SBOMs. A pilot program for the collection, storage, and analysis of SBOMs should be introduced within the framework of the EITaaS program. As the DAF makes a transition towards software as a service models, it is crucial for the government to have capabilities for gathering comprehensive data about the software being utilized. SBOMs can act as a significant facilitator in improving software SCRM, augmenting contractor cybersecurity accountability, and safeguarding sensitive national security information. This paper argues that the DOD's swift and effective implementation of SBOMs can contribute significantly to strengthening the nation's cyber defense infrastructure.

I. SUMMARY

This chapter illuminated significant cyber supply chain incidents targeting the United States, underscoring the detrimental effects of these attacks on national security, economic stability, and technological infrastructure. The profound repercussions of these incidents, combined with our professional responsibilities and academic insights, form the foundation of our pursuit to address this intricate challenge. In this paper, our three primary objectives are to validate the problem statement, identify a potential solution, and provide recommendations to the EITaaS Program Office. Following this, we outline our discoveries from the H4D project, the subsequent innovation capstone, and our system dynamics modeling project. Our exploration includes the development of an MVP and strategic efforts to bridge the EITaaS program with the DOD CIO, launching a pilot program focused on SBOMs. The ultimate aim is to innovate and bolster mechanisms safeguarding the cyber supply chain, thus fortifying a more resilient national defense framework.

II. SUMMARY OF STAKEHOLDERS

When considering the impacts of cyber threats on the IT infrastructure, it is important to consider the perspectives of stakeholders in a variety of different organizations. Throughout this project, we engaged with numerous government agencies as well as leaders in the cybersecurity industry to seek critical feedback to understand the threat landscape and technical intricacies that contribute to an inherently complex problem. The organizations listed below have been identified as the key stakeholders and have a deep understanding of the problem, current standards, regulations, common business practices, and applicable laws governing the use and security of IT.

A. ENTERPRISE INFORMATION TECHNOLOGY AS A SERVICE PROGRAM OFFICE

The EITaaS program is a DAF initiative and was designed to be an answer to the call for an updated IT infrastructure while delivering world-class IT support for more than 800,000 DAF end users (Department of the Air Force [DAF], 2022). This enterprise-wide blanket purchase agreement (BPA) offers IT support for all major commands, the DAF, the United States Space Force, and many geographically separated units globally (DAF, 2022). Through this BPA, IT is procured as a service and offers support for users of hundreds of different interfaces and IT configurations across 180 locations worldwide (DAF, 2022).

The EITaaS Program Office is based at Hanscom AFB in Bedford, MA, under AFLCMC. The SCRM team managing this program are the primary stakeholders for supply chain illumination, software risk management, visibility, and mitigation of cybersecurity threats and vulnerabilities. The EITaaS Program Office is also the primary sponsor for the work we completed during our H4D project, and the continuation of this effort as an innovation capstone project. With an enterprise-wide IT service, the EITaaS Program Office recognized there would be significant software risk incurred through the use of commercial IT services on such a large scale and were unsure how to manage this risk or achieve an acceptable level of oversight of its contractor and subcontractors. As the

key driver of IT modernization within the DAF, this office plays a central role in fostering technology advancements with robust cybersecurity practices and promoting the adoption of cutting-edge enterprise solutions that benefit the warfighter. Their strategic vision and resource allocation for managing risk may have significant impacts on how the DAF safeguards their software applications and platforms from malicious activity.

B. DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

The DOD CIO is the senior advisor to the Deputy Secretary of Defense and the Secretary of Defense for Information Technology (Department of Defense [DOD], n.d.). They are accountable for all matters relating to cybersecurity, communication and information systems, digital modernization, and more (DOD, n.d.) As a major decision-making body, the DOD CIO possesses significant authority over tech policy, adoption, and implementation across the DOD. This office provides crucial guidance, oversight, and strategic direction for leveraging emerging technologies to enhance defense capabilities. The DOD CIO drives strategic initiatives for the use and implementation of cloud computing, data migration to commercial cloud architectures, deterrence of malicious cyber activity, and the use of artificial intelligence (DOD, n.d.) The DOD CIO acknowledges that there is a lack of clear, unifying guidance on security of IT, which hinders modernization efforts and may result in increased security risks and malicious attacks (DOD, n.d.). As a result, the DOD has encountered challenges with the adoption of technological advancements and modernization, which has led to disproportionate efforts and increased cybersecurity risk (DOD, n.d.). As a significant decision-maker and policy writer for matters regarding IT modernization and cybersecurity, our team engaged with this organization throughout the course of this project to streamline efforts and align with DOD initiatives.

C. DEPARTMENT OF THE AIR FORCE CHIEF INFORMATION OFFICER

The DAF CIO communicates information insights and requirements, catering to the unique needs of the DAF's IT landscape. As a key stakeholder, the DAF CIO's office offers domain-specific expertise and fosters collaboration with relevant stakeholders within the DAF ecosystem. Their involvement ensures alignment with DAF initiatives, streamlining

efforts and adoption of robust cybersecurity and risk management practices. The chief technology officer at the Office of the CIO is responsible for the adoption, resilience, and strategic technical vision of the Enterprise IT portfolio for the DAF (Office of the Chief Information Officer [Office of the CIO], 2021). The DAF chief technology officer has called for the implementation of modernized applications and resilient networks through an iterative approach to cultivate a secure IT environment for the DAF (Office of the CIO, 2021). The chief technology officer is at the forefront of IT modernization within the DAF and has led the way for initiatives like Zero Trust and Identity, Credential, and Access Management within the DAF (Office of the CIO, 2021). During the course of this project, the EITaaS Program Office has been in discussions with the DAF CIO to align with DAF initiatives and seek out guidance to enable the success of these efforts.

D. FEDERAL AND DEFENSE AGENCIES

Although our team was not able to contact all federal and defense agencies, they are all impacted by the challenges faced by the EITaaS Program Office and are vulnerable to malicious activity related to software and IT. Federal agencies, representing diverse governmental bodies and functions, are significant stakeholders that contribute to the success of cybersecurity and software risk management by providing resources for improving the software and IT landscape. Their participation fosters interagency collaboration and the sharing of best practices. As beneficiaries of technological advancements, federal agencies drive the adoption of innovative solutions in their respective domains and provide essential feedback for continuous improvement. DOD agencies, encompassing various specialized entities within the DOD, play a vital role as stakeholders in cyber defense and software risk management. Their unique missions and operational requirements necessitate tailored technology solutions. Collaboration with these agencies ensures that the new policies and practices address specific challenges, enhance interoperability, and support mission-critical operations.

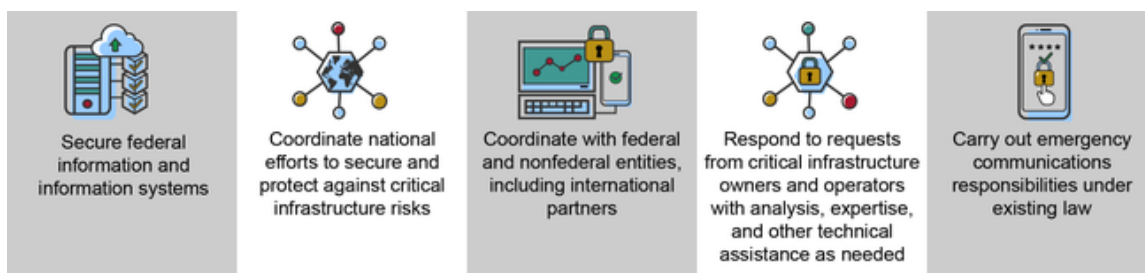
1. Department of Homeland Security

The Department of Homeland Security contributes to the enhancement and resilience of the nation's cybersecurity posture by assessing malicious cyber activity and

reinforcing defenses in an environment that is volatile and constantly evolving. (U.S. Department of Homeland Security [DHS], 2023). The Department of Homeland Security has prioritized the enhancement of software supply chain security in alignment with Executive Order 14028. This entails the enforcement of crucial provisions, such as obliging software developers to enhance their software’s transparency and public accessibility of security data (DHS, 2023)

2. Cybersecurity and Infrastructure Security Agency

On November 16, 2018, the Cybersecurity and Infrastructure Security Agency (CISA) Act was signed (Cybersecurity and Infrastructure Security Agency [CISA], 2022). This act elevated the mission of the Department of Homeland Security and established CISA to protect the nation’s critical infrastructure from cyber threats. The agency coordinates and collaborates with numerous government and private sector organizations to fortify cyber defenses and help organizations prepare for, respond to, and mitigate the impact of cyberattacks through their “Shields Up!” initiative (CISA, 2022). CISA offers key insights and is a proponent of collaboration among all agencies and encourages all stakeholders to share information about cyber events to mitigate threats to critical software infrastructures (CISA, 2022). Figure 1 discusses the agency’s obligations under the CISA Act as described by an analysis conducted by the GAO.



Source: GAO analysis of the Cybersecurity and Infrastructure Security Agency Act of 2018; images: Buffaloboy/istock.adobe.com. | GAO-23-106428

Figure 1. Analysis of CISA. Source: GAO (2023)

3. National Institute of Standards and Technology

NIST is an agency of the Department of Commerce that develops cybersecurity standards, guidelines, frameworks, and other resources for industry, federal agencies, and the public to utilize (NIST, 2016). NIST has prioritized a focus on emerging technologies, identity and access management, trustworthy networks, and platforms and risk management practices in an effort to align with Executive Order 14028 for improving the nation's cybersecurity (NIST, 2016).

E. WARFIGHTER

The EITaaS program Wave 1 BPA was designed to deliver world-class IT support for the DAF. At the forefront of military operations, warfighters represent the end users and beneficiaries of the EITaaS program. Their perspectives and feedback provide essential insights into the usability and effectiveness of new technologies and methodologies for reducing and mitigating software risk. As critical stakeholders, their engagement throughout the life of the contract ensures that IT solutions align with the practical needs and realities of the warfighting environment. The warfighter drives the need for robust IT services, but they also drive the need for a rigorous risk management framework. Every line of code, for every application, for each piece of software, for every system, within each desktop, for each member is an opportunity for cyberattack and other types of malicious activity. The warfighter not only has a need for world-class IT support, they have a need for world-class cybersecurity and risk management to safeguard defense assets and information.

F. CONTRACTORS

Contractors, as interested stakeholders in cybersecurity and software risk management, are instrumental in developing and implementing novel technological solutions. Their proficiency and experience contribute to the success of risk mitigation practices by providing specialized knowledge and technical capabilities regarding software. Collaboration with contractors with expertise in the realm of software risk management and cybersecurity facilitates the realization of ambitious risk management goals and strengthens the security of defense systems.

G. SUMMARY

This chapter introduced key stakeholders relevant to the software SCRM challenges discussed in this report. Many of these stakeholders play critical roles in the guidance, direction, and policies that govern how federal and defense agencies tackle software risk and the growing threat of malicious attacks. However, many of these efforts are ambiguous, fragmented, or uninformed and do not align with a singular unified effort toward a common goal. This further complicates and slows efforts to address an already complex problem faced by all government agencies. Although Executive Order 14028 dictates that all federal agencies must make strides to strengthen the nation's cybersecurity, it lacks clear guidance on how to do so, which has hindered efforts to comply with the order. Although government agencies like NIST and CISA have taken the lead on guidance, little to no efforts have been made to align federal and defense agencies on actions to be taken to meet the intent of the executive order.

III. SUMMARY OF METHODOLOGY

In this section, we delve into the methodologies employed during our innovation capstone research. We use four main methodologies while conducting our innovation capstone project: the Lean Launchpad in the H4D course, engaged scholarship via working groups, the goals- decisions- signals- data model, and system dynamics. Each method plays a significant role in discovering information and coming to our final recommendations. These approaches are designed to address complex challenges actively and dynamically, allowing us to deliver meaningful solutions. Rooted in rigorous research, iterative problem-solving, and a commitment to understanding and meeting the real needs of our stakeholders, these methodologies provide structure and adaptability for navigating the multifaceted landscape of national cybersecurity challenges effectively.

A. HACKING 4 DEFENSE

The Lean Launchpad methodology, employed in H4D, stands as a potent and inventive approach for tackling intricate national security issues. Originally co-developed by Steve Blank, this methodology underscores the importance of swift iteration and customer discovery to ascertain that the proposed solutions align with the actual requirements of end users (Blank, 2009). Within the framework of H4D students actively interact with a multitude of stakeholders, including the military, intelligence community, and commercial industry, to attain a profound comprehension of the problem domain before crafting potential solutions.

We began the Lean Launchpad process by forming an interdisciplinary team as NPS MBA students and EITaaS program members, then immersing ourselves in the problem. We conducted in-depth interviews with potential users and beneficiaries, seeking to understand pain points, operational constraints, and existing gaps. Armed with insights gathered during this discovery phase, we iteratively built and tested prototypes of our proposed solutions, also known as MVPs. This was the implementation of the Build-Measure-Learn feedback loop, Figure 2, highlighted in the course book, *The Lean Startup* by Eric Ries (Ries, 2011).

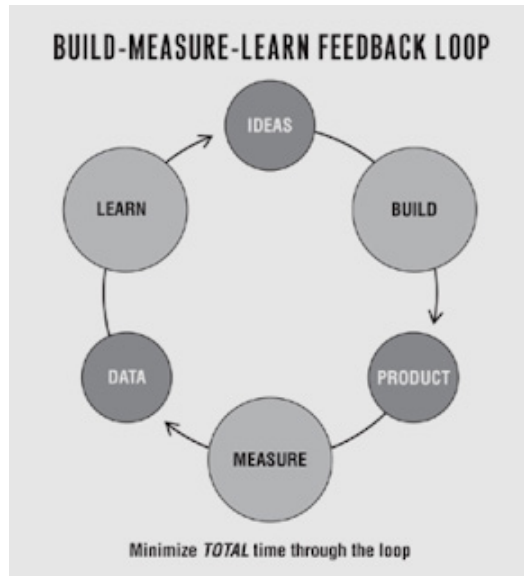


Figure 2. Build-Measure-Learn Feedback Loop. Source: Ries (2011)

The emphasis on constant feedback and validated learning allowed our team to refine ideas rapidly, ensuring a higher likelihood of success when our suggested solution is eventually implemented (BMNT, n.d.).

In order to develop initial MVPs, we used Mission Model and Value Proposition Canvases developed from Alexander Osterwalder’s Business Model Canvas (Blank, 2019). Filling out canvases allowed our team to determine main stakeholders to the EITaaS problem and develop hypotheses to test with our solution. H4D’s application of the Lean Launchpad methodology has proven to be highly effective in creating tangible solutions to some of the most pressing national security challenges (Blank, 2009). By combining rigorous problem-solving with a focus on end-user needs, this methodology produces innovative and relevant outcomes. Moreover, the hands-on experience gained by students through the H4D program prepares them for the real-world challenges of working in complex, high-stakes environments, making it a transformative learning experience with significant practical implications (Blank, 2009).

B. WORKING GROUPS

As we continued our MBA capstone project, working groups offered us a collaborative methodology to build on the progress made during the H4D project. Working

groups can be created in any industry as individuals coming together from different competencies to solve a problem (Phillips & Phillips, 1993). We continued working with the interdisciplinary team that included our H4D project members, relevant stakeholders, and other experts and advisors. These working groups facilitated ongoing discussions, brainstorming, and knowledge-sharing sessions to refine and fine-tune the proposed solutions based on the real-world insights and feedback gathered during the H4D project.

Working groups provided several advantages in this continuation process. They offered us a structured platform for regular meetings, ensuring that our collaboration did not fade away after the initial project completion. By maintaining consistent communication with the EITaaS SCRM team, we continued to build on the relationships established during H4D and fostered a deeper understanding of the organizations' needs and constraints.

Also, working groups allowed us to engage in in-depth discussions and explore potential implementation strategies with connected industries outside the DOD. This ongoing dialogue enabled us to gain a more comprehensive understanding of the practical challenges of SBOMS and how software contractors might react when the EITaaS team implements the proposed solutions. Being able to incorporate companies that are at the forefront of developing SBOMs in our working groups was critical in being able to adapt and refine our recommendations and final solution.

Working groups offer a mechanism for cocreation (Davies et al., 2010) and engaged scholarship (Mathiassen, 2017). By involving stakeholders from the organizations in the process, such as the DOD and DAF CIOs, we created a collaborative environment that increased buy-in and ownership of the solutions. This engagement is essential for ensuring successful implementation beyond the capstone project.

As we continued our collaboration through working groups, we leveraged the expertise of our team members, mentors, and stakeholders to iteratively improve the proposed solutions. By combining our academic knowledge, the practical insights from H4D, and organizations' inside and outside the DOD on-the-ground experience, we

developed more robust and tailored recommendations that have a higher likelihood of making a meaningful impact.

C. GOALS, DECISIONS, SIGNALS, AND DATA

The Goals, Decisions, Signals, and Data (GDSD) model, developed by Daniel J. Finkenstadt, Rob Handfield, and Peter Guinto, presents a comprehensive framework to aid organizations in effectively managing risk in a world dominated by data published by California Management Review Insights (2022). At its core, the model revolves around the four interconnected components: goals, decisions, signals, and data. By focusing on the interconnected components of goals, decisions, signals, and data, this model prompts critical questions essential to managing supply chain risks, which is a central concern for our project. As we delved into the intricacies of our problem, Figure 3 served as a visual guide, helping us align our strategies with proven principles and best practices in risk management.

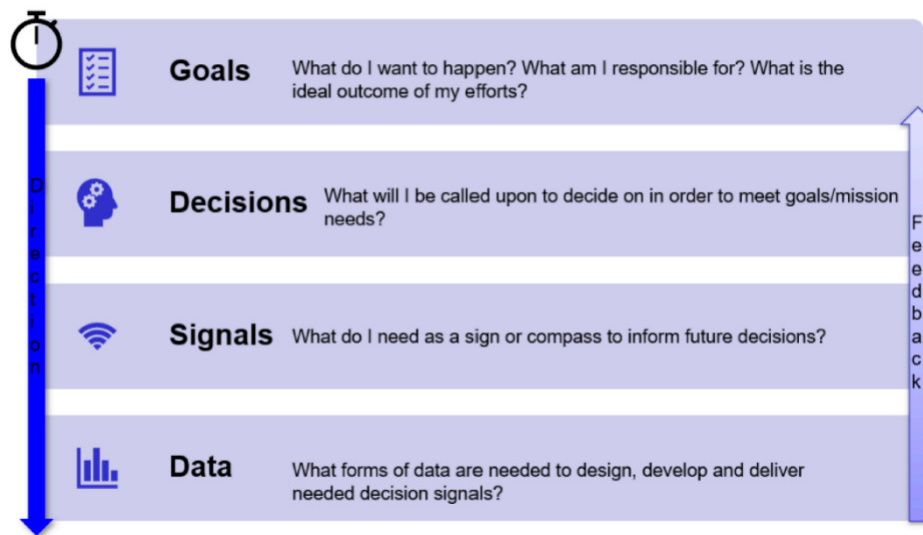


Figure 3. GDSD Model. Source: Finkenstadt et al. (2022)

The GDSD model emphasizes the significance of clearly defined goals and objectives (Finkenstadt et al., 2022). By understanding the EITaaS program's desired

outcomes for their software supply chain management, we were able to identify potential risks within the process. This step ensured our solution and recommendations were working to achieve the program's overall goals and helped determine what data would be important to analyze to achieve those goals.

Informed decision-making is crucial in effective risk planning, and our team needed to understand what decisions EITaaS program managers would be making to address software risks. The decisions made by program managers would affect what signals they want to see to be able to take risk mitigation actions and understand the state of their program software. Knowing their decision process and the risk factors managers care about determines what data we should analyze.

The GDSD model also emphasizes the importance of recognizing and interpreting relevant signals in the operating environment (Finkenstadt et al., 2022; Siangpipop, 2022). The decisions EITaaS program managers must make about software and program risks determine what the most efficient signals would be to help analyze decision pathways. In using the model, we needed to answer the question of what signals would be essential in telling program managers that they need to take risk mitigation actions. Our final solution needed to address those decision-making signals in data and action-prompting visuals (Siangpipop, 2022).

Data plays a pivotal role in the GDSD model, as it is essential for informing risk management strategies (Finkenstadt et al., 2022). Understanding the EITaaS software SCRM process allowed us to identify the necessary data to collect and analyze for creating signals, making informed risk mitigation decisions, and achieving the program's goals. Utilizing this model empowered us to delve into SBOMs and align the risks that program managers base their decisions on with the data contained in the SBOMs. The GDSD model encourages a holistic approach to risk planning, where goals, decisions, signals, and data are interconnected and feed into each other (Finkenstadt et al., 2022). By integrating these components, organizations can establish a robust risk management process that enables them to navigate the complexities of a data-saturated world effectively (Finkenstadt et al., 2022).

D. SYSTEMS DYNAMICS

System Dynamics is a methodology that provides a holistic approach to understanding and modeling complex systems (Sterman, 2000). It focuses on the interconnections and feedback loops between various components of a system rather than analyzing individual parts in isolation. By studying the dynamic behavior of systems over time, it seeks to identify how changes in one part can lead to ripple effects throughout the entire system. This approach is particularly useful in addressing challenges that arise from the complexity and interconnectedness of real-world systems. By utilizing this approach, we were able to look at the software supply chain and its connecting federal policies as a whole process and determine how the introduction of SBOMs affects it.

The core idea of System Dynamics lies in recognizing that systems are composed of multiple elements that interact and influence each other's behavior. It emphasizes the importance of considering both the short-term and long-term consequences of decisions and actions within a system. By using modeling and simulation techniques, System Dynamics enables analysts and decision-makers to gain insights into the system's behavior and test various scenarios before implementing real-world changes. We started with a casual loop diagram (CLD) to elucidate the fundamental feedback loops and interrelationships between a SBOM policy, the frequency of cyber incidents, and resultant economic consequences. We then modeled the system with certain assumptions to try and quantitatively assess the efficacy of a SBOM policy in reducing the number of successful cyberattacks and their associated economic losses.

Systems thinking, an integral part of System Dynamics, encourages a shift from linear thinking to understanding the underlying structures and patterns that govern system behavior (Meadows, 2009). Instead of attempting to solve isolated problems, it encourages analyzing the entire system to identify leverage points for effective interventions. System Dynamics helps identify feedback loops, delays, and nonlinear relationships within systems, allowing decision-makers to develop more effective strategies and policies. By using system dynamics we attempted to untangle the intricate web of relationships and variables within the software supply chain, thereby providing a more informed foundation upon which to assess the efficacy of implementing a SBOM policy.

IV. H4D PROJECT

This chapter discusses that actions taken within our H4D project. Throughout this chapter, we will meticulously detail each step of our H4D journey, emphasizing our rigorous approach to problem discovery. Our methodology involved extensive stakeholder interviews, in-depth research, and sponsor feedback, all aimed at shedding light on the multifaceted issue faced by EITaaS program. Moreover, we embarked on a journey of rapid iteration, developing multiple MVPs to address the problem's nuances. As we progress, our aim is to crystallize the validated problem statement, solidifying our contribution to the EITaaS program's mission.

A. PROBLEM DISCOVERY

One of our initial primary objectives in the H4D project was to develop a comprehensive understanding of the problem and identify its root cause, which affected our sponsor. Over the course of ten weeks, we embarked on an extensive research journey, delving into current supply chain and cybersecurity policies and processes to better understand the problem's context. However, relying solely on academic research and literature to grasp the complexity of the problem space was insufficient. Personal experiences with the problem and insights into the related processes proved invaluable. During the H4D project, we conducted a series of thirteen interviews with various stakeholders within the EITaaS program, leaders in the cybersecurity industry, and sister service organizations that operated within the same problem domain. These interviews, ranging from thirty minutes to an hour each, involved tailored questions designed for each individual or organization. Table 1 lays out who we interviewed in this process and what our main discoveries and takeaways were.

Table 1. H4D Interviews and Main Takeaways

Date	Interviewed	Main Takeaways
30 Sept 22	EITaaS Program Logistics	- Little insight into software supply chain and 2nd or 3rd tier suppliers - Established the need to identify risks and develop mitigation plans
13 Oct 22	Fortress Information Security Sr. Account Executive Defense Industry Solutions	- There are companies in the software supply chain security industry that utilize SBOMs and have monitoring platforms
13 Oct 22	EITaaS Program Intelligence	- Need to map the software supply chain, remove bad actor influence from contracts, determine who uses current software in the AF
13 Oct 22	Resilinc VP Government Affairs	- Supply Chain mapping in any industry is intensive and shadowed - All BOMs are dynamic
24 Oct 22	EITaaS Program Cybersecurity	- There is significant communication with other offices to track threats, cybersecurity cannot be done individually - 90–95% of vulnerabilities are identified by the vendor
25 Oct 22	Portfolio Integration and Analysis Lead, AFLCMC Armament Directorate, Rapid Enterprise Solutions Division	- Built organic dashboard to have more insight into hardware supply chain - Information is from Navy Supplier Database
26 Oct 22	Anchore Personnel	- A majority of software today is built from open sources and is very complex - Anchore has a dashboard that uses SBOMs and visualizes risks in the software
27 Oct 22	MITRE Personnel	- There are many different types of risks and organizations use different taxonomy to discuss the same types of risks - There may be issues in building an DOD accessible database for software component information
1 Nov 22	AFMC HQ Logistics, Civil Engineering, Force Protection and Nuclear Integration/A4RM	- Internal Dashboard is being created for SCRM teams to use for pre-award discrete supplier reviews to vet vendors before contract award - Risk taxonomy must align across organizations for a dashboard to be successful
3 Nov 22	Eglin Supply Chain Business Intelligence Team AFMC AFLCMC Armament Directing Contracting Office	- Making connections between data in the BOMs and critical risks is imperative for a successful dashboard - If BOMs are not in a standard format, manual edits must be made in order to be read by the database that feeds the dashboard

Date	Interviewed	Main Takeaways
		- A collaboration to add SBOM data could be possible
3 Nov 22	Exiger – Supply Chain Mapping Government Team	- Exiger has a General Services Administration (GSA) contract to support SCRM activities, such mapping the supply chain and creating dashboards
15 Nov 22	NAVAIR SCOM Personnel	- The Navy Supplier Database could be updated to include SBOMs with just contractor information to begin with - Visibility with BOMs is typically Tier 1 or 2 and can increase contract costs
17 Nov 22	Science Applications International Corporation, ServiceNow, EITaaS Wave 1 Contractor	- Current contractors have limited understanding of SBOM practices - Without a better understanding they could not provide us with an SBOM for a small software

Our primary focus during these interviews was to uncover the threats and vulnerabilities present within a software supply chain and solicit insights from those closely associated with the system on potential mitigation strategies. As we progressed through the Enterprise Innovation Design course and deepened our understanding of the problem, we experienced moments of gaining fresh insights and information. These revelations prompted us to revisit individuals we had previously interviewed, seeking additional answers, and further refining our comprehension of the problem. The interviews, conducted throughout the duration of the Enterprise Innovation Design course, furnished us with crucial insights that played a pivotal role in the iterative development of our final H4D MVP and the final compilation of our mission model canvas (see the appendix).

B. FIRST MVP ITERATION

As career contract officers responsible for procurement within different facets of the DAF, our initial instinct led us to seek out companies in the software industry capable of providing supply chain mapping and risk assessment services. As seen in Table 1, we conducted interviews with several companies, aiming to gain a deeper understanding of their software supply chain processes and identify existing solutions designed to address gaps and vulnerabilities. Our primary objective was to compile a list of commercially available services that the EITaaS team could potentially acquire to enhance their software supply chain risk mitigation efforts, referred to as course of action 1.

Our interactions with industry experts revealed that some existing solutions had the potential to support the EITaaS team in their Supply Chain Risk Management (SCRM) procedures. These insights were inspired by the 2021 AFLCMC Standard Process *Supply Chain Risk Management* (AFLCMC/LG-LZ, 2021) which offered valuable information regarding the current SCRM process.

While the standard SCRM process primarily expects the use of commercial SCRM solutions in step 6.6, “Leverage Commercial Supply Chain Illumination,” our interviews with industry representatives suggested that these commercial solutions could be effectively integrated into additional steps of the process. Figure 4, originally from the AFLCMC document, illustrates this integration.

We pinpointed commercial applications suitable for use beyond supply chain illumination, specifically in two essential steps: step 6, “Conducting Supply Chain Threat Assessments,” and step 8, “Conducting Continuous Supply Chain Risk Monitoring,” as part of course of action 2, our main recommendation to our sponsors for this MVP. These applications included commercial companies specializing in software threat assessment and others entirely dedicated to ongoing software risk monitoring.

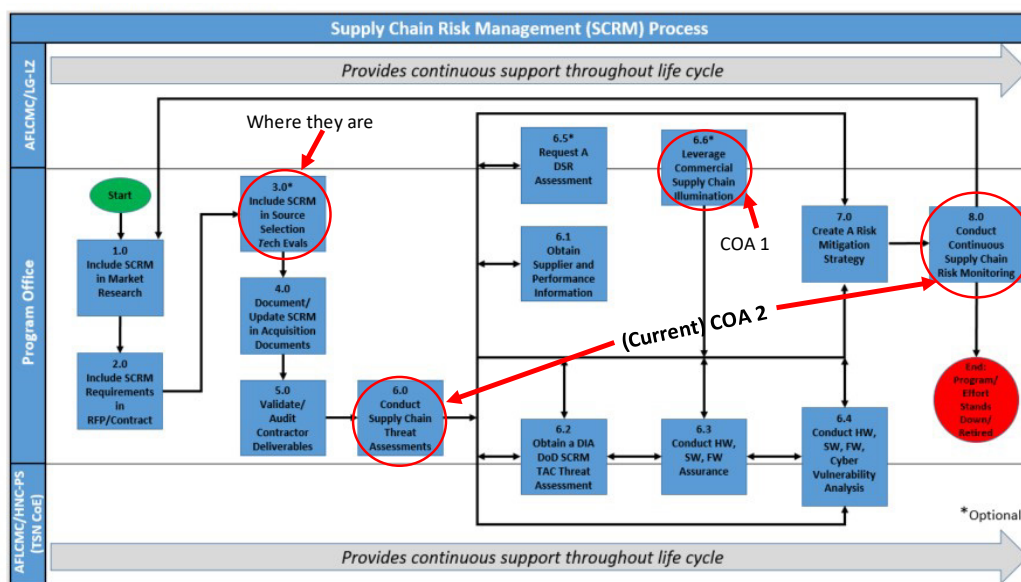


Figure 4. SCRM Process Flowchart. Adapted from AFLCMC/LG-LZ (2021)

We presented this first MVP to our sponsor to mixed feedback. The market research this MVP provided could be used to implement one of the commercial solutions in the short term, especially those that already have a federal contract in place. However, the EITaaS program did not have the funding to support those types of purchases for any length of time. Moreover, their limited knowledge about the information requirements for these solutions and the potential costs they might incur on their software contracts added to the challenge. For these reasons, we continued iterating on the MVP.

C. SECOND MVP ITERATION

As there was concern over the cost of outsourcing the supply chain mapping and risk assessment for the EITaaS program, we began looking into what types of organic dashboards were currently being used within the DAF. Our team interviewed John Hill, the Portfolio Integration and Analysis Lead at AFLCMC Armament Directorate in the Rapid Enterprise Solutions Division. He discussed the dashboard tool they developed to have greater insight into the hardware supply chain for different weapon systems and armament platforms (interview with author J. Hill, personal communication, October 25, 2022). This dashboard tracks and monitors hardware parts from over 10,000 suppliers and connects that information to federal government websites such as the System for Award Management. The armament directorate contracting office has a team of skilled individuals, the Eglin Supply Chain Business Intelligence (SCBI) Team, that help manage the data that flows into the dashboard and how it is visualized. The information for this dashboard is derived from hardware bills of materials (HBOMs), initially supplied from the contractors to their program office and by the end of the process is stored by the Naval Air Systems Command (NAVAIR) Supplier Database (G. Parry et al., personal communication, November 3, 2022). The dashboard developed by the AFLCMC Armament Directorate extracts HBOM information from a repository created and maintained by NAVAIR called the Supplier Database which contains HBOM information from over 50,000 vendors. Utilizing this extensive repository hosted by a sister service decreases duplication of efforts as the vendors for Air Force weapon system vendors may overlap with Navy vendors. The analysis the SCBI team accomplishes with this

information allows the program managers of these weapon systems to have risks and vulnerabilities within their supply chains identified in a single location.

Our second MVP attempted to tailor an armament management dashboard by incorporating the specific features required for analyzing SBOMs. Initially, our objective was to use this enhanced dashboard to identify risks related to foreign influence, organizational ownership, and supplier locations within the software supply chain. We explored the potential of NAVAIR's Supplier Database repository to accommodate SBOMs by introducing additional quantifiable categories.

Yet, our understanding of SBOMs was limited at this point, and we assumed that software components could be listed similarly to hardware components. Completing the H4D project made it evident that this assumption was inaccurate. Unlike HBOMs, which consist of tangible components that are relatively easy to track, SBOMs involve intangible components. Overall, our second MVP's primary focus was to collaborate with the AFLCMC Armament Directorate, Rapid Enterprise Solutions Division, to utilize their in-house supply chain risk management dashboard. The objective was to identify and manage significant supplier risks. However, our problem discovery process revealed that a dashboard solely dedicated to tracking supplier risks would not comprehensively address EITaaS' supply chain visibility challenges. To be effective, a dashboarding tool needed to identify risks within the software domain, a capability that the existing SCBI tool lacked.

D. H4D FINAL MVP

Our final MVP during the H4D course consisted of multiple elements. First, we aimed to leverage the existing capabilities of the SCBI dashboard and assess the feasibility of integrating SBOM information and analysis into this tool. We actively engaged in several discussions with Science Applications Implementation Corporation, the current contractor providing IT services at Hanscom Air Force Base, to facilitate the submission of an SBOM for the software product. Unfortunately, we encountered a challenge during these discussions. While there may be companies that work with SBOMs, many prime contractors may not have exposure to SBOM usage, or fully understand the significance of their content. As a result, we were unable to obtain an SBOM from Science Applications

Implementation Corporation for testing within the SCBI tool and NAVAIR Supplier Database.

Had we collected SBOM data, our next step would have involved collaborating with NAVAIR to obtain vendor commercial and government entity codes for input into the NAVAIR Supplier Database. The existing features of the SCBI dashboard allowed EITaaS program managers to visualize crucial information. For instance, the tool generated a map displaying the geographic locations of suppliers and illustrating their connections to other contractors and suppliers within the supply chain.

In our second MVP, we recognized that incorporating SBOMs into a pre-existing dashboard created to track tangible assets posed significant challenges. The second aspect of our MVP involved the future expansion and customization of the SCBI tool for software applications. To ensure the success of the SCBI tool in this context, several extenuating considerations were revealed, including SBOM standardization, alignment with risk taxonomies, and the adoption of best practices in software supply chain data visualization.

SBOM standardization was a significant consideration because a main step in the process to incorporate data into the SCBI tool was formatting HBOMs from different armament programs into a readable format for NAVAIR's Supplier Database. It is an important step as NAVAIR must adhere to a specific format for acceptance into the Supplier Database and seamless integration into the dashboard. A sentiment we heard from multiple sources was the difficulty in maintaining an up-to-date dashboard when the necessary data was received in a different format every time. Therefore, before adding SBOMs to the SCBI tool, a standardized format should be agreed upon for the DOD. Figure 5 identifies a minimum of four organizations that should be included to create a single standardization of formatting for SBOMs received by the federal government. These organizations are NIST, who is the primary agency developing SBOM standards, CISA, who has the foremost information on how SBOMs affect cybersecurity measures, NAVAIR, who developed and maintains the Supplier Database, and the EITaaS Program Office, who would be collecting these SBOMs and correcting the formatting if inconsistent.

SBOM

Standardization Collaboration

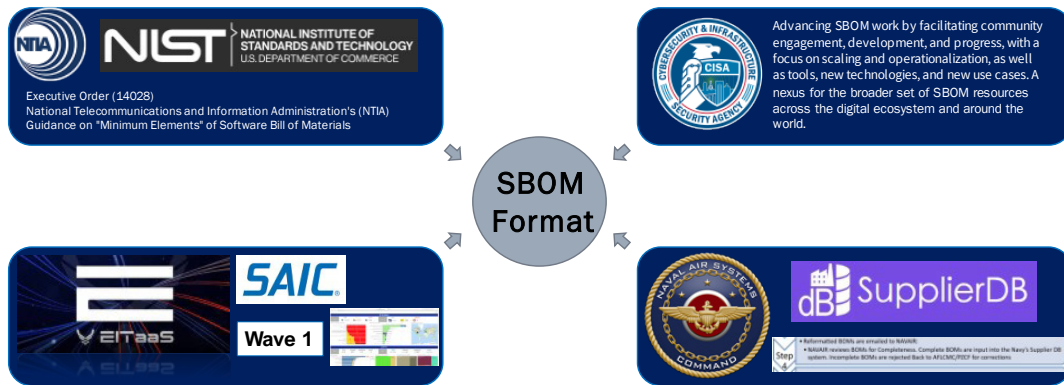


Figure 5. Final H4D MVP SBOM Standardization Collaboration

To ensure consistent provision of essential SBOM information for connecting potential supply chain vulnerabilities to cybersecurity measures across federal organizations, standardizing SBOMs was crucial. This standardization required uniform data elements in a consistent format, enabling compatibility with various systems and dashboards. However, an aspect we hadn't fully contemplated was the potential tradeoff of mandating a government-unique SBOM standard for DOD contractors. During this phase of our research, we recognized that while standardizing SBOMs could enhance software risk management, it might pose challenges for non-traditional or small business contractors who were relatively new to the term SBOM and this level of standardization within the federal government and DOD.

Furthermore, we recognized the critical need to align risk taxonomies across the DOD. To achieve collaboration and maximize the utility of a unified dashboard for both hardware and software SCRM, it is imperative that all DOD organizations adopt a common risk language and can categorize components and potential vulnerabilities in a consistent manner. With the increased focus on supply chain management and cybersecurity (Korbren, 2023), the USD (A&S) introduced a draft SCRM taxonomy in late 2022, followed by a SCRM framework in 2023, which promotes the adoption of uniform risk

terminology across all DOD entities (2023). Failure to align these taxonomies could compromise our ability to effectively identify and analyze risk (Office of USD (A&S), 2023). Such alignment is crucial for ensuring that risk assessments and mitigation strategies are consistent and coherent across the entire DOD. This harmonization also opens the possibility of using the dashboard as a collaboration hub for SCRM among organizations, as illustrated in Figure 6.



Adapted from Air Force Life Cycle Management Center, Air Force Materiel Command, Air Force Office of Special Investigations, LinkedIn, National Security Agency, Naval Air Systems Command, Office of the Director of the National Intelligence, System for Award Management (n.d.).

Figure 6. Final H4D MVP Vision: SCBI Collaboration Hub.

During this process, we uncovered the need for extensive collaboration between services and various organizations in the realms of software cybersecurity and supply chain management. To address this requirement, an internal dashboard like the one depicted in Figure 6 could serve as a dedicated hub, fostering collaboration among different risk management stakeholders to enhance risk mitigation. This solution involves the flow of SBOMs from program offices to NAVAIR, where they are integrated into the Supplier Database and the SCBI tool. The tool then condenses SBOM data into user-friendly visuals

for identifying software supply chain risks and vulnerabilities. These insights can be internally assessed by associated intelligence communities.

While this approach promises faster identification of significant supply chain risks, it poses several logistical challenges. Questions arise regarding the storage of SBOMs, whether with program managers, NAVAIR, or within individual service or DOD repositories. Security measures for this repository need careful consideration. The frequency of SBOM updates, access control for the collaborative dashboard, data security, risk severity scoring, and the best visualization methods for communicating to program managers are among the key issues. Specifically concerning software supply chains and SBOMs, integrating this data with DOD risk categories requires detailed examination. These questions served as pivot points for our post-H4D research, extending beyond the project's conclusion.

E. VALIDATED PROBLEM STATEMENT

After multiple interviews with DOD organizations, commercial software security companies, and countless hours of reading federal policy and documents on software risk mitigation, we were able to create a validated problem statement.

The EITaaS SCRM team does not have the organic capability to dynamically map out their program supply chain. They need the ability to rapidly identify and react to emerging cyber supply chain threats.

The work we did over the 10-week period cumulated in organizing a supply chain education and training roundtable that brought together members from our sponsor team and leaders in industry. Figure 7 is a photo of our H4D collaboration with the EITaaS Program Office being recognized with the FY22 AFLCMC Annual Logistics Functional Team Award. Starting from the left is Jason Blacksborg and Peter Lee from the EITaaS Program Office, then our team, Phillip Nguyen, Madison Tikalsky, Samantha Durlauf, and our advisor, Daniel Finkenstadt.



Figure 7. FY22 AFLCMC Annual Logistics Functional Team Award Presentation

Moving forward from H4D, our learnings from each MVP enabled us to identify the key information required for the EITaaS SCRM team's success. A deep understanding of SBOMs is required to request SBOMs from contractors and analyze that information for risk, rather than just supplier information.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SBOM DISCOVERY POST H4D

After completion of the H4D project and the Enterprise Innovation Design course, the team decided to continue this research as an Innovation Capstone Project for the MBA program at NPS. The problem statement flowed through multiple iterations with several MVPs as potential solutions, yet we believed there was still so much work that could be done. The IT and software supply chain landscapes are ever-evolving and their security has become a rapidly growing concern among federal agencies and the private sector. During the H4D project, our team learned that SBOMs could potentially be a vital tool in the illumination of software supply chains, and the identification and management of software vulnerabilities, but we still did not have an inclusive understanding of how it could be done. We launched into another phase of discovery after completion of the H4D project. This phase included the development of a comprehensive understanding of SBOMs, navigating the landscape and diversity of existing SBOM formats, unveiling the expansive use cases of SBOMs, how vulnerabilities can potentially be identified within SBOMs and mapped to critical software risk categories, and how these vulnerabilities could potentially be monitored and managed.

A. UNDERSTANDING SBOMS

To understand how SBOMs could be used in the identification of software vulnerabilities, our team first needed a comprehensive understanding of their foundational concepts, component breakdown and multifunctional uses. The development and use of SBOMs has grown into a collaborative effort as federal agencies like the National Telecommunications and Information Administration (NTIA) and CISA are at the forefront of their implementation to address growing cybersecurity concerns. These agencies, as well as those already utilizing SBOMs in industry, have highlighted SBOMs as a key piece for effective software risk management and software supply chain illumination. An SBOM is essentially a machine-readable list of ingredients for a piece of software (CISA, n.d.). This exhaustive list is an inventory of a software's components, it contains baseline information about each component and describes the relationships

between the components, which are known as dependencies (CISA, n.d.) The baseline component information typically includes the supplier, the author of the component's code, the version, the unique identifier and where it falls in the relationship hierarchy. These data fields, as seen in Figure 8, are generally the minimum fields included in all SBOM formats. This information can be used to trace a software's supply chain, identify known vulnerabilities, and measure its level of risk.

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

Figure 8. NTIA required SBOM elements. Source: NTIA (2021b)

B. EXISTING SBOM FORMATS

The diversity of the software landscape has driven the need for various SBOM formats that cater to different technological use-cases. In 2021, NTIA working groups identified three key SBOM formats already widely used by software firms: Software Package Data Exchange (SPDX), CycloneDX (CDX) and Software Identification (SWID), all of which are in an open-source machine-readable formats with origins in different software-centric organizations (National Telecommunications and Information Administration 2021c). Each format has specific use cases, with unique strengths and

limitations. Understanding the strengths and limitations of each is critical for selection of the most appropriate format to increase visibility and manage software risk.

The SPDX format states a description of software components, copyright and security information to facilitate illumination of software supply chains (National Telecommunications and Information Administration, 2021c). This format's creation was intended to create a standard for metadata exchange and allow information to be shared along the supply chain . An SPDX SBOM's use cases include:

- Description of a system's components and their relationships
- Licensing and copyright information
- Tracking to individual source files
- Container inventory, indicators for known vulnerabilities and other component information

CDX is an open-source format designed to be a security-centric SBOM standard that increases visibility of a software's supply chain. This format contains component information and their hierarchical relationships, metadata and whether or not the inventory of a component is complete. The use cases include:

- An inventory of components
- Software supply chain risk attestations
- Licensing information
- Traceability of origins, also known as provenance of a component
- Capabilities for fully automated SBOM creation (and Information Administration, 2021c).

Although a top contender for the DOD use-case scenarios, this format is constantly evolving, which creates challenges when trying to standardize how SBOMs are obtained and generated.

The SWID format was intended to facilitate tracking of software installed on a device. This format tracks the life cycle of a software component from when it is installed, updated, patched or uninstalled. The SWID format also states descriptive information of software components, such as the product name, version, dependencies, and other standardized component information. The use cases include:

- Continuous monitoring of installed software
- Identifying appropriately updated or patched software
- Identifying software vulnerabilities
- Identifying and preventing installation of corrupted software and other uses cases.

To demystify the different formats, NTIA has created a crosswalk for the nomenclature of each attribute for each of the formats, see Figure 9.

Attribute	SPDX	CycloneDX	SWID
Author Name	Creator	metadata/authors/author	<Entity> @role (tagCreator), @name
Timestamp	Created	metadata/timestamp	<Meta>
Supplier Name	PackageSupplier	Supplier publisher	<Entity> @role (softwareCreator/publisher), @name
Component Name	PackageName	name	<softwareIdentity> @name
Version String	PackageVersion	version	<softwareIdentity> @version
Component Hash	PackageChecksum Or VerificationCode	Hash "alg"	<Payload>../<File> @[hash-algorithm]:hash
Unique Identifier	DocumentNamespace combined with SPDXID	bom/serialNumber component/bom-ref	<softwareIdentity> @tagID
Relationship	Relationship: DESCRIBES; CONTAINS	(Inherent in nested assembly/subassembly and/or dependency graphs)	<Link> @rel, @href

Figure 9. Title of attributes for each SBOM type. Source: NTIA (2021c)

These formats, recommended by both NTIA and CISA, are widely used by software managers in industry and have the greatest potential for matching use-cases relevant to the DOD. Each has its own strengths and weaknesses and each format may be more appropriate to utilize at different stages of a software's life cycle. This has created a contentious SBOM format debate surrounding which format is most effective for software supply chain illumination. This debate creates a conflict for uniformity and further complicates the creation and collection of SBOMs for software risk management for both DOD and the private sector.

C. IDENTIFYING VULNERABILITIES

Software development has evolved at an unprecedented rate in the last few decades. Developers can now utilize publicly available libraries of code, also known as “open source” code to simplify software creation (Kerner, n.d.). Although these practices simplify software development, they also create vulnerabilities by limiting visibility of the software supply chain (Kerner, n.d.). This makes it exceedingly difficult for developers to have accountability of the code they utilize. A piece of software may utilize thousands of lines of open-source code, making it near impossible to track which pieces of software have hidden vulnerabilities. Executive Order 14028 highlights SBOMs as a solution to illumination of the software supply chain, yet there are no processes or infrastructure currently in place to utilize SBOMs effectively.

This has led to one of the greatest challenges our team has faced during this research, once an SBOM is generated, what does one do with it? Utilizing the GDSD model our team identified that in a software risk management framework, the SBOM provides the data, which informs the demand signals for risk, which inform risk-management decisions, which enable achievement of the goals of a risk management team, Figure 10. To identify the risks, we needed to identify where they would reside within an SBOM.

Goals	Decisions	Signals	Data
1. Mandate: Executive Order 14028 on Improving the Nation's Cyber Security 2. DOD Risk Taxonomy: Narrowed down to top two risk sub-categories: A. Foreign Ownership Control or Influence – Provenance B. Technology and Cyber Security – Critical Hardware/Software Vulnerability. 3. Quote: "IT services we provide for our airmen are secure and reliable by lowering SCRM risk." - Peter Lee, SCRM Lead	Determine the necessary Supply Chain Risk Management measures for the EITaaS program.	Dashboard for highlighting provenance and software vulnerability risks. 1. Provenance Visibility Score: Indicates the known origins of components. 2. Vulnerability Visibility Score: Demonstrates our awareness of the components within our software.	Utilizing a Software Bill of Materials to gain insight on the origin and components of the software in use.

Figure 10. SBOM GDSD

Software developers and software risk managers have access to public databases which document vulnerable code, software applications and libraries (NIST, n.d.-a). These databases, such as the Common Vulnerability and Exposure program which was created in 1999, is maintained by MITRE corporation to facilitate the identification of software components with known vulnerabilities. Utilizing publicly available SBOM samples, our team was able to identify locations of known vulnerabilities for individual components inventoried within SBOMs, however, the sheer volume of components contained within SBOMs, makes this process incredibly tedious and likely unrealistic for risk managers to perform on a regular basis.

D. MAPPING VULNERABILITIES TO SOFTWARE RISK CATEGORIES

To better understand how to identify vulnerabilities and potential threats within SBOMs, our team needed to understand what types of risk are relevant to the EITaaS program. After discussion of our intent, our sponsor identified risk taxonomy relevant to the DOD with 11 main risk categories and 27 subcategories which can be grouped with parallels to MITRE's System of Trust. This framework was developed by the MITRE

Corporation, a nonprofit focused on the development and advancement of national security (MITRE Corporation, n.d.-b). The System of Trust was intended to be a framework focused on identifying trustworthy supplies, suppliers and services through a robust supply chain security framework with analysis of 14 key risk areas and over 1,200 risk factors (MITRE Corporation, n.d.-a).

Through the creation of a crosswalk between DOD risk taxonomy and MITRE's supply chain risk taxonomy we were able to highlight the five most critical categories to the EITaaS Program's risk management framework. The EITaaS SCRM team identified green categories as a direct translation, yellow are close translations and red are indirect translations of MITRE's System of Trust to DOD taxonomy, see Table 2. There was one category within the DOD taxonomy that could be correlated with two MITRE categories; DOD's foreign ownership control or influence has similar connotations to MITRE's external influences and maliciousness categories.

Table 2. Crosswalk for MITRE Risk Categories to DOD Risk Categories

MITRE	DOD
External influences • Relationships w/countries of concern • Operational locations in CoC • Foreign incorporation • Geopolitical instability • National corruption & governance • Political vulnerability	Foreign Ownership Control or Influence • Counterintelligence Analysis • Nationalization • Partnership w/State-owned Entity • Provenance
Susceptibility • Customers • Industry Sector • Location • Personnel • Technical	Economic • Demand Shocks • Economic Instability Infrastructure • Buildings conditions • Equipment
Quality Culture • Low CMMI rating • Internal SCRM policy/practice	Policial and Regulatory • New Regulations, Changes in Policy

MITRE	DOD
• Subcontractor supply chain health/risk	
Maliciousness • Foreign Intelligence Service influence • Fraud and Corruption • Legal/law issues • Sanction list status	Political and Regulatory • Corruption • Government Policies Foreign Ownership Control or Influence • Sabotage • Veiled Venture • Cyber/Industrial Espionage Compliance • Fraud • Ethics Violation
Organizational security • Facility Access • Software Access • Hardware Access • Cyber Threat Activity • Data security status • Security training • Vulnerabilities	Manufacturing and Supply • Material Sources • Sole Source Dependency • Outsourcing • Equipment Downtime Technology and Cyber Security • Critical Hardware/Software Vulnerability • Cyber Attack • Data Breach • Unsecure Networks or Systems Product Quality and Design • Counterfeit parts • Non-conforming parts Infrastructure • Security

This information provided key insights critical to understanding DOD risk and the focus of software risk management teams. In order to interpret how SBOMs could be utilized to identify these types of risks, our team chose a single risk subcategory and searched for indicators within simple SBOM samples. During early phases of the H4D

project, the EITaaS SCRM team identified that one of their greatest concerns was the inability to conduct subcontractor vetting. The program office was unsure where software originated or who created the components utilized to create the software and relied heavily on contractors to self-identify areas of risk (DAF, 2022). This creates a lack of visibility of the software supply chain and makes risk management processes fundamentally more difficult and complex than tangible supply chains, especially where lower tier subcontractors are concerned. The EITaaS SCRM team was unable to identify if software originated from untrustworthy sources or if any software components were vulnerable to exploitation.

This inspired our selection of the provenance subcategory to demonstrate how SBOMs could be utilized to increase visibility and mitigate risk. Provenance, as defined by NIST, is the “The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data.” (National Institute of Standards and Technology, n.d.-b). Provenance risk is closely tied to the origins of software. Utilizing SBOM samples, we discovered that if the author of a piece of software can be identified, but the authors of dozens of open-source components within the software cannot be identified, then the software is inherently riskier than software that does identify authors of all components. Through our experimentation we were able to prove that SBOMs can illuminate just how many components lack provenance and can be assigned a risk score based on that level of provenance.

E. WORKING GROUPS

During our post-H4D discovery phase, we actively practiced engaged scholarship by collaborating with working groups actively addressing real-world problems, which aligned with our research goals to enhance software supply chain risk management for the DOD (Mathiassen, 2017).

As we pursued inter-agency collaboration on SBOM utilization and integration into DOD-specific risk management processes, our interactions extended to a broader network of stakeholders. Among these engagements, one of the most notable collaborations was

with the DOD CIO, which proved to be a pivotal moment that illuminated a traversable path for managing software supply chain risks within the DOD.

Our scholastic engagement also included the 309th Software Engineering Group at Hill Air Force Base, who are actively working to incorporate SBOMs into software risk analysis and cybersecurity. This group is involved in cultivating a better understanding of SBOMs by developing them in-house and obtaining SBOMs from their own contractors, providing essential insights into the practicalities and challenges of SBOM implementation.

To further enhance our research efforts, we formed a working group with a DAF employee experienced in creating dashboards. This collaboration was instrumental for establishing realistic parameters for developing our own prototype dashboard for SBOM analysis and software SCRM visualizations.

The significance of these interactions lies in their potential to reshape the DOD's approach to software supply chain risk management. Leveraging the practical experiences and outcomes from these collaborations, the DOD can establish a comprehensive, agile, and adaptive approach to software risk management. The lessons learned and strategies developed within these collaborations have the power to inform DOD-wide policies, disseminating best practices and innovative methodologies across various military branches and departments. This collective engagement represents not only a practical step forward but also a strategic blueprint for enhancing DOD's cybersecurity posture, enabling a robust defense against the ever-evolving landscape of the software supply chain.

F. SUMMARY

To summarize this phase of exploration, our team examined the fundamental principles upon which SBOMs were built. This foundational understanding led us to recognize the minimum elements required for constructing a comprehensive SBOM, as recommended by the NTIA. This exploration extended to the investigation of existing and widely adopted SBOM formats prevalent in industry practices, including SPDX, CycloneDX, and SWID. Assessment of these formats allowed us to discern their unique

attributes, strengths, and potential limitations, providing a comprehensive understanding on the importance of SBOM structure with relevance to the DOD.

A significant aspect of our exploration involved identifying vulnerabilities within the software components and mapping them meticulously to risk categories unique to the DOD's operational context. This mapping process was vital, as it not only highlighted potential weaknesses but also enabled a basic understanding of their possible impact within the DOD's software supply chains. This multifaceted understanding became the cornerstone of our vision for a robust supply chain risk management framework. It allowed us to conceptualize a framework that not only addresses vulnerabilities but also factors in the specific challenges faced by the DOD, ensuring a proactive, adaptive, and resilient defense against evolving threats in the dynamic landscape of software supply chains.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. FINAL MVP: SBOM DASHBOARD PROTOTYPE

A. FINAL MVP HYPOTHESIS

We believed that the EITaaS program was facing a gap—a lack of comprehensive technical comprehension regarding the creation, storage, and processing of SBOMs. This was not just an academic supposition. During our preliminary discussion with our sponsor, our queries about SBOMs elicited responses that pointed toward a limited, perhaps even nebulous, understanding of the topic. Consequently, our final hypothesis to test crystallized around the idea that we could enhance the EITaaS program’s grasp on SBOMs by conceptualizing, designing and executing a prototype of a straightforward SBOM process. This, in turn, would strategically position them to roll out a pilot SBOM program, setting the stage for deeper exploration and learning from field use.

B. NPS SBOM DASHBOARD MVP

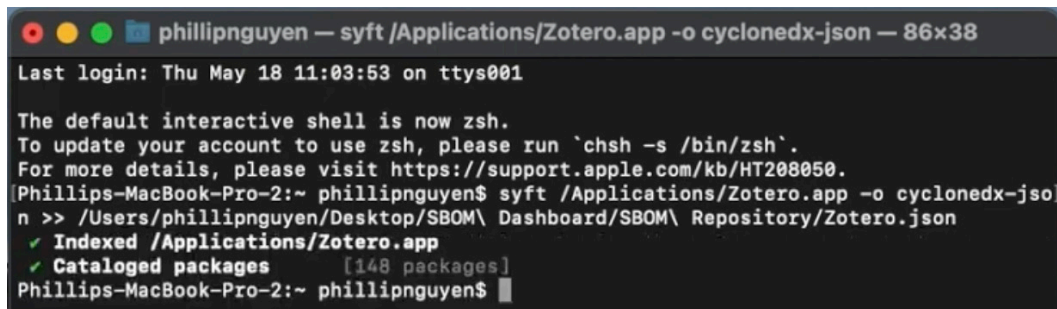
The primary objective behind our final MVP was to establish a rudimentary process encompassing SBOM generation, storage, scanning, and vulnerability identification. Leveraging a medley of open-source software, the capabilities of ChatGPT, Python programming, and personal hardware resources, we successfully orchestrated a basic SBOM procedure at no financial expense.

1. SBOM Development

The foundational step in our journey was the creation of an SBOM for a designated software. For our study, we chose Zotero as our exemplar. As an open-source application frequently employed by NPS students for thesis citation management, Zotero emerges as an ideal candidate for analysis. Its intrinsic nature as an open-source application developed through other open-source software components makes it representative for our purpose (Corporation for Digital Scholarship, 2023).

Initiating the process required us to prepare his MacBook for Syft’s installation. This necessitated the installation of Homebrew—an open-source software package management system optimized for macOS, renowned for its ability to streamline software

installations (Nguyen, 2023a). With Homebrew firmly in place, the path was paved for the installation of Syft. Once armed with Syft, we directed it to scan Zotero with the objective of generating an SBOM. Employing the terminal commands as illustrated in Figure 11, Syft executed the task with precision, producing an SBOM within mere seconds.



```
phillipnguyen — syft /Applications/Zotero.app -o cyclonedx-json — 86x38
Last login: Thu May 18 11:03:53 on ttys001

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
Phillips-MacBook-Pro-2:~ phillipnguyen$ syft /Applications/Zotero.app -o cyclonedx-json
n >> /Users/phillipnguyen/Desktop/SBOM\ Dashboard/SBOM\ Repository/Zotero.json
✓ Indexed /Applications/Zotero.app
✓ Cataloged packages [148 packages]
Phillips-MacBook-Pro-2:~ phillipnguyen$
```

Figure 11. Syft Mac Terminal Commands Adapted from Apple Inc., (2022b)

Upon completion, the SBOM was exported as a .json file. This file was then saved to a designated folder on a desktop, which we established as our primary SBOM repository.

2. SBOM Repository

SBOMs, by design, are machine-readable files. To extract their full potential, especially for representation on a dashboard, they require a centralized storage system or repository. For the scope of our project, we opted for a pragmatic approach. As depicted in Figure 12 the SBOM generated for Zotero, alongside other SBOMs we cultivated, was stored in a dedicated file folder on our personal laptop. This file folder was not merely a storage location but was conceptualized and operationalized to serve as our primary repository, integral for our dashboard’s functionality.

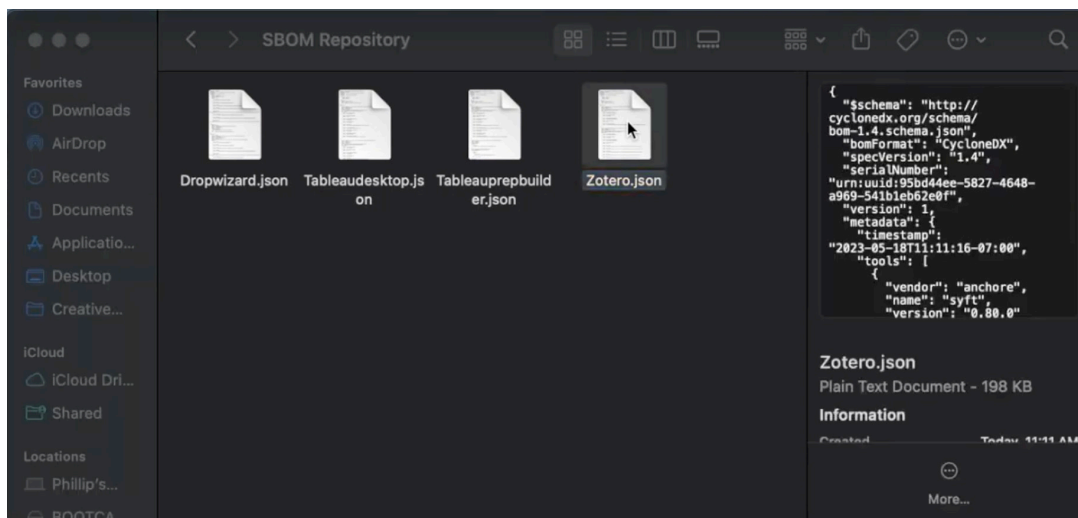


Figure 12. Zotero Generated SBOM in File Folder Repository.
Adapted from Apple Inc. (2022a)

This file folder was not merely a storage location but was conceptualized and operationalized to serve as our primary repository, integral for our dashboard’s functionality.

3. SBOM Digestion

As showcased in Figure 13, the initial page of our generated SBOM for Zotero offers a glimpse into its complexity. It adheres to the CDX SBOM format and is presented as a .json file type—a format renowned for its machine-readability. However, therein lies a fundamental challenge. The sheer volume and intricacy of data encapsulated within SBOMs render them overwhelming for human interpretation. SBOMs can span thousands of lines, each containing pivotal information.

This challenge is not unique to our context. As highlighted by Captain Siangpipop in his NPS thesis titled “Visualizing Business Intelligence,” the contemporary dilemma is not the scarcity of data but it’s overwhelming abundance. He notes, “In our day and age, there is no longer a problem of lack of data rather the problem today is too much data, or data saturation/InfoObesity” (Siangpipop, 2022). Captain Siangpipop’s thesis as well as Whitley’s article, “Why Too Much Data is a Problem and How to Prevent It” underscores

the pressing need for efficient mechanisms to digest and distill the essence from such extensive datasets (Siangpipop, 2022; Whitler, 2018).

```
{
  "$schema": "http://cyclonedx.org/schema/bom-1.4.schema.json",
  "bomFormat": "CycloneDX",
  "specVersion": "1.4",
  "serialNumber": "urn:uuid:1c9cfd2a-b041-4409-842b-7e8abdb061eb",
  "version": 1,
  "metadata": {
    "timestamp": "2023-05-12T15:10:39-07:00",
    "tools": [
      {
        "vendor": "anchore",
        "name": "syft",
        "version": "0.80.0"
      }
    ],
    "component": {
      "bom-ref": "897e9237189dbaf6",
      "type": "file",
      "name": "/Applications/Zotero.app"
    }
  },
  "components": [
    {
      "bom-ref": "pkg:npm/%40tootallnate/once@2.0.0?package-id=e2f4c6877ed20d2c",
      "type": "library",
      "name": "@tootallnate/once",
      "version": "2.0.0",
      "cpe": "cpe:2.3:a:@tootallnate\\once:\\@tootallnate\\once:2.0.0:*:*:*:*:*",
      "purl": "pkg:npm/%40tootallnate/once@2.0.0",
      "properties": [
        {
          "name": "syft:package:foundBy",
          "value": "javascript-lock-cataloger"
        },
        {
          "name": "syft:package:language",
          "value": "javascript"
        },
        {
          "name": "syft:package:metadataType",
          "value": "NpmPackageLockJsonMetadata"
        },
        {
          "name": "syft:package:type",
          "value": "npm"
        },
        {
          "name": "syft:location:0:path",
          "value": "Contents/PlugIns/ZoteroSafariExtension.appex/Contents/Resources/safari/utilities/package-lock.json"
        }
      ]
    },
    {
      "bom-ref": "pkg:npm/%40ungap/promise-all-settled@1.1.2?package-id=6c3c9519a5dd40ba",
      "type": "library",
      "name": "@ungap/promise-all-settled",
      "version": "1.1.2",
      "cpe": "cpe:2.3:a:@ungap\\promise-all-settled:\\@ungap\\promise-all-settled:1.1.2:*:*:*:*:*",
      "purl": "pkg:npm/%40ungap/promise-all-settled@1.1.2",
      "properties": [
        {
          "name": "syft:package:foundBy",
          "value": "javascript-lock-cataloger"
        },
        {
          "name": "syft:package:language",
          "value": "javascript"
        }
      ]
    }
  ]
}
```

Figure 13. Zotero in CycloneDX Version 1.4 SBOM Format as .json File Type. Source: Apple Inc (2022c)

Confronted with this immense data volume, our solution pivoted towards harnessing the power of Python—a versatile programming language ideal for data processing tasks. We embarked on creating a dashboard capable of extracting and showcasing pertinent data from the machine-readable SBOMs.

Figure 14 offers an illustrative journey of our process. It is noteworthy to mention that our group started this endeavor with no prior coding experience. However, this

potential hindrance was deftly navigated with the assistance of ChatGPT, which served as our guide in the Python coding realm. Through its guidance, we were able to sculpt an efficient and user-friendly SBOM dashboard.

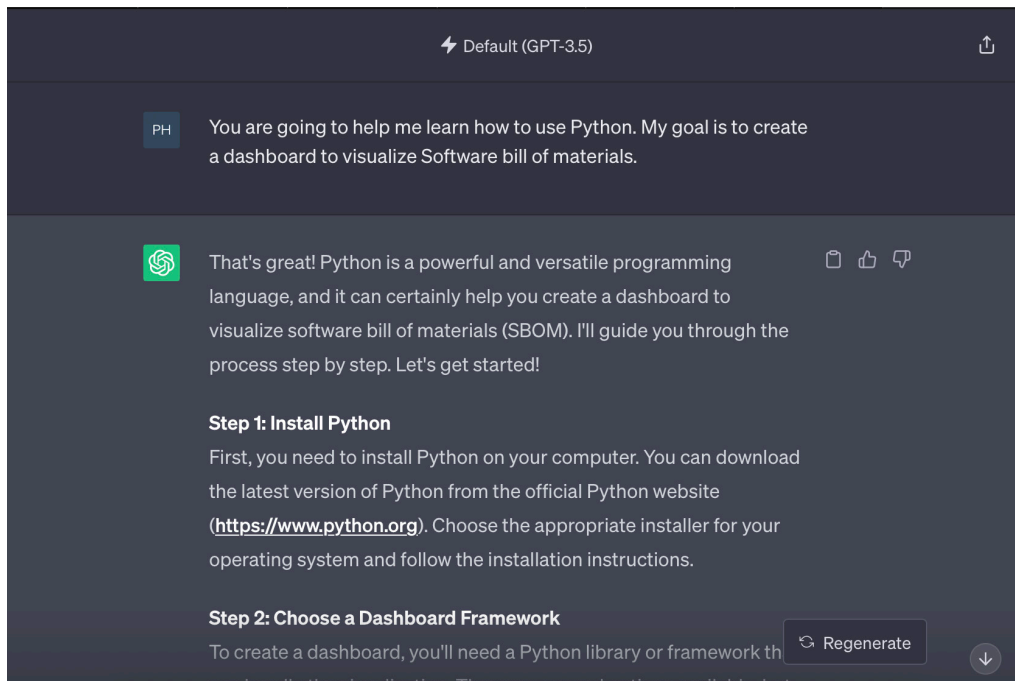


Figure 14. ChatGPT Sample Prompt for Python Coding Assistance. Adapted from OpenAI (2023)

The journey from conception to realization wasn't a straightforward one. It entailed 182 distinct prompts within ChatGPT, each acting as a steppingstone towards the ultimate goal—a functional dashboard. The process, while challenging, was highly instructive. After investing approximately four hours in meticulously transferring, adapting, and refining code snippets from ChatGPT to Python, we successfully amalgamated the various pieces of Python code.

Figure 15 visually encapsulates this developmental journey, showcasing both the iterative process through ChatGPT prompts and the resultant Python code. The culmination of this rigorous effort is a dashboard that not only processes vast amounts of SBOM data but also presents it in a digestible and user-centric manner.

```

import os
import glob
import dash
import webbrowser
from dash import dcc
from dash import html
import json
from dash.dependencies import Input, Output, State
from dash.dash_table import DataTable
from urllib.parse import quote

# Folder path containing SBOM files
sbom_folder = '/Users/phillipnguyen/Desktop/SBOM Dashboard/SBOM Repository/'

# Get list of SBOM file paths from the folder
sbom_files = glob.glob(os.path.join(sbom_folder, '*.json'))

# Create an empty list to store component details from all SBOMs
component_details = []

# Loop through each SBOM file
for sbom_file in sbom_files:
    # Load the SBOM JSON data from file
    with open(sbom_file) as file:
        sbom_data = json.load(file)

    # Extract relevant information from SBOM data
    components = sbom_data.get('components', [])

    # Get the last part of the file path without extension
    sbom_name = os.path.splitext(os.path.basename(sbom_file))[0]

    # Append component details from the current SBOM to the overall list
    component_details.extend([
        {
            'sbom_file': sbom_name,
            'name': component.get('name', 'Unknown'),
            'version': component.get('version', 'Unknown'),
            'purl': component.get('purl', 'Unknown').replace('pkg:', ''),
            'cpe': component.get('cpe', 'Unknown')
        }
        for component in components
    ])

# Build your Dash dashboard using the SBOM data
app = dash.Dash(__name__)

app.layout = html.Div(
    children=[
        dcc.Location(id='url', refresh=False),
        html.H1("NPS SBOM Dashboard v1.0 (CycloneDX)", style={'text-align': 'center'}),
        html.H3("Filter by SBOM File:"),
        dcc.Dropdown(
            id='sbom-dropdown',
            options=[
                {'label': os.path.basename(file_path).replace('.json', ''), 'value': file_path}
                for file_path in sbom_files
            ],
            placeholder="Select SBOM File"
        ),
        html.H3("Component Details:"),
        dcc.Input(
            id='search-input',
            type='text',
            placeholder='Search by component name...',
            style={'width': '300px', 'margin-bottom': '10px'}
        ),
        DataTable(

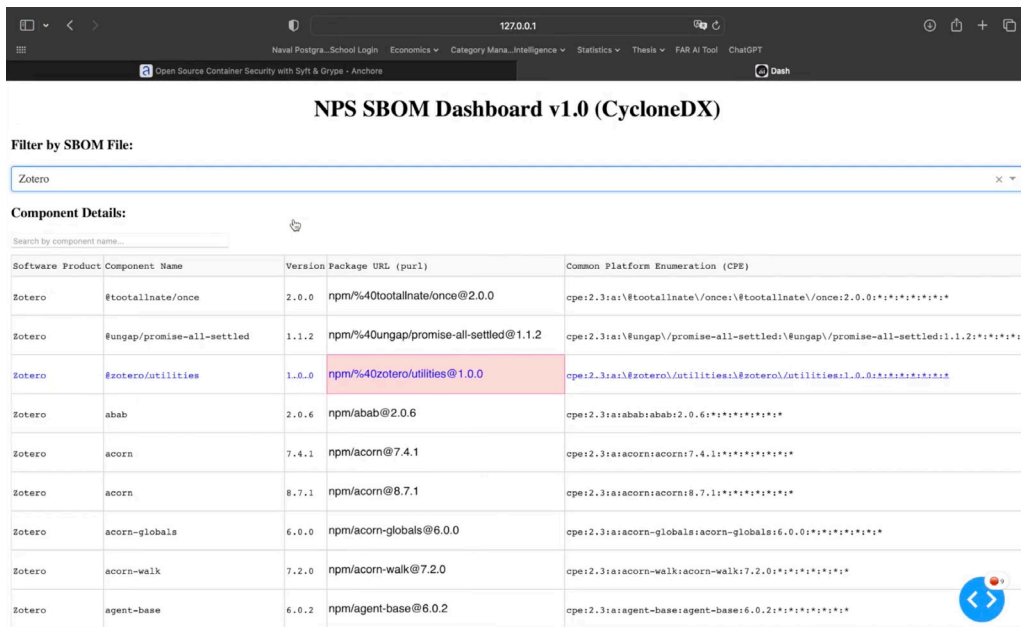
```

Figure 15. SBOM Extraction Python Code. Adapted from Python Software Foundation (2023)

Upon execution, the Python code rapidly scans each SBOM in our repository. It then extracts key information and populates our dashboard, presenting the data in an organized table format for easy interpretation and analysis.

4. SBOM Dashboard

The inaugural version, NPS SBOM Dashboard v1.0, efficiently retrieved data from the SBOMs in our repository. It presented this information coherently in a table format, as depicted in Figure 16.



NPS SBOM Dashboard v1.0 (CycloneDX)

Filter by SBOM File:
Zotero

Component Details:

Software Product	Component Name	Version	Package URL (purl)	Common Platform Enumeration (CPE)
Zotero	#tootallnate/once	2.0.0	npm/%40tootallnate/once@2.0.0	cpe:2.3:a:\#tootallnate\once:\#tootallnate\once:2.0.0:*:*:*:*:*
Zotero	#ungap/promise-all-settled	1.1.2	npm/%40ungap/promise-all-settled@1.1.2	cpe:2.3:a:\#ungap\promise-all-settled:\#ungap\promise-all-settled:1.1.2:*:*:*:*:*
Zotero	#zotero/utilities	1.0.0	npm/%40zotero/utilities@1.0.0	cpe:2.3:a:\#zotero\utilities:\#zotero\utilities:1.0.0:*:*:*:*:*
Zotero	abab	2.0.6	npm/abab@2.0.6	cpe:2.3:a:abab:abab:2.0.6:*:*:*:*:*
Zotero	acorn	7.4.1	npm/acorn@7.4.1	cpe:2.3:a:acorn:acorn:7.4.1:*:*:*:*:*
Zotero	acorn	8.7.1	npm/acorn@8.7.1	cpe:2.3:a:acorn:acorn:8.7.1:*:*:*:*:*
Zotero	acorn-globals	6.0.0	npm/acorn-globals@6.0.0	cpe:2.3:a:acorn-globals:acorn-globals:6.0.0:*:*:*:*:*
Zotero	acorn-walk	7.2.0	npm/acorn-walk@7.2.0	cpe:2.3:a:acorn-walk:acorn-walk:7.2.0:*:*:*:*:*
Zotero	agent-base	6.0.2	npm/agent-base@6.0.2	cpe:2.3:a:agent-base:agent-base:6.0.2:*:*:*:*:*

Figure 16. NPS SBOM Dashboard V1.0 (CycloneDX) Interface

The table within the NPS SBOM Dashboard ensures immediate accessibility and clarity for all software components listed. Additionally, users can filter the dashboard by specific SBOM files or software applications, further enhancing usability, as demonstrated in Figure 17.

Filter by SBOM File:



Select SBOM File

- Tableauprepbuilder
- Zotero
- TableaudeSKTOP
- Dropwizard

Figure 17. NPS SBOM Dashboard Filter Feature

The dashboard further optimizes user experience by hyperlinking Package uniform resource locators. This feature allows users to swiftly access the source repository of a particular software component, as illustrated in Figure 18.

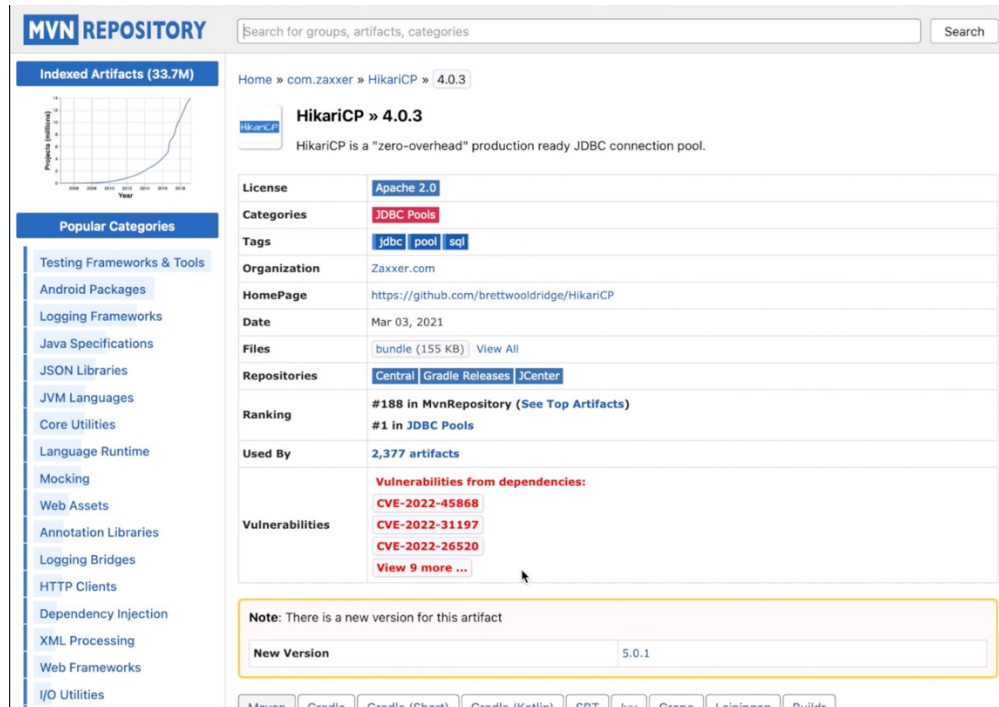


Figure 18. Component HikariCP Version 4.0.3. Source: Rodriguez Olivera (2023)

Accessing the software component's repository offers multiple advantages. Not only can one validate the software version in use, but also ensure that the application is leveraging the most recent version, which ideally incorporates the latest patches and updates. For instance, the HikariCP component, version 4.0.3, has been identified with 12 known vulnerabilities. Further investigation would reveal the availability of a newer, potentially more secure version of this component.

One of the pivotal features of the SBOM dashboard is its component search functionality. This becomes particularly invaluable when a program office receives an alert regarding a vulnerability. With the search tool, they can swiftly identify all software applications that incorporate the flagged vulnerable component. For illustrative purposes, Figure 19 showcases a search for the component "commons-codec."

NPS SBOM Dashboard v1.0 (CycloneDX)				
Filter by SBOM File:				
Select SBOM File				
Component Details:				
commons-codec				
Software Product	Component Name	Version	Package URL (purl)	Common Platform Enumeration (CPE)
Tableauprepbuilder	commons-codec	1.15	maven/commons-codec/commons-codec@1.15	cpe:2.3:a:apache:commons-codec:1.15:*:*:*:*:*
Tableauprepbuilder	commons-codec	1.15	maven/commons-codec/commons-codec@1.15	cpe:2.3:a:apache:commons-codec:1.15:*:*:*:*:*
Tableauprepbuilder	commons-codec	1.15	maven/commons-codec/commons-codec@1.15	cpe:2.3:a:apache:commons-codec:1.15:*:*:*:*:*
Tableauprepbuilder	commons-codec	1.15	maven/commons-codec/commons-codec@1.15	cpe:2.3:a:apache:commons-codec:1.15:*:*:*:*:*
Tableauprepbuilder	commons-codec	1.15	maven/commons-codec/commons-codec@1.15	cpe:2.3:a:apache:commons-codec:1.15:*:*:*:*:*
TableaudeSKTOP	commons-codec	1.15	maven/commons-codec/commons-codec@1.15	cpe:2.3:a:apache:commons-codec:1.15:*:*:*:*:*
TableaudeSKTOP	commons-codec	1.15	maven/commons-codec/commons-codec@1.15	cpe:2.3:a:apache:commons-codec:1.15:*:*:*:*:*
Dropwizard	commons-codec	1.11	maven/commons-codec/commons-codec@1.11?type=jar	Unknown

Figure 19. Component Search Feature

Utilizing the component search feature, it becomes evident that the “commons-codec” component is incorporated into three distinct software products within our repository. This insight underscores the importance of the dashboard in facilitating rapid vulnerability assessment across multiple applications.

5. MVP Results

To succinctly showcase our complete SBOM process, we curated a comprehensive demo video and made it accessible via YouTube as seen in Figure 20:

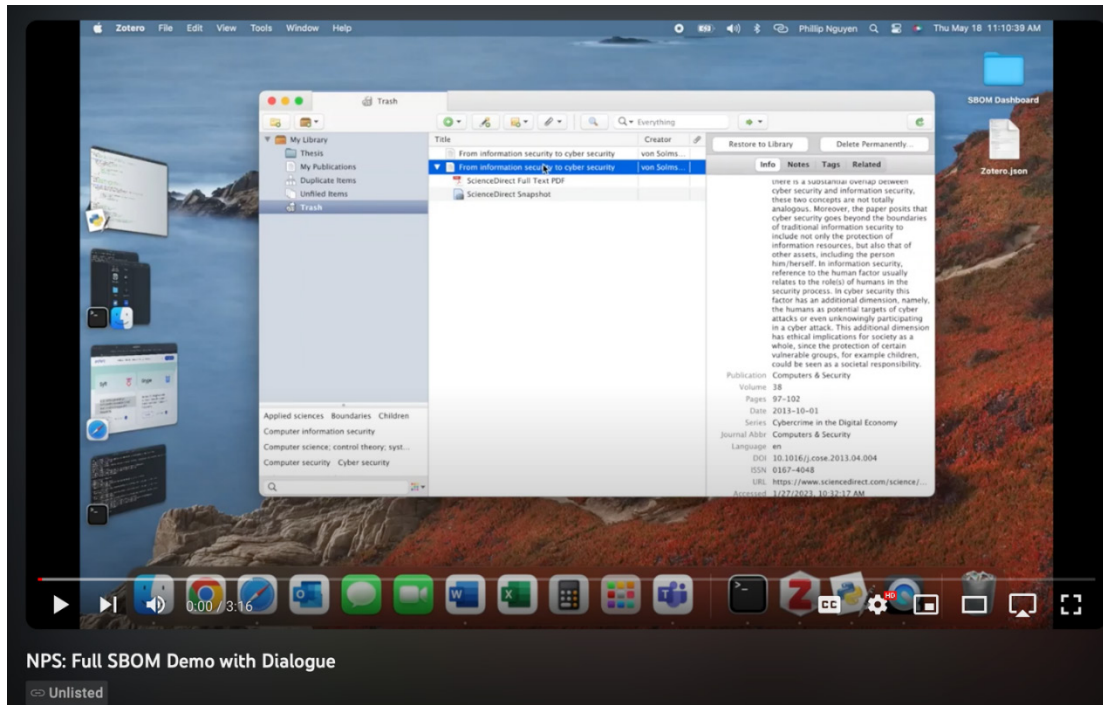


Figure 20. NPS: Full SBOM Demo with Dialogue. Source: Nguyen (2023b)

You can watch the full video here: <https://www.youtube.com/watch?v=Dy1KM7456jg>.

6. Final MVP Summary

The EITaaS Program Office’s response to our MVP was overwhelmingly positive. As articulated by Mr. Peter Lee, our visual demonstration served as a pivotal tool in clarifying and simplifying the concept of SBOMs. The need of the hour for the EITaaS program was a foundational understanding of SBOMs, and our MVP catered to this precise requirement. By offering them this hands-on, unbiased, and in-depth demo, we illuminated the path regarding how SBOMs can be efficiently formulated, preserved, processed, and employed.

We are optimistic that armed with this newfound clarity, the EITaaS program stands well-equipped to embark on their SBOM pilot program. Beyond immediate education, our MVP has laid down a framework that the EITaaS program can adapt and expand upon, laying the groundwork for their bespoke SBOM procedure.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. SYSTEM DYNAMICS SBOM POLICY MODEL

After developing a prototype of a software SCRM dashboard, there was a need to understand the process that would sustain the acquisition of SBOMs, what portions of the current acquisition system may be impacted by an SBOM policy, and determine if we could quantify what impact a SBOM policy would have on the DAF. The DAF has spent between \$7 billion and \$8 billion annually on IT contracts from 2018 to 2022 (AFICC/KA, 2023). As the DAF continues to outsource its IT Services, the organization needs to find better ways to minimize the risk associated with outsourcing. The software supply chain ecosystem is complex and consists of numerous components, contributors, distribution channels, technologies, and practices (Schwartz, 2021). The lack of transparency over this complex cyber supply can expose the DAF to cyberattacks. According to IBM, “the global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years” (2023).

As we discovered through our prior research, one potential way the DAF could minimize cyber incident risk is by adopting a SBOM policy. According to the NTIA, “An SBOM provides those who produce, purchase, and operate software with information that enhances their understanding of the supply chain, which enables multiple benefits, most notably the potential to track known and newly emerged vulnerabilities and risks” (NTIA, 2021b). The DAF needs to find a way to reduce the number of malicious attacks and the economic damage that comes from these cyberattacks. Mandating that contractors provide SBOMs would increase transparency into the contributors, composition, and functionality of the software products that the DAF is purchasing. This increased transparency would enhance the DAF’s ability to detect software vulnerabilities independently, enhance the accountability of contractors, and strengthen the collaboration on tackling software vulnerabilities between government and the private sector. Our system dynamics model posits that the adoption of an SBOM policy within the DAF will lead to a reduction in both the frequency of successful cyberattacks and the associated economic losses.

SBOMs are under active consideration by the DOD as a mechanism to augment cybersecurity within the software supply chain (White House, 2021). Despite its potential

merits, the adoption of a SBOM policy has met resistance both within governmental circles and the broader private sector. One core issue contributing to this resistance is the inherent complexity of the software supply chain ecosystem; a complexity so formidable that it challenges comprehensive understanding and straightforward policy formulation.

In navigating this complexity, system dynamics emerges as a valuable analytical tool. As noted by Sterman, a leading authority in the field

Complex dynamic systems introduce multiple barriers to effective learning and understanding. Overcoming these challenges to improve our comprehension of such systems is itself a complex issue. System dynamics offers a robust methodology for gaining invaluable insights into scenarios characterized by dynamic complexity and policy resistance. Its application is increasingly observed in both corporate strategy and public policy domains to formulate more efficacious policies (Sterman, 2000, p. 39).

This multidimensional perspective underscores the potential of system dynamics to untangle the intricate web of relationships and variables within the software supply chain, thereby providing a more informed foundation upon which to assess the efficacy of implementing an SBOM policy.

A. SBOM CAUSAL LOOP DIAGRAM

A causal loop diagram (CLD) is a qualitative tool that can help us understand the cause and effect relationships of key variables related to SBOMs within the DAF's software supply chain IT acquisition system. According to Sterman

CLDs are an important tool for representing the feedback structure of systems. Long used in academic work, and increasingly common in business, CLDs are excellent for quickly capturing your hypotheses about the causes of dynamics, eliciting and capturing the mental models of individuals or teams, and communicating the important feedback you believe are responsible for a problem (Sterman, 2000, p. 137).

Within the CLD, causal links are designated as either positive or negative, indicated by a (+) or (-) symbol respectively. To clarify, Sterman states, a positive link signifies that an increase in the causal factor will correspondingly lead to an increase in the outcome, and vice versa for a decrease. Conversely, a negative link indicates that an increase in the causal factor will lead to a reduction in the outcome, and a decrease will result in an

elevation of the outcome (Sterman, 2000, p. 139). The main feedback loops in our CLD as seen in Figure 21, are AF IT Acquisition, AF Software Security, Contractor (KTR) Software Security, AF SCRM, AF IT Manpower and AF Contracts. Throughout our system dynamics project, in our CLD and model, we abbreviated contractor to “KTR” for brevity in our figures.

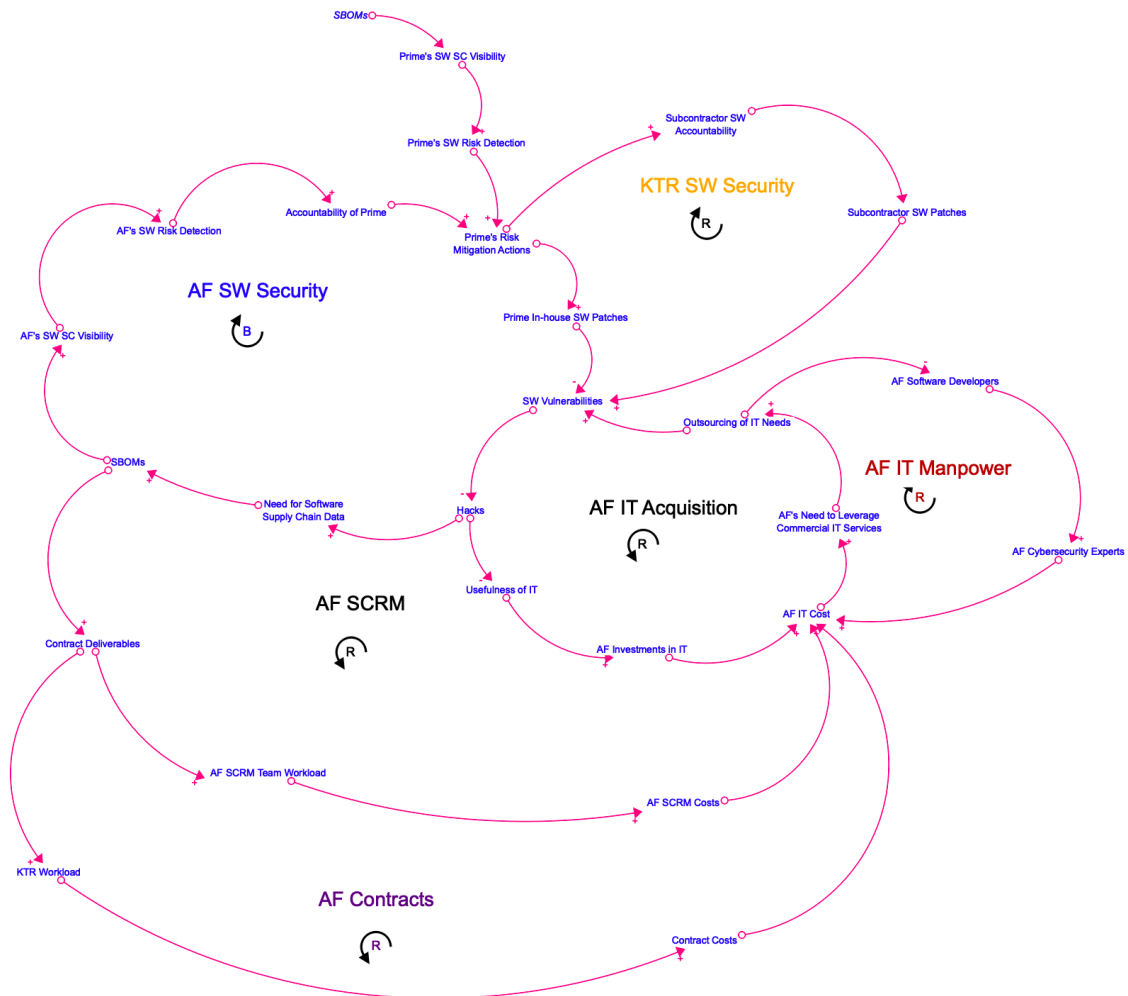


Figure 21. SBOM CLD. Adapted from ISEE Systems (2023)

We believe these are the main feedback loops responsible for cyberattacks and affected by a SBOM policy. The main variables connecting these feedback loops are

cyberattack attempts, further known as hacks, SBOMs, and the total cost to the DAF for their IT, referred to as AF IT cost.

1. AF IT Acquisition Loop

The main feedback loop is the reinforcing AF IT Acquisition loop as seen in Figure 22.

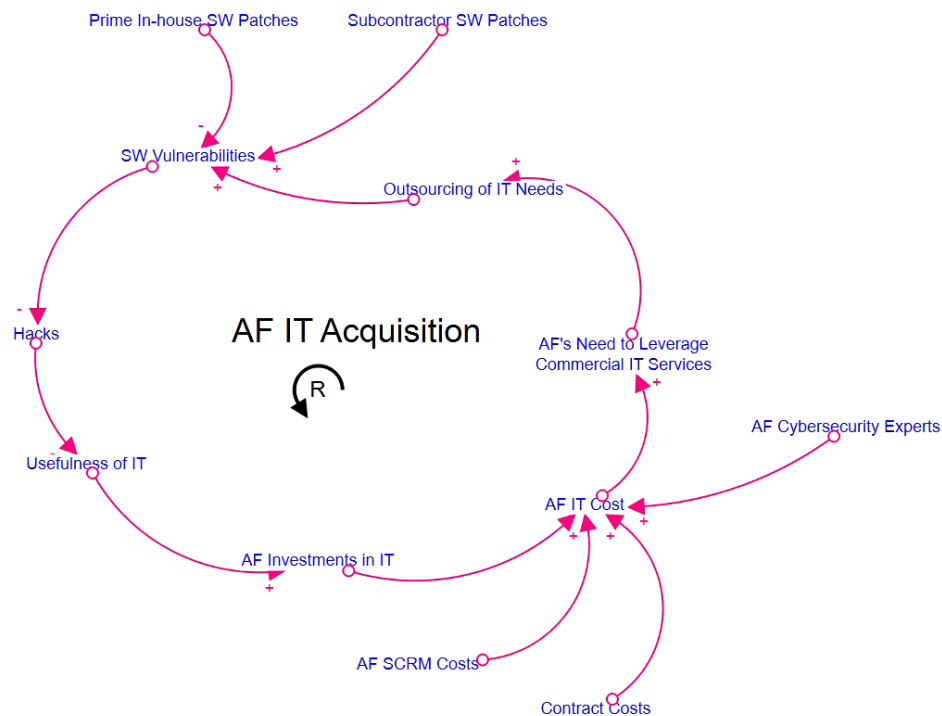


Figure 22. AF IT Acquisition CLD Section. Adapted from ISEE Systems (2023)

This section elaborates on the logic governing this loop by delineating the causal links connecting the involved variables. We commence our explanation with the initial variable: “Usefulness of IT.” In this reinforcing loop, the causal sequence can be summarized as follows. An increase in the “Usefulness of IT” spurs greater “AF Investments in IT.” Elevated “AF Investments in IT” lead to a rise in “AF IT Costs.” Rising “AF IT Costs” amplify the “AF’s Dependency on Commercial IT Services.” This heightened dependency, in turn, accelerates “Outsourcing of IT Needs.” An uptick in

outsourcing engenders a surge in “Software Vulnerabilities.” “Software Vulnerabilities” escalate the frequency of cyberattack attempts, commonly referred to as “Hacks.” A rise in “Hacks” undermines the “Usefulness of IT,” thus closing the loop.

2. AF Security Loop

The second loop, AF Software Security, Figure 23, connects the variables “Hacks” and “SBOMs.” As more hacks into the AF network are detected there is an increasing need for software supply chain data. It has been discovered that the best way to gather supply chain data for software is with SBOMs as the NTIA states that SBOMs increase vulnerability identification (NTIA, 2021b).

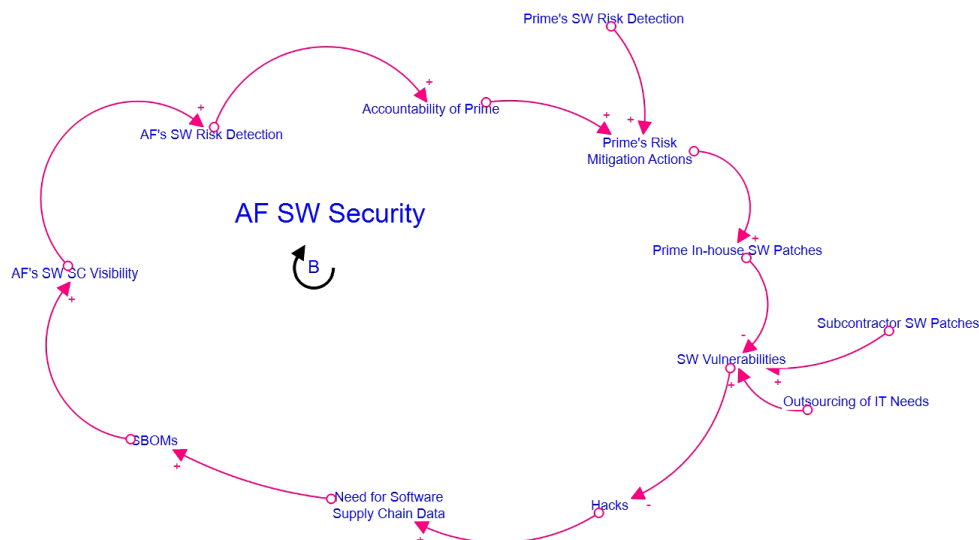


Figure 23. AF Software Security CLD Section. Adapted from ISEE Systems (2023)

We commence our explanation with the initial variable: “SW Vulnerabilities.” An increase in “Software Vulnerabilities” leads to a rise in the incidence of cyberattacks, commonly termed “Hacks.” A surge in hacks intensifies the demand for robust “Software Supply Chain Data.” This elevated demand consequently boosts the adoption of “SBOMs.” With increased SBOM adoption, visibility into the AF’s software supply chain is enhanced. Enhanced visibility improves the AF’s capability for software risk detection. Greater risk

detection heightens the “Accountability of the Prime” contractor involved. Heightened accountability encourages more proactive “Prime [contractor] Risk Mitigation Measures.” These measures result in an escalation in both “Prime In-house Software Patches” and “Sub-KTR Software Patches.” Finally, the increased frequency of these patches contributes to a reduction in “Software Vulnerabilities,” completing the loop.

3. Contractor Software Security Loop

This loop describes the causal loop between prime and subcontractors in the software supply chain. This loop, Figure 24, is an extension of the aforementioned AF Security Loop and outlines the dynamics that influence software security at both the prime contractor and subcontractor levels. An uptick in prime contractor accountability precipitates an increase in proactive “Risk Mitigation Actions” by the prime contractor. These heightened “Risk Mitigation Actions” induce a corresponding rise in “Sub-KTR Software Accountability.” Elevated “Sub-KTR Software Accountability” catalyzes an increase in the frequency of “Sub-KTR Software Patches.” The proliferation of these patches, in turn, contributes to a reduction in “Software Vulnerabilities.” The loop continues and closes through the AF Security Loop.

4. AF Supply Chain Risk Management Loop

The AF SCRM reinforcing loop plays an important role as AF SCRM teams request and analyze SBOMs. They are responsible for managing risk within their software supply chain. This loop serves as an extension of the earlier discussed AF IT Acquisition Loop and focuses on how SCRM teams, tasked with software supply chain risk management, interact with various variables. The causal chain is articulated as follows. A rise in “Software Vulnerabilities” incites an escalation in “Hacks.” Increased hacks heighten the demand for comprehensive supply chain data. This augmented demand triggers an uptick in the generation and provision of “SBOMs.” The proliferation of “SBOMs” expands the “Contract Deliverables” that SCRM teams are obligated to scrutinize. This expansion contributes to an increase in the “SCRM Workload,” in turn escalating the associated “SCRM Costs.” As “SCRM Costs” rise, this exerts upward pressure on the overall “AF IT Costs.”

5. AF Contracts Loop

This section explores the feedback loop involving AF contracts focusing on how the requisition of SBOMs from software contractors can impact the AF's overall IT costs. This loop serves as a connector between the AF SCRM Loop and the AF IT Acquisition Loop. The causal chain operates as follows. An increase in "Contract Deliverables," stemming from the requirement for SBOMs, leads to a commensurate increase in "KTR Workload." The elevated "KTR Workload" results in an upswing in "Contract Costs." This escalation in "Contract Costs" exerts an upward influence on the total "AF IT Costs." This dynamic then flows back into the AF IT Acquisition Loop, creating a reinforcing cycle.

6. AF IT Manpower Loop

The final feedback loop included is a reinforcing AF IT Manpower loop that is affected by the outsourcing of AF IT needs which impacts the number of cybersecurity personnel kept or added to the career field to handle hacks. This loop highlights how changes in the sourcing strategy for IT needs can influence the composition and cost of in-house technical manpower. The causal chain unfolds as follows. An acceleration in the "Outsourcing of IT" functions precipitates a reduction in the demand for "AF Software Engineers." This reduction in demand for software engineers inversely leads to an amplified need for "Cybersecurity Experts" within the AF. The enhanced requirement for "Cybersecurity Experts" subsequently contributes to an escalation in total "AF IT Costs."

After mapping the significant portions of the relationships of key variables related to SBOMs within the DAF's software supply chain IT acquisition system, we could translate those variables from qualitative to quantitative in a model to try and measure the impact of a SBOM policy on the system.

B. SBOM SIMPLE SYSTEM DYNAMICS MODEL

A system dynamics model serves as a quantitative instrument, facilitating the simulation of SBOM policy implementation within the DAF in a controlled, virtual environment. As articulated by Sterman, "modeling is a disciplined, scientific, and rigorous process, challenging the modeler and client at every step to surface and test assumptions,

gather data, and revise their models – both formal and mental” (Sterman, 2000). One of the principal benefits of leveraging such models for policy decision-making lies in the ability to conduct tests within a virtual setting. This obviates the risk of real-world repercussions, thereby providing an optimal platform for the preliminary evaluation of policy initiatives.

System dynamics models are calculus-based mathematical representations of internal systems that generate problematic behavior (Sterman, 2000). These models incorporate stocks, which signify the accumulation or integration of measurable units, along with in-flows and out-flows, representing the rate or differentiation of accumulation (Sterman, 2000). Moreover, converters are employed to provide mathematical inputs to flow equations or for analysis (Sterman, 2000). In this case, that problematic behavior are cyberattacks on DAF systems. Our final model can be seen depicted in Figure 24.

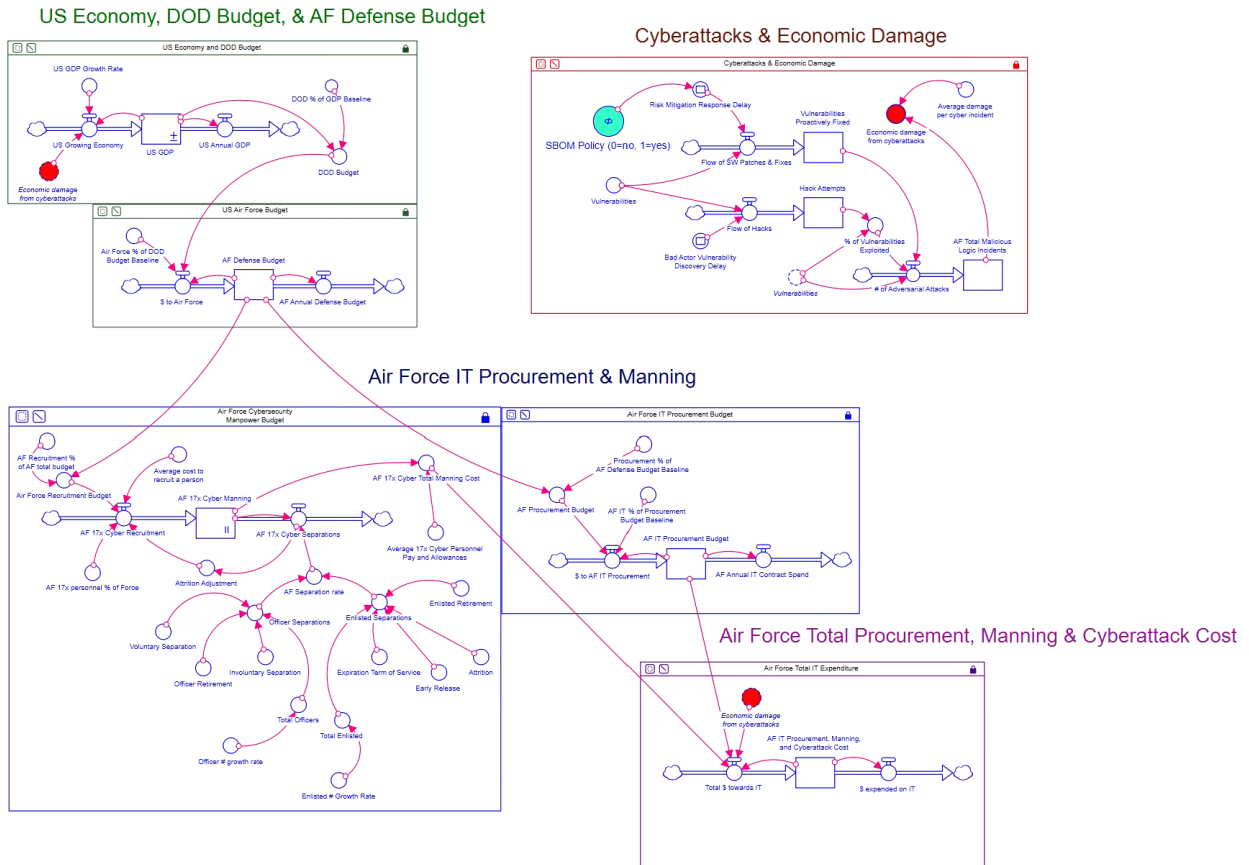


Figure 24. SBOM System Dynamics Model. Adapted from ISEE Systems (2023)

The first step in building our model included determining what components made up the total amount the DAF spends in the pursuit of IT and both preventing and reacting to cyberattacks. We determined the main components were the manning cost for cybersecurity specialists, Air Force Specialty Code (AFSC) 17X – Cybersecurity Operation Officers, the procurement IT contract costs, and the economic damages from successful cyberattacks. There were several decisions and assumptions that went into calculating and modeling these elements.

1. U.S. Economy and DOD Budget Model Section

To be able to show growth of the budgets to pay for these costs over ten years, we needed to model the U.S. Economy and Gross Domestic Product (GDP), Figure 25.

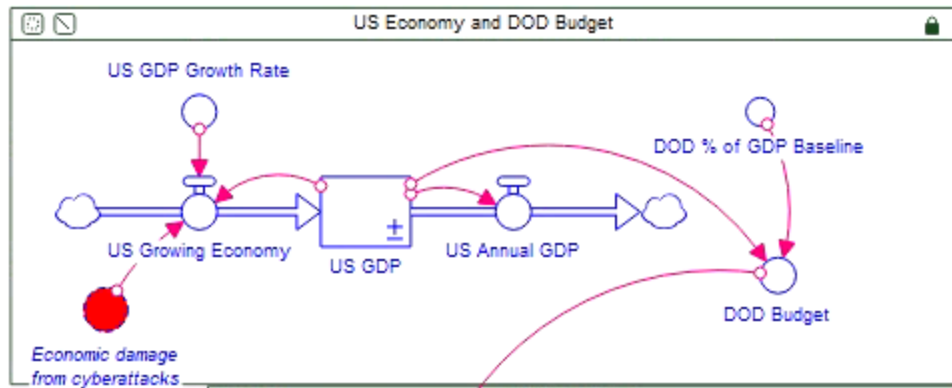


Figure 25. U.S. Economy and DOD Budget Model Section. Adapted from ISEE Systems (2023)

We started with data from 2020, where the U.S. GDP Growth Rate was 9.5%, significantly different from the projected annual growth rate of 1.7% from 2021–2030 (Congressional Budget Office, 2020). To effectively model the impacts on the U.S. economy, we needed to account for the annual growth rate and align it with the ten-year projections. Another crucial factor influencing the U.S. economy is economic damage from cyberattacks, specifically those targeting DAF IT systems. All these statistics directly affect the DOD budget. To build this section of the model we applied the assumptions and calculations seen in Table 3.

Table 3. U.S. Economy and DOD Budget Elements

ELEMENT	FORMULA	
Converter, U.S. GDP Growth Rate	'20 GDP growth rate smoothed down to predicted growth rate (Congressional Budget Office, 2020)	SMTHN(0.017, 3, 3, 0.09598488)
Converter, Economic damage from cyberattacks	Calculated from Cyberattacks & Economic Damage model sector	AF Total Malicious Logic Incidents*Average damage per cyber incident
Inflow, U.S. Growing Economy	Damage from federal cyberattacks affects U.S. GDP; therefore, included in calculation with annual growth rate	$US\ GDP * (1 + (US\ GDP\ Growth\ Rate)) - \text{Economic damage from cyberattacks}$

ELEMENT		FORMULA
Stock, U.S. GDP	'20 Q3 GDP (Mataloni & Aversa, 2021)	Initial Value "211,700,000,000"
Outflow, U.S. Annual GDP	Included for continual growth of the model	US GDP
Converter, DOD % of GDP Growth	('20 DOD Budget/'20 U.S. GDP) smoothed to average percentage (Peter G. Peterson Foundation, 2023)	SMTHN(0.028, 1, 1, 0.03489627)
DOD Budget	Calculated for context of later model sectors and to demonstrate expected growth of connected budgets	US GDP*DOD % of GDP Baseline

The primary goal of this section was to model the U.S. economic growth and establish a dependable calculation for the DOD budget. This serves as a foundation for the subsequent section, which delves into defining the Air Force budget in more detail.

2. AF Defense Budget Model Section

While the Department of Defense encompasses multiple military service branches, our research and model concentrate exclusively on the Air Force's segment. This requires us to dissect the Department of Defense budget to focus on the Air Force's specific allocation.

As illustrated in Figure 26, we initiated the model elements outlined in Table 4, by extrapolating data from the DOD budget.

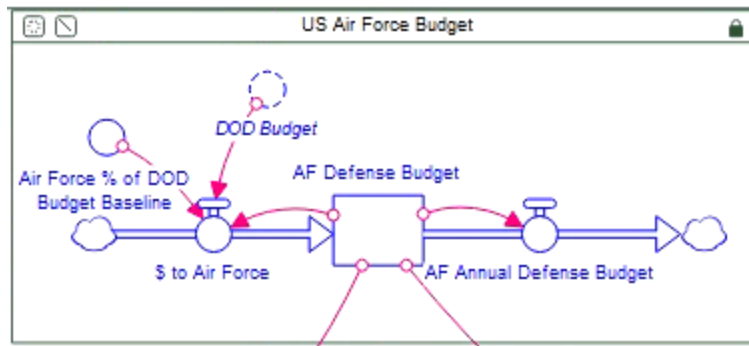


Figure 26. U.S. AF Budget Model Section Adapted from ISEE Systems (2023)

To ensure the utmost accuracy and reliability of our model, we used data spanning from 2020–2022, as documented in the references provided below. This detailed approach allowed us to quantify the financial parameters for the DAF.

Table 4. AF Defense Budget Elements

ELEMENT	DESCRIPTION	FORMULA
Converter, AF % of DOD Budget Baseline	‘20-’22 Total U.S. Air Force Enacted Budget per year (Department of the Air Force, 2022b)/Total Department of Defense Budget Authority per year (Department of Defense, 2021)	Initial Value “0.215”
Inflow, \$ to AF	Calculated as the annual designated dollar amount moved into AF accounts	$AF\ Defense\ Budget + ((DOD\ Budget * AF\ \% \ of\ DOD\ Budget\ Baseline) - AF\ Defense\ Budget)$
Stock, AF Defense Budget	‘20 Total U.S. Air Force Enacted Budget (Department of the Air Force, 2022b)	Initial Value “168,100,000,000”
Outflow, AF Annual Defense Budget	Calculated for the spending of the money in the AF budget	AF Defense Budget

Once we had an appropriately quantified DAF budget, we needed to continue to break it into the portions directly used to support the acquisition of commercial information technology and maintain cybersecurity career field manpower.

3. AF Cybersecurity Manpower Budget Model Section

In the analysis of DAF cybersecurity personnel economics, the complexity of factors influencing recruitment, retention, and attrition required a comprehensive approach, demonstrated in the number of converters seen in Figure 27 of the model.

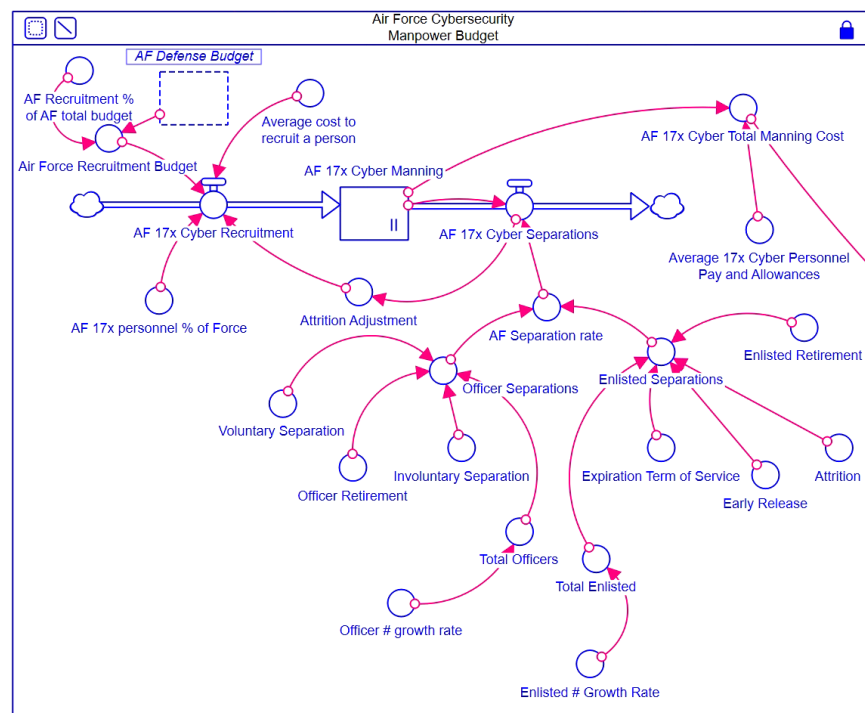


Figure 27. AF Cybersecurity Manpower Budget Section.
Adapted from ISEE Systems (2023)

We commenced by examining the Fiscal Year (FY) 2020 and 2022 Air Force Military Personnel Appropriation budgets, focusing on the recruitment allocation. To ascertain the cost-per-recruit, we developed a conversion ratio rooted in the percentage of the overall budget earmarked for recruitment activities, which can be seen in Table 5.

The flow of new cybersecurity personnel into the DAF was then calculated. This was achieved by dividing the recruitment budget by the average cost to onboard a single recruit, yielding the total influx of new personnel. To isolate the inflow specific to the cybersecurity field, we utilized data from GAO Report 23–105423, titled *Military Cyber Personnel – Opportunities Exist to Improve Service Obligation Guidance and Data*

Tracking (Farrell, 2022). According to this source, the AFSC 17X, pertaining to Cyberspace Operations Officers, was the most relevant for our investigation.

By applying the proportion of AFSC 17X personnel to the total incoming recruits, we isolated the inflow of cybersecurity-focused personnel, specifically those within the 17X category. For attrition rates, a weighted average was calculated based on the FY 2020 and 2022 attrition data for both officers and enlisted personnel, yielding an average attrition rate specific to the 17X specialty.

To quantify the economic impact, we multiplied the number of 17X personnel by their average salary, computed via a weighted average approach. This considered both the average salaries for officers and enlisted personnel, as well as their respective proportions within the 17X specialty. Subsequently, the aggregate economic burden of 17X personnel was determined by multiplying the total headcount by their average salary.

Table 5. AF Cybersecurity Manpower Budget Elements

ELEMENT	DESCRIPTION	FORMULA
Converter, AF Recruitment % of AF total budget	'20-'22 AF recruitment budget by year/AF defense budget by year (Department of the Air Force, 2021)	SMTHN(0.00047523, 2, 2, 0.00034847)
Converter, AF Recruitment Budget	A function of AF Defense Budget converter & AF Recruitment % of AF total budget converter	AF Defense Budget*AF Recruitment % of AF total budget
Converter, Average cost to recruit a person	'22 AF recruitment budget/'22 recruiting numeric goals	Initial Value "2,515.68"
Converter, AF 17X personnel % of Force	'21 reported number of 17X personnel/('21 Direct Program End Strength Enlisted+'21 Direct Program End Strength Officers)	Initial Value "0.027746"
Converter, Attrition Adjustment	A function of the AF 17X Cyber Separations outflow smoothed over 12 months	SMTH1(AF 17X Cyber Separations, 12)
Inflow, AF 17X Cyber Recruitment	A function of AF Recruitment Budget converter, Average cost to recruit a person converter, AF 17X personnel % of Force converter and attrition Adjustment converter	(AF Recruitment Budget/ 12)/Average cost to recruit a person*AF 17X personnel % of Force+Attrition Adjustment
Stock, AF 17X Cyber Manning	'21 reported number of 17X personnel (Farrell, 2022)	Initial Value "9,529"
Converter, Enlisted # Growth Rate	(('22 Direct Program End Strength Enlisted-'20 Direct Program End	Initial Value "0.00365726"

ELEMENT	DESCRIPTION	FORMULA
	Strength Enlisted)/2)/'20 Direct Program End Strength Enlisted	
Converter, Total Enlisted	'22 Direct Program End Strength Enlisted (Department of the Air Force, 2021)	$263,585 * (1 + \text{Enlisted \# Growth Rate})$
Converter, Expiration Term of Service	'22 ETS Losses Enlisted/'22 Direct Program End Strength Enlisted	Initial Value "0.03971968"
Converter, Early Release	'22 Programmed Early Release Losses Enlisted/'22 Direct Program End Strength Enlisted	Initial Value "0.00359067"
Converter, Attrition	'22 Attrition Losses Enlisted/'22 Direct Program End Strength Enlisted	Initial Value "0.02488979"
Converter, Enlisted Retirement	'22 Retirement Losses Enlisted/'22 Direct Program End Strength Enlisted	Initial Value "0.04330281"
Converter, Enlisted Separations	A function of total enlisted converter and the different enlisted separation rates	$(\text{Total Enlisted} * (\text{Expiration Term of Service} + \text{Early Release} + \text{Attrition} + \text{Enlisted Retirement})) / \text{Total Enlisted}$
Converter, Officer # growth rate	$((\text{'22 Direct Program End Strength Officers} - \text{'20 Direct Program End Strength Officers}) / 2) / \text{'20 Direct Program End Strength Officers}$	Initial Value "0.00816082"
Converter, Total Officers	'22 Direct Program End Strength Officers	$63,474 * (1 + \text{Officer \# growth rate})$
Converter, Voluntary Separation	'22 Voluntary Separation Losses Officers/'22 Direct Program End Strength Officers	Initial Value "0.02677104"
Converter, Officer Retirement	'22 Retirement Losses Officers/'22 Direct Program End Strength Officers	Initial Value "0.0346923"
Converter, Involuntary Separation	'22 Total Involuntary Losses Officers/'22 Direct Program End Strength Officers	Initial Value "0.00153465"
Converter, Officer Separations	A function of total officer converter and the different officer separation rates.	$(\text{Total Officers} * (\text{Voluntary Separation} + \text{Officer Retirement} + \text{Involuntary Separation})) / \text{Total Officers}$
Converter, AF Separation rate	A function of Officer separation rate converter and enlisted separation rate converter.	$\text{Officer Separations} + \text{Enlisted Separations}$
Outflow, AF 17X Cyber Separations	A function of AF 17X Cyber Manning stock and AF Separation rate converter.	$\text{AF 17X Cyber Manning} * \text{AF Separation rate}$
Converter, Average 17X Cyber Personnel Pay and Allowances	'21 Cyber 17X Spend/'21 17X Personnel (Farrell, 2022)	Initial Value "103,816.54"
Converter, AF 17X Cyber Total Manning Cost	A function of AF 17X Cyber Manning Stock and Average 17X Cyber Personnel Pay and Allowances converter.	$\text{AF 17X Cyber Manning} * \text{Average 17X Cyber Personnel Pay and Allowances}$

The ultimate result of the AF Cybersecurity Manpower Budget segment within our model is the overall expenditure associated with cybersecurity personnel within the DAF, expressed as a component of the total DAF expenditure allocated for information technology life cycles.

4. AF IT Procurement Budget Model Section

The Air Force IT Procurement Budget, Figure 28 is another critical aspect of our model. A specific allocation within the Air Force Defense Budget is designated for IT procurement, found under category one in the Air Force's category management strategy (AFICC/KA, 2023). This allocation plays a pivotal role in discerning the proportion of the total expenditure that the DAF allocated to IT contracts.

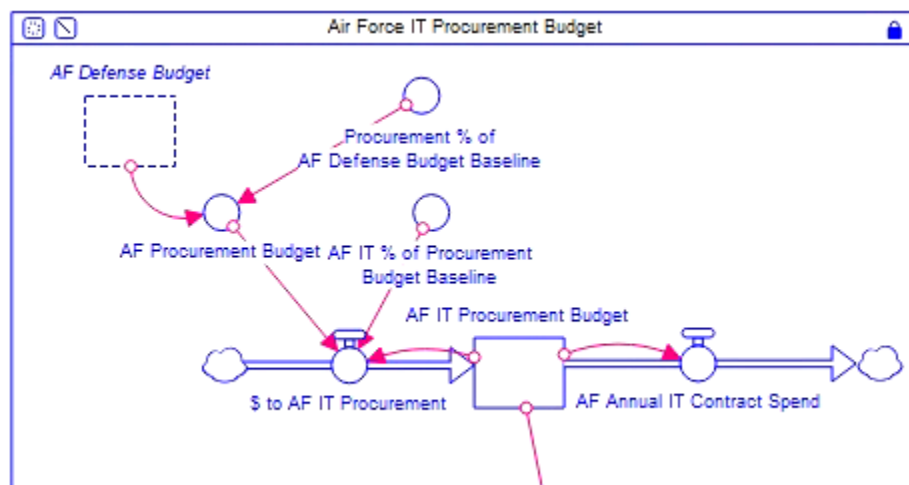


Figure 28. AF IT Procurement Budget Section. Adapted from ISEE Systems (2023)

For this calculation, we referred to the Air Force Business Intelligence Tool for Contract Spend data from FY22. We isolated the IT Category Total expenditure and divided it by the Total Contract Spend to identify the portion of the procurement budget allocated to IT contracts. Calculations from this data for our model can be seen in Table 6.

Table 6. AF IT Procurement Budget Elements

ELEMENT	DESCRIPTION	FORMULA
Converter, Procurement % of AF Defense Budget Baseline	Procurement spend was pulled from AFBIT. Percentage was calculated by dividing procurement spend over the AF Budget (AFICC/KA, 2023).	SMTHN(0.59, 1, 1, 0.534)
Converter, AF Procurement Budget	A function of AF Defense Budget converter and Procurement % of AF Defense Budget Baseline converter.	AF Defense Budget*Procurement % of AF Defense Budget Baseline
Converter, AF IT % of Procurement Budget Baseline	2022 IT Procurement spend was pulled from the AFBIT and divided by the AF Procurement budget to get a percentage.	Initial Value “0.084103636”
Inflow, \$ to AF IT Procurement	A function of AF IT Procurement Budget stock, AF Procurement Budget converter and AF IT % of Procurement Budget Baseline converter	AF IT Procurement Budget+((AF Procurement Budget*AF IT % of Procurement Budget Baseline)-AF IT Procurement Budget)
Stock, AF IT Procurement Budget	2020 IT Procurement spend was pulled from AFBIT and was used as the initial value.	Initial Value “8,353,661,383”
Outflow, AF Annual IT Contract Spend	The outflow is a simple function of the AF IT Procurement Budget.	AF IT Procurement Budget

In our model, cybersecurity personnel expenses and expenditures related to the procurement of DAF IT systems make up a substantial part of the overall cost of information technology systems for the DAF. However, these elements, while significant, are not the primary focus when assessing the validity of model objective. Our central objective is to understand how the adoption of a SBOM policy within the DAF impacts the frequency of successful cyberattacks and the resulting economic losses. The subsequent step in our modeling process involved the intricate task of depicting how SBOMs influence this system.

5. Cyberattacks and Economic Damage Model Section

Arguably the most critical sector in our analysis, the segment depicted in Figure 29, scrutinizes the incidence of cyberattacks and their corresponding economic ramifications, particularly in the context of how a SBOM policy might mitigate these costs.

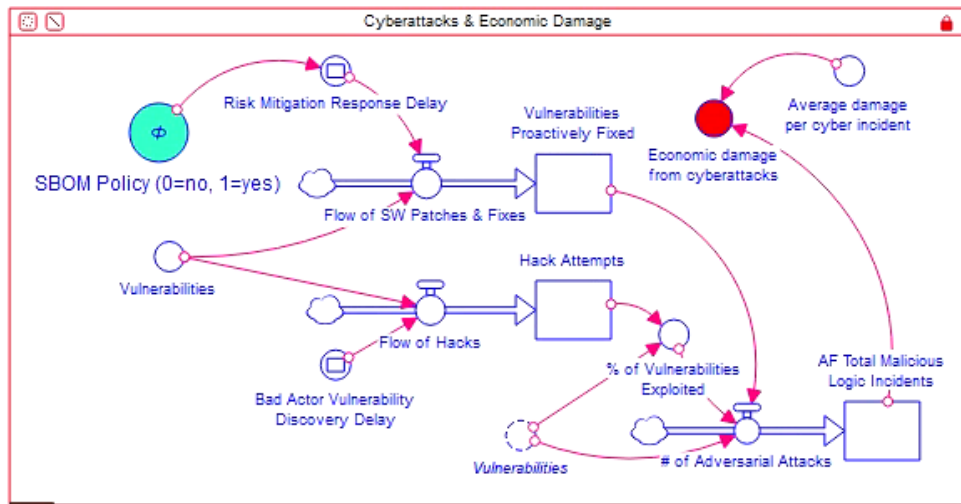


Figure 29. Cyberattacks and Economic Damage Model. Adapted from ISEE Systems (2023)

Our initial step involved assessing the frequency of vulnerabilities the DAF could expect in their information technology software. Based on the GAO Report 23–105084, the DOD encounters approximately 1,000 cyber incidents on an annual basis (Kirschbaum & Franks, 2022). To model this variability, we employed a stochastic function with a range of 900–1,100 to represent the likely volume of vulnerabilities confronting the DAF.

The first subsystem in our analysis focuses on the flow of software patches and the stock of proactively remedied vulnerabilities. The rate of patch deployment is influenced by the volume of vulnerabilities and a converter variable, termed “Risk Mitigation Response Delay.” Our research indicates a response time ranging from 14–60 days for a typical vulnerability. An SBOM policy activation switch was integrated into the model, which, when engaged, shortens the response delay to 1–7 days. This assertion is corroborated by NTIA, which posits that SBOMs expedite the identification and

remediation of vulnerabilities (NTIA, 2021b). Various case studies further substantiate that SBOM implementation can trim response time from weeks to mere minutes (LeanIX, n.d.).

The second subsystem entails the flow of cyberattacks and the accumulated stock of attempted hacks. We developed a converter variable to randomize the “Bad Actor Detection Delay,” based on a window of 1 to 30 days (Townsend, 2023). The flow of cyberattacks is contingent upon the identified vulnerabilities and the delay in bad actor detection. The accumulated cyberattack attempts subsequently feed into a converter that estimates the percentage of successful exploits, which is a function of both the number of vulnerabilities and accumulated hack attempts.

Both subsystems feed into a third subsystem that quantifies the financial impact. This subsystem computes the flow of actual attacks based on the number of identified vulnerabilities, the proportion of successful exploits, and the volume of proactively patched vulnerabilities. This resultant flow is then aggregated into a stock termed “AF Total Malicious Logic Incidents.” Citing the IBM 2023 report on the cost of a data breach, the average expense incurred by a large-scale corporate data breach in 2023 surpasses \$4 million (IBM, 2023). By multiplying the number of malicious logic incidents by this average cost, we derive the annual economic damage attributable to cyberattacks. All calculations that make up the cyberattacks and economic damage section of our model can be seen in Table 7.

Table 7. Cyberattacks and Economic Damage Elements

ELEMENT	DESCRIPTION	FORMULA
Converter, SBOM Policy (0=no, 1=yes)	This Converter acts like a switch. 0 means no SBOM policy and 1 means there is an SBOM policy	Initial value “0 or 1”
Delay Converter, Risk Mitigation Response Delay	This represents the time to respond to a SW vulnerability. This converter is a function of the SBOM policy switch converter. If there is a SBOM policy, the response delay is shorter than without a SBOM policy	IF (“SBOM Policy (0=no, 1=yes)” > 0)THEN RANDOM((1/365), (7/365)) ELSE RANDOM((14/365), (60/365))

ELEMENT	DESCRIPTION	FORMULA
Converter, Vulnerabilities	According to GAO the DOD experiences around 1K cyber incidents annually. We used a random function to simulate volatile numbers of vulnerabilities (Kirschbaum & Franks, 2022)	$\text{RANDOM}(900, 1100)$
Inflow, Flow of SW Patches & Fixes	This represents the flow of SW fixes based on a function how quickly good actors can respond to a vulnerability and the number of vulnerabilities in the wild	$(\text{Vulnerabilities}/\text{Risk Mitigation Response Delay})/\text{Vulnerabilities}$
Stock, Vulnerabilities Proactively Fixed	We used 0 as the initial value because we do not know the number of vulnerabilities fixed in 2020. This stock represents the number of vulnerabilities patched.	Initial Value “0”
Delay Converter, Bad Actor Vulnerability Discovery Delay	It can take between 1 and 30 days for a bad actor to find a vulnerability in the wild (Townsend, 2023)	$\text{RANDOM}((1/365), (30/365))$
Inflow, Flow of Hacks	This represents the flow of hacks based on a function of the number of vulnerabilities in the wild and how quickly bad actors can discover them	$(\text{Vulnerabilities}/\text{Bad Actor Vulnerability Discovery Delay})/\text{Vulnerabilities}$
Stock, Hack Attempts	We used 0 as the initial value because we do not know the number of hack attempts in 2020. This stock represents the number of hack attempts based on the inflow of hacks.	Initial Value “0”
Converter, % of Vulnerabilities Exploited	This represents the percentage of vulnerabilities exploited. This is a function of the number of hack attempts and the number of vulnerabilities in the wild.	$\text{Hack Attempts}/\text{Vulnerabilities}$
Inflow, # of Adversarial Attacks	This represents the flow of adversarial attacks based on the number of vulnerabilities exploited and the number of vulnerabilities fixed.	$(\text{Vulnerabilities}-\text{Vulnerabilities Proactively Fixed})^{**}\% \text{ of Vulnerabilities Exploited}^{**}$
Stock, AF Total Malicious Logic Incidents	We used 0 as the initial value because we do not know the number of incidents that AF experienced in 2020. This stock	Initial Value “0”

ELEMENT	DESCRIPTION	FORMULA
	accumulates the flow of adversarial attacks.	
Converter, Average damage per cyber incident	According to IBM, this is the average cost per cyber incident (IBM, 2023).	Initial Value “4,450,000”
Converter, Economic damage from cyber attacks	This represents the economic damage resulting from the number of total malicious logic attacks.	AF Total Malicious Logic Incidents*Average damage per cyber incident

This comprehensive model enables a nuanced understanding of the cyber risk landscape and offers empirical support for the potential efficacy of a SBOM policy in reducing both the frequency of cyberattacks and their consequent economic damage.

6. AF Total IT Expenditure Model Section

The concluding sector of our model serves as an integrative element, aggregating variables across manning, procurement, and cyber incident costs to furnish a comprehensive picture of the Air Force’s total IT expenditure, Figure 30.

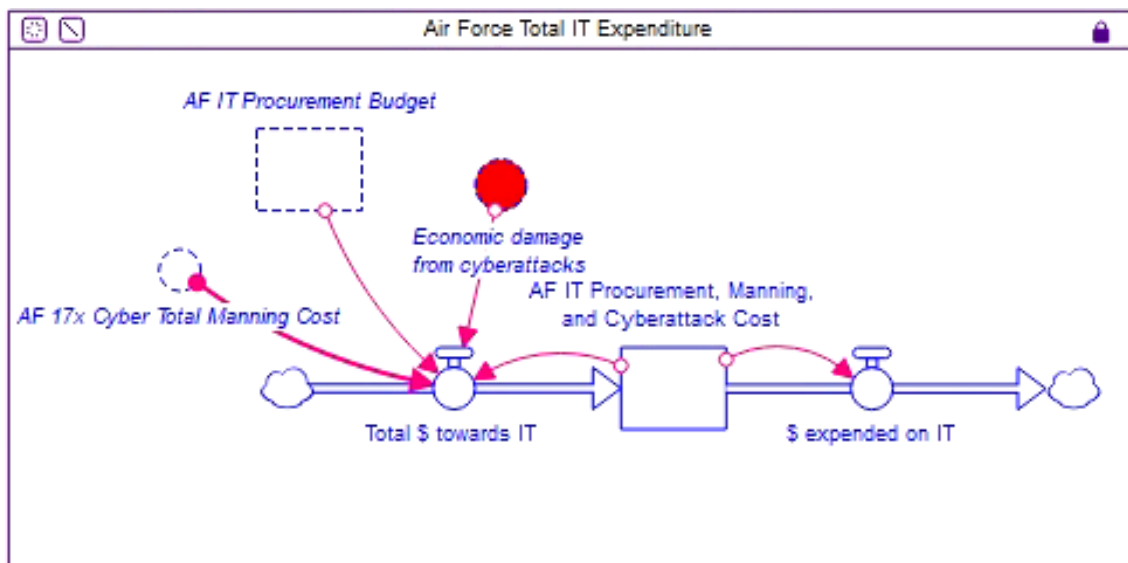


Figure 30. AF Total IT Expenditure Section. Adapted from ISEE Systems (2023)

The principal of this sector is to measure shifts in the percentage of DAF’s overall IT expenditure attributed to economic losses from cyberattacks, both with and without the implementation of a SBOM policy, calculations depicted in Table 8.

Table 8. AF Total IT Expenditure Elements

ELEMENT	DESCRIPTION	FORMULA
Inflow, Total \$ towards IT	This represents the total flow of money spent on IT in the AF from the manning, procurement and cyberattack sections of the model.	AF 17X Cyber Total Manning Cost + AF IT Procurement Budget + Economic damage from cyberattacks + “AF IT Procurement, Manning, and Cyberattack Cost”
Stock, AF IT Procurement, Manning, and Cyberattack Cost	This represents the accumulation of the total money spent on IT within the AF.	Initial Value “0”
Outflow, \$ expended on IT	This represents the outflow of the total AF IT cost.	“AF IT Procurement, Manning, and Cyberattack Cost”

By consolidating these costs, we derive a comprehensive metric—Total AF IT Expenditure—that enables us to assess the relative impact of each sector. Specifically, we evaluate how the economic damages emanating from cyber incidents contribute to this total expenditure under different policy scenarios.

7. Model Interface

Our user interface consists of two distinct pages. The first page, depicted in Figure 34, provides a comprehensive overview of the model’s outcomes when run under two scenarios: one with a SBOM policy implemented and another without it. This page enables users to quickly grasp the potential implications of adopting a SBOM policy and offers a summary of the model’s overall results.

On the second page, illustrated in Figure 31, users can access a graph that visualizes the annual number of cyberattacks in relation to the quantity of vulnerabilities proactively addressed, hack attempts, and the total count of malicious attacks on the DAF.

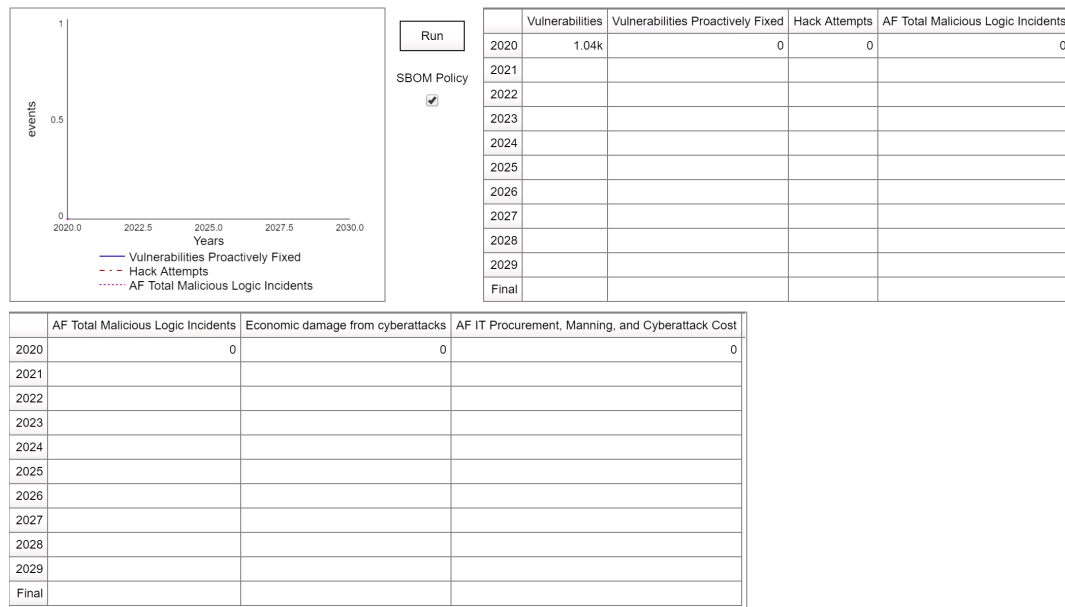


Figure 31. Software Bill of Material System Dynamics Model Interface.
Adapted from ISEE Systems (2023)

Additionally, this section of the interface includes two tables, each representing the results of a single model run. Users can toggle between the two scenarios, one with a SBOM policy and one without, using a switch. A “Run” button is also provided to initiate the model’s execution.

C. FINDINGS AND ANALYSIS

Upon the model’s completion, we conducted numerous iterations to ensure its accuracy and determine the meaningfulness of the results. These iterations equipped us with the essential information needed to ensure our calculations reflected actual data and provided meaningful outputs that we could use to assess the potential impact of a SBOM policy given our assumptions.

In our model, the economic damage caused by cyberattacks is deducted from the annual U.S. GDP. The growth in U.S. GDP and federal government budgets depicted over the ten-year model runtime aligns with the projections for U.S. GDP growth. This growth trend generally indicates the availability of more funds for various budgets (Congressional

Budget Office, 2020). Figure 32 presents the consistent outcomes of the initial two sectors within our model.

	US GDP Growth Rate	US GDP	DOD Budget	AF Defense Budget
2020	0.096	21.2T	739B	168B
2021	0.092	23.3T	702B	158B
2022	0.0706	25.3T	726B	154B
2023	0.0479	26.9T	759B	158B
2024	0.0326	28T	787B	163B
2025	0.0242	28.9T	809B	169B
2026	0.0201	29.5T	826B	174B
2027	0.0183	30.1T	842B	177B
2028	0.0175	30.6T	857B	181B
2029	0.0172	31.2T	872B	184B
Final	0.0171	31.7T	887B	188B

Figure 32. U.S. Economy, DOD Budget, AF Budget Sector Results. Adapted from ISEE Systems (2023)

To test our model's fit for the initial three years of its runtime, we initiated it with 2020 data for U.S. GDP, the Department of Defense budget, and the DAF defense budget. The reported U.S. GDP for 2021 was \$23.2 trillion (Mataloni & Aversa, 2021) and \$25.7 trillion in 2022 (Mataloni, 2023), and our model calculations closely mirror these figures. The DOD reported a total budget authority of \$714 billion for 2021 and \$728 billion for 2022 (Austin III, 2021). Our model's DOD budget estimates were only slightly lower, with a \$12 billion variance for 2021 and a \$2 billion variance for 2022. These variances suggest that the equations within the model are a good fit to the reference modes.

Unlike the notable fluctuations observed in the overall budgets of the DOD and DAF over the ten-year simulation, the AF Cybersecurity Procurement & Manpower Budget sectors exhibit relative stability, Figure 33. This stability can be attributed to consistent increases in the U.S. GDP and the corresponding budget allocations.

	AF Procurement Budget	AF IT Procurement Budget	AF 17x Cyber Manning	AF 17x Cyber Total Manning Cost
2020	89.8B	8.35B	9.26k	961M
2021	90.4B	7.86B	9.31k	966M
2022	90.3B	7.67B	9.36k	971M
2023	92.9B	7.68B	9.4k	976M
2024	96.4B	7.86B	9.44k	980M
2025	99.6B	8.12B	9.49k	985M
2026	102B	8.37B	9.53k	989M
2027	105B	8.6B	9.56k	993M
2028	107B	8.8B	9.6k	997M
2029	109B	8.97B	9.64k	1B
Final	111B	9.14B	9.67k	1B

Figure 33. AF Cybersecurity Procurement and Manpower Budget Sector Results. Adapted from ISEE Systems (2023)

The most notable cost fluctuations in our model are observed in the sectors associated with the SBOM policy. When the model is executed with and without an SBOM policy, the impact of such a policy becomes evident, as shown in Figure 34. The graphs illustrate the number of vulnerabilities proactively fixed, due to whether a SBOM policy is implemented or not, the number of hack attempts, and the number of AF total malicious logic incidents over a period of ten years. The gauges give an easily visualized total number of AF total malicious logic incidents for the tenth year.

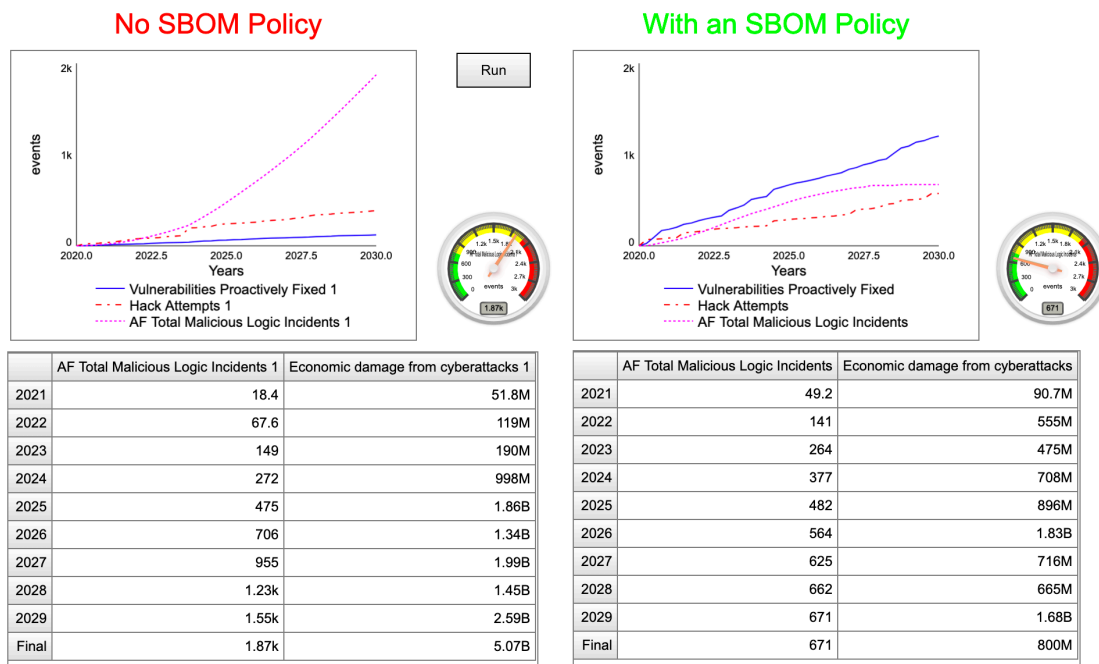


Figure 34. With and Without SBOM Policy Run Results. Adapted from ISEE Systems (2023)

In the absence of a policy that actively identifies software vulnerabilities and mitigates risk, there is a substantial increase in the number of successful malicious logic incidents (pink dotted line). We ran the model through 10 iterations, focusing on the variables, AF Total Malicious Logic Incidents and Economic Damage from Cyberattacks. Through those multiple iterations of the model, it was consistently evident that the number of AF Total Malicious Logic Incidents is higher without a SBOM policy than with one. This empirical evidence strongly supports the conclusion that the adoption of SBOMs can effectively reduce the frequency of successful cyberattacks.

As depicted in Figures 35 and 36, the implementation of SBOMs plays a pivotal role in mitigating the economic damage resulting from cyberattacks.

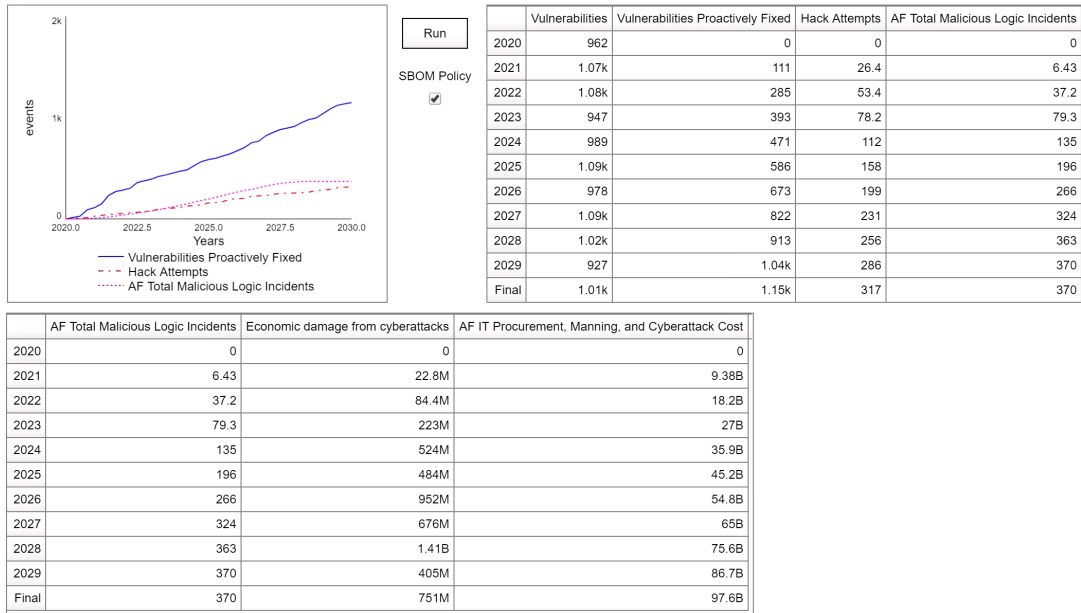


Figure 35. With SBOM Policy Run Results.
Adapted from ISEE Systems (2023)

This mitigation is achieved through a gradual and consistent increase in the identification and rectification of vulnerabilities over the years, as operational processes improve. Consequently, this proactive approach leads to a reduction in the number of successful cyberattacks, effectively curbing their economic impact versus what is seen without an SBOM policy in Figure 36.

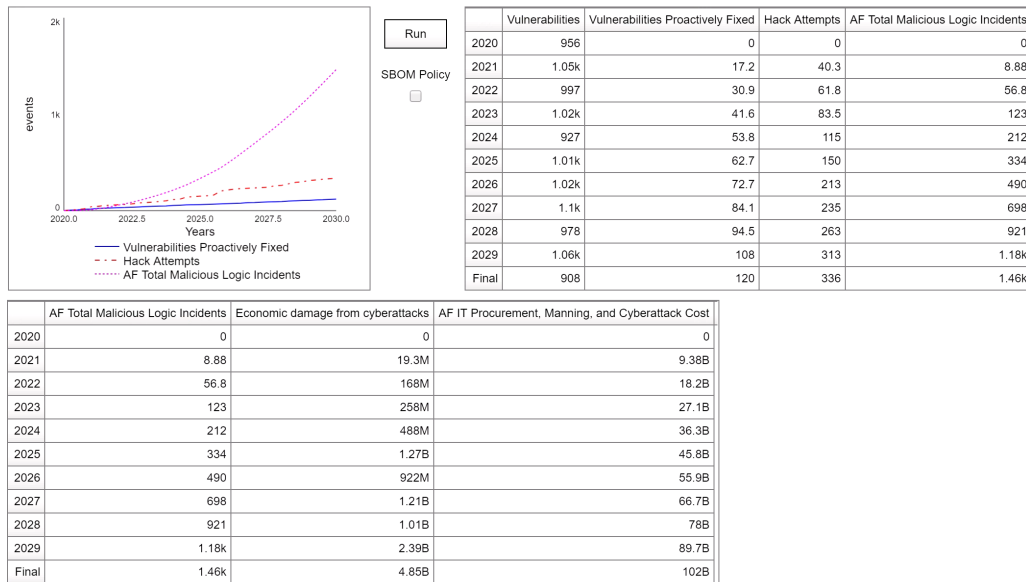


Figure 36. Without SBOM Policy Run Results.
Adapted from ISEE Systems (2023)

We assert that our calculations are conservative in nature, as they utilize global average costs per cyber incident. Given the sensitive nature of the information pertaining to U.S. national security interests, it is reasonable to assume that the actual costs of Air Force cyber incidents would likely be higher.

Upon analyzing the impact of an SBOM policy on the DAF's IT budget and the costs associated with cyberattacks, we have observed consistent and significant differences between scenarios with and without the policy, as illustrated in Figures 35 and 36. In the absence of an SBOM policy, the economic damage caused by malicious logic attacks constitutes approximately 5% of the total IT cost. However, with the implementation of an SBOM policy, the proportion of IT cost attributed to successful cyberattack damage is reduced to approximately 2%. Over a ten-year period, this 3% difference represents a significant financial advantage, the potential for approximately \$7 billion or more in savings, for the DAF.

While there may be slight variations due to random variables in the model, the consistent trend supports the validity of this analysis. As previously noted, our calculations are likely conservative, given that they are based on global average costs per cyber incident

which may be skewed below the median expected impact of a defense-related attack given the additional risks to national security. Consequently, the difference in the proportion of IT costs attributed to cyberattacks, with and without the implementation of an SBOM policy, could be even more substantial than our estimates suggest.

Based on the comprehensive analysis undertaken in this research, the adoption of a SBOM policy emerges as a strategically sound approach for the DAF in reducing both the frequency of successful cyberattacks and associated economic losses. The study employed a multi-faceted approach, incorporating both qualitative and quantitative research methodologies to substantiate the potential policy.

First, the CLD serves as a qualitative tool that elucidates the positive causative relationships between the implementation of an SBOM policy and enhanced visibility within the DAF's software supply chain. This increased transparency provides the necessary framework to heighten the accountability of contractors, thereby empowering the DAF to enforce more rigorous software risk mitigation measures. The likely result is a marked reduction in the frequency of successful cyberattacks affecting the DAF.

Secondly, our model offers quantitative substantiation for the adoption of an SBOM policy. The model indicates that the implementation of such a policy would expedite the software patching process. The direct consequence of this increased responsiveness is a corresponding decline in both the success rate of cyberattacks and the resultant economic impact on the DAF.

In summation, the evidence gathered and analyzed in this study collectively makes a compelling case for the initiation of an SBOM policy within the DAF. Such a policy would not only contribute to a more secure cyber environment but would also be economically prudent, thereby aligning well with the organization's broader strategic imperatives.

D. MODEL LIMITATIONS AND FUTURE RESEARCH

Our SBOM model, conducted within the constraints time and ongoing government exploration of SBOM nuances, provides valuable insights but has inherent limitations that

warrant further research. Notably, our model predominantly focuses on how implementing an SBOM policy could potentially reduce the frequency and economic impact of successful malicious logic attacks within the DAF. However, it is essential to acknowledge that our model does not encompass all the intricate factors and variations related to the actual implementation costs of such a policy. Understanding the financial implications of SBOM policy deployment within the DAF remains an important avenue for future research to address.

A critical aspect that our model does not incorporate involves the interplay between 17X personnel manning and the response time required to identify software vulnerabilities. Simultaneously, our analysis does not delve into how the volume of software vulnerabilities impacting the DAF affects the allocation and manning of 17X personnel. Investigating the dynamic relationship between these elements and the impact on cybersecurity is a promising area for further research.

In our causal loop diagram, we acknowledge the linkage between implementing an SBOM policy and the potential rise in SCRM workload and costs for contractors. However, our model does not quantitatively express this connection between the SBOM policy, DAF SCRM manning and associated costs, and the financial implications for contractors. This gap highlights the need for comprehensive research to explore the intricate relationships and evaluate the effects of SBOM policy adoption on these key aspects of DAF cybersecurity and procurement.

VIII. ROADMAP AND RECOMMENDATIONS FOR THE DOD

The utilization of SBOMs has demonstrated immense potential in fortifying software supply chains and managing risk to ensure the security of critical software ecosystems. However, SBOM implementation within the DOD would require an iterative and strategic roadmap with a set of well-informed, holistic, and actionable recommendations to be successful. This chapter discusses a comprehensive protocol for the utilization of SBOMs within the DOD, outlining key strategies and considerations through each stage of implementation. Each section focuses on a critical piece, including the education of internal stakeholders, fostering collaboration among diverse organizations and federal agencies, adopting and implementing best practices, developing a robust process framework for SBOM utilization and retention, and the creation of a SBOM standard tailored to the government's needs. Through these sections, we present a forward-thinking approach that not only acknowledges the challenges but also explores proactive solutions, ensuring that SBOMs become an integral piece of the DOD's cybersecurity arsenal.

A. EDUCATION OF INTERNAL STAKEHOLDERS

Elevating the understanding and awareness of SBOMs among internal stakeholders is a foundational step toward effective implementation. The idea of true supply chain risk management teams is just now starting to take shape within the DOD, making this an ideal time to inject SBOM education into that process. To ensure a seamless transition to the utilization of an SBOM management framework, internal stakeholders must become knowledgeable on SBOMs and the need for a more proactive approach. This step places heavy emphasis on the need for tailored training programs and knowledge dissemination initiatives to enable stakeholders to make critical decisions regarding cyber risk.

Throughout our H4D and capstone projects it became increasingly clear that the use and implementation of an SBOM management framework remains predominately nebulous among federal agencies. During the H4D project, our sponsors communicated the

difficulties surrounding compliance with Executive Order 14028 and believed compliance was deeply tied to the ability to evaluate risk associated with lower tier subcontractors. The EITaaS program managers were aware SBOMs could be a potential solution to increasing supply chain visibility but were unsure how the SBOM data would communicate levels of risk or signal a need for mitigation. Moreover, the DOD CIO office discussed how current guidance on implementation of SBOM usage is severely limited and hinders efforts to comply with the Executive Order.

As such, our team recommends stakeholder education on software risks, SBOMs and their use cases to be paramount for a proactive workforce. Software risk managers should take the lead on the development of education initiatives, developing these initiatives internally, or with the aid of leaders in the software risk management industry. Training and information dissemination should also be tailored to the individual impacts of each stakeholder. Supply chain risk management teams may need the most training and most up to date information regarding known vulnerabilities, malicious activity, and the current SBOM protocols, but training and sharing of general information on malicious activity should be disseminated even to the lowest level to empower users to become more vigilant regarding cybersecurity and alert proper channels when suspicious activity surfaces.

Education and training should encompass three overarching objectives for software risk managers. Objective one: Understand the anatomy of an SBOM. This objective creates a general understanding of SBOMs, the different formats, and the data they contain, facilitating SBOM literacy. The goal of this objective is the ability to break down an SBOM and understand its individual elements and the relationships between its different components. Objective two: Identify and map software risks. A key component of SBOM utilization is understanding how these software artifacts can reveal vulnerabilities and how those vulnerabilities are tied to specific risk categories. This competency enables risk managers to make appropriate determinations to manage and mitigate risk. Objective three: Establish risk scoring and mitigation strategies. In order for risk managers to make decisions on risk, they must understand how risks are scored based on organization-specific

risk scoring practices. This competency must include the risk mitigation procedures and strategies based on the severity and criticality of the risk.

By empowering DOD personnel through education and knowledge dissemination initiatives focused on in-depth insights into SBOMs' significance and usage, a culture of cybersecurity consciousness can be nurtured, laying a solid foundation for SBOM integration into existing processes.

B. COLLABORATION AMONG STAKEHOLDERS

Collaboration stands as possibly the most essential piece for successful SBOM implementation and utilization. During the course of this project, our team has discussed software development processes, software supply chains, software risk management, the current state of SBOM usage and how to comply with Executive Order 14028 with a variety of different organizations including numerous federal agencies and experts in SBOM management. Each of these discussions was critical to our understanding of the software risk landscape and how to cultivate a way forward to address emerging software threats. Without these deliberate collaborative efforts, our team would be unable to fathom the depth and complexity of this wicked problem or how it could potentially be solved.

For SBOM implementation within the DAF, our team recommends collaboration among key stakeholders such as the EITaaS Program Office, the 309 Software Engineering Group, NIST, CISA, the DAF CIO as well as the DOD CIO to cultivate working groups focused on compliance with Executive Order 14028 and to create a proactive approach to address vulnerabilities in software. Current efforts toward SBOM utilization between these organizations are largely fragmented and focused on different initiatives at varying stages to achieve the same goal. Although our team has attempted to streamline efforts and create cross-functional working groups, initiatives still appear to be disjointed among the different agencies. Collaboration among these stakeholders to establish SBOM management processes would facilitate and unify efforts to create a standardized and robust framework that all federal agencies can adopt and utilize (NTIA, 2021b, p. 4).

More specifically, our team recommends collaboration between the EITaaS program, the DAF CIO and the DOD CIO on a pilot program to experiment with SBOM

management processes and demystify the significance of SBOMs in mitigating software risk. This experimentation should also include processes for obtaining data from contractors to generate SBOMs internally or designating a specific format and process for contractors to deliver SBOMs to government agencies upon request. The pilot should also include exploration of supply chain illumination, identification of vulnerabilities and risk management and mitigation procedures through SBOM utilization.

The results of this pilot would provide invaluable insights into how to address this complex problem. These insights could potentially inform policies across the DOD for software risk management processes and inform how to strengthen cybersecurity of software overall. The pilot program offers a real-world testing ground to inform key aspects of risk management. By assessing SBOM content, it empowers risk managers to make informed decisions for risk mitigation. Furthermore, insights derived from the pilot are essential for determining what information is the most impactful in mitigating risk and should be included in the SBOM format. This, in turn, shapes the structure of SBOMs within the risk management framework, focusing on actionable data and alignment with DOD risk categories.

Practical implementation of SBOM requirements is another essential focus of the pilot. The pilot program will explore how industry can provide SBOMs efficiently, preferred formats, and the associated costs. Furthermore, the pilot helps determine the frequency of SBOM updates. These insights ensure that SBOMs remain current and effective in mitigating cybersecurity risks. Effective communication of risk data is vital in the cybersecurity landscape. The pilot program collaborates with program managers to identify the most meaningful visualizations for SBOMs and software risk information. Additionally, it contributes to defining acceptable risk levels within the realm of software supply chain vulnerabilities. These insights, drawn from real-world experiences and industry practices, set the stage for robust cybersecurity policies and standards that align with the DOD's objectives. In essence, the pilot program is an invaluable tool for data-driven risk management, practical implementation, effective communication, and policy development within the DOD's cybersecurity strategy.

By promoting open channels of communication, shared learning outcomes, and cross-functional collaboration, the DOD can harness the collective intelligence of its workforce, ensuring a unified approach toward SBOM integration across various departments and projects.

C. COLLECTION, ADOPTION AND IMPLEMENTATION OF BEST PRACTICES

Although interest in the utilization of SBOMs has grown significantly in recent years, SBOMs have been implemented as a solution to address software risk for over a decade (Muro, 2022, p. 101). By drawing from standard practices in industry and successful modalities, supply chain risk managers can create a pragmatic approach to SBOM collection and implementation of SBOM management processes. This approach can encompass the entire SBOM life cycle, from creation to continuous monitoring, identification of vulnerabilities, and the mitigation of risks for efficient and standardized implementation, while also addressing potential challenges and bottlenecks. Best practices serve as guiding principles in the utilization of SBOMs; the collection and adoption of these practices within the DOD would initiate proactive efforts, ease implementation, and allow for risk mitigation to occur in tandem with refinement of the risk management framework.

For example, the DOD's adoption of existing SBOM standards advocated by NIST and CISA would enable the collection of SBOMs in commonly used formats from contractors and allow risk managers to analyze the data for vulnerabilities and gain key insights into their software supply chains. Adoption of common risk scoring practices like the Common Vulnerability Scoring System and tailoring these practices to DOD-specific needs would create an easily digestible picture of software risk levels with minimal effort. Furthermore, adopting a universally recognized risk scoring framework enables the DOD to effectively assess the criticality of vulnerabilities and minimize duplicative efforts and government-unique costs that may serve as barriers to entry into government markets by non-traditional defense firms. Adoption of these common practices would ensure efficiency and enable risk mitigation within the DOD to begin much more quickly than attempting to create software risk management processes without direction.

The implementation of standard practices also requires engagement with leaders in software risk management in industry to either enlist, adopt, or tailor existing capabilities to mitigate software risk near term. To enlist the expertise of industry, the DOD should leverage contractors with competence in software risk management, utilizing their capabilities to the full extent while developing internal software risk management competencies. Engagement with industry also fosters collaborative partnerships that bridge gaps and enhance the defense sector's resilience against evolving supply chain threats.

During both H4D and our innovation capstone, our team engaged with numerous vendors in the software risk management industry that have exhibited a robust understanding of how to identify, manage, visualize, and mitigate risk. However, the DOD should not solely rely on external software risk management frameworks long term, as the DOD is concerned with risks that likely do not fully align or differ greatly from the focus of industry, as discussed in previous sections. The DOD should seek feedback from stakeholders in industry and learn from their expertise but should not purchase their services and accept them as an all-encompassing solution to the problem. Furthermore, the quality and effectiveness of risk management services provided by contractors may be difficult to discern without internal competencies in software risk management.

D. DEVELOP A SOFTWARE RISK MANAGEMENT FRAMEWORK

A robust software risk management framework is essential to translate theoretical knowledge into actionable outcomes. Although risk management frameworks are utilized throughout the DOD to address different types of risk, such as those associated with hardware, a framework specific to the management of software-related risks would illuminate exploitable vulnerabilities that are not currently identified, managed, or mitigated within the DOD. This framework should include the meticulous creation of processes for SBOM utilization within the DOD, encompassing phases from SBOM generation and vulnerability scanning to risk identification, assessment, mitigation, and continuous monitoring. By systematically defining these processes, the DOD can establish clear protocols, ensuring consistency, accuracy, and repeatability of processes in SBOM

usage, while also allowing for adaptability to the rapidly evolving software risk environment.

These processes can be enhanced utilizing dashboard modalities to provide intuitive visual representations of the vulnerability landscape, enabling swift identification of vulnerabilities and their corresponding levels of severity. This type of data visualization also facilitates rapid-decision-making in response to emerging cyber threats. Through visual analytics, stakeholders can quickly pinpoint areas within the software supply chain that demand immediate attention, allowing for swift mitigation and proactive risk management.

E. CREATION OF AN INCLUSIVE SBOM STANDARD

Although software risk managers in the private sector utilize common SBOM formats to achieve seamless integration and continuity, we recommend the DOD create an adaptation of a common SBOM format tailored to consider government-specific needs. By adapting a standardized SBOM format, the DOD gains the ability to tailor and include parameters that align with its risk taxonomy and strategic needs without creating excessive friction for commercial solutions. The tailoring of this SBOM format must be a collaborative effort between the DOD and leaders in the SBOM management industry to eliminate the threat of stifling innovation and creating barriers to entry for leading software developers. By fostering this collaborative effort, the DOD not only protects its own interests but also contributes to a more robust and secure cybersecurity landscape for both the government and industry.

This approach mirrors the insights shared in the article “Uncle Sam Rising,” emphasizing the importance of not hindering industry innovation and collaboration by creating unnecessary barriers (Josephson et al., 2018). The DOD landscape encompasses rapid response scenarios, contingency environments, classified information, and diverse operational needs. The DOD’s unique needs demand a standard that not only satisfies the government’s requirements and ensures compliance but also fosters unfettered collaboration with industry. Drawing inspiration from industry practices, the DOD can shape a standard that is both compliant and agile. This approach not only aligns with

government objectives but also ensures that the DOD remains at the forefront of innovation. This adaptive SBOM standard would be a catalyst for streamlined software risk management processes. It enables mission partners, contractors, and other federal agencies to integrate their software data efficiently, enhancing visibility across the supply chain without increasing friction. By striking this balance, the DOD can guarantee its cybersecurity requirements are met while fostering an environment where industry partners are encouraged, rather than deterred, to engage with government efforts.

IX. LIMITATIONS AND FUTURE RESEARCH

This section discusses areas of our research that revealed a need for further exploration within the DOD's software risk management landscape. These unexplored aspects hold the potential to enhance the DOD's understanding of the software supply chain and software risk management strategies. In conjunction with the limitations of our SBOM policy system dynamics model in section VII, we have identified several lines of effort we believe are necessary for SBOMs to be a successful tool for software SCRM and closing the gap in our nation's cybersecurity.

A. INFORMATION DISSEMINATION AND SBOM TRAINING PROGRAMS

During our research it was apparent that there is a dire need for knowledge dissemination initiatives and carefully curated SBOM training programs within the DOD. This requirement stems from the complex nature of software supply chains and the multifaceted challenges posed by software vulnerabilities and malicious actors. An effective training program should introduce the intricacies of software supply chains and the fundamentals of SBOMs, equipping the risk management workforce with a general understanding of the software risk landscape.

While we recognized the significance of these initiatives, our exploration revealed limitations in our research – the absence of a detailed framework for implementation. To bridge this gap, further research is required to develop a holistic approach to the education of risk managers and other stakeholders. This approach should encompass not only the foundational aspects of SBOMs and software supply chains but also explore the complexities of supply chain illumination, varied types of software risks, potential threats, methods of exploitation employed by malicious actors, and real-world case studies illustrating identification, mitigation, and monitoring of risks. Training programs should also include exploration of risk assessment techniques and data visualization strategies which would empower DOD personnel to innovate efficient ways to manage software risk.

In essence, the creation and implementation of information dissemination processes and SBOM training programs represent a critical area that requires further research. This

comprehensive approach is essential to elevating the competency of DOD's risk management workforce, ensuring they are well-equipped to navigate the complex and ever-evolving landscape of software risk.

B. SBOM RETENTION AND REPOSITORY PROCEDURES

The current state of the DOD's software risk management practices requires further investigation into the development of SBOM retention procedures. Our research revealed a notable absence of a comprehensive strategy for SBOM retention within the DOD. This deficiency underscores the need for in-depth exploration of the complexities related to SBOM storage. Critical questions remain unanswered: Where should SBOMs be securely stored to ensure maximum security? Who should maintain them? How frequently should they be updated to mirror the dynamic software landscape? Can updates be automated to enhance efficiency? Should multiple repositories be considered, each with varying levels of restriction?

Managing software supply chain risk entails more than mere data collection; it also includes the careful planning and implementation of secure retention protocols. Once SBOMs are acquired, their secure storage is critical to prevent the exploitation of sensitive data. SBOM repositories can rapidly become prime targets for malicious actors, escalating cybersecurity concerns. While a central repository might seem convenient, consolidating this data creates a potential gold mine for sensitive information, rendering it more vulnerable. To mitigate this risk, it becomes imperative to establish a secure repository with robust encryption protocols and stringent access controls.

The NTIA (2023) emphasizes that, despite concerns about potential misuse of SBOMs by malicious actors, the defensive benefits of supply chain transparency outweigh these risks. SBOMs illuminate the supply chain, assisting risk managers in identifying vulnerabilities within software components. These artifacts level the asymmetrical advantage by providing standardized, machine-readable decision support, thus fortifying cybersecurity defenses (NTIA, 2023).

Creation of secure SBOM repositories requires active management, meticulous cataloging, and update protocols. SBOMs age quickly and require regular regeneration with new software updates. The development of a secure SBOM repository may involve distributing stored SBOMs across multiple locations based on data type and sensitivity. Alternatively, a jointly managed repository by the federal government and contractors may share liability and reduce risk but increase vulnerability to cyberattacks.

The implications of these inquiries are profound. Restrictive access protocols ensure that sensitive information remains in the hands of authorized personnel, mitigating the risk of malicious exploitation. Automated updates, if feasible, enable real-time risk assessment, enhancing the DOD's agility in responding to emerging threats. However, striking the right balance between security and accessibility is crucial, as excessively restrictive measures could hinder timely information dissemination, impacting the DOD's ability to effectively counter threats.

C. SBOM FORMAT DEVELOPMENT

The intricate process of SBOM format development within the DOD is not only a technical challenge but a delicate balance between specificity and inclusivity. Our research illuminated a significant aspect: the format's creation demands a collaborative effort that transcends government stakeholders alone. By acknowledging the pivotal role of contractors in the DOD's ecosystem, we recognize that an overly restrictive or excessively DOD-specific SBOM standard could inadvertently hinder contractor-government interactions. This challenge highlights the importance of not alienating contractors with overly stringent standards.

Our research took the initial step toward an inclusive and adaptable SBOM format. It is imperative to learn from past missteps and ensure that the development process involves a wide array of voices, including experts in industry and contractors that will likely be impacted by the SBOM requirements. This collaborative approach not only ensures that the government's needs are met but also fosters an environment where contractors feel encouraged and supported to provide their services and expertise to the government.

Further research is required to address how a government format can strike a balance between specificity for DOD needs and inclusivity for contractors, what elements are rigid and necessary for national security, and where flexibility can be introduced. How can the format encourage, rather than hinder, collaboration between government entities and contractors? These inquiries necessitate further exploration, drawing upon insights from diverse stakeholders. The ultimate goal is not just the creation of a standard but the cultivation of an environment where government-contractor collaboration thrives.

D. ADVANCEMENT OF DASHBOARDING CAPABILITIES

During our research, we successfully developed a prototype for a software risk management dashboard, a testament to the ability to create software risk management tools internally. This prototype, although rudimentary, showcased the feasibility of scanning SBOMs and distilling complex data into easily understandable information, thereby identifying known vulnerabilities quickly and effectively. However, our prototype only scratched the surface of what is possible.

The advancement of dashboarding capabilities represents a compelling area for future research and innovation within the DOD. While our AI-driven prototype demonstrated the concept's viability, internal DOD entities possess an untapped wealth of expertise in software development and program management. Leveraging these internal capabilities could lead to the creation of sophisticated, SBOM scanning and monitoring systems specifically designed for the DOD's unique software landscape.

This area for further research is not just an option; it is a strategic imperative. By investing in the development of internal SBOM scanning and monitoring tools, the DOD can achieve several critical objectives. First, internal solutions can be finely tuned to meet DOD's specific requirements and security standards, ensuring a precise fit for the organization's needs. Second, fostering internal capabilities cultivates a culture of innovation and autonomy, enabling the DOD to stay ahead in the ever-evolving landscape of cyber threats. Third, with a robust internal system, the DOD can exercise a higher degree of control and customization, enabling swift, real-time responses to emerging vulnerabilities and threats.

This internal development approach aligns with broader national security imperatives. By reducing reliance on external entities and proprietary software, the DOD enhances its resilience against supply chain disruptions and potential vulnerabilities introduced through third-party solutions.

E. OPTIMIZATION OF DATA VISUALIZATION

Throughout our research, we were constantly reminded of the criticality and intricacy of optimization of data visualization. While the importance of visualizing SBOM vulnerabilities and software visibility levels was evident, our exploration revealed our limitations of translating raw SBOM data into actionable insights. Despite our extensive research, determining the most effective data visualizations for the DOD remained an elusive goal.

This challenge signifies a compelling area for continued research, demanding further exploration and innovation. The need for optimized data visualization cannot be overstated; it acts as the bridge between raw data and informed decision-making. The efficacy of software risk management processes hinges not only on the ability to collect data but also on their capacity to transform this data into clear, strategic visualizations. Visualization optimization is not just an augmentation to the dashboard; it is a fundamental component that enables proactive risk management decision-making.

Optimization of data visualization is foundational for proactive software risk management. It represents the difference between data overload and strategic clarity. By continuing this research, the DOD and its software developers can develop innovative ways to distill complexity, ensuring that SBOM data translates into actionable intelligence, fortifying the DOD against the intricate challenges of software risks.

THIS PAGE INTENTIONALLY LEFT BLANK

X. CONCLUSION

In the labyrinthine realm of cybersecurity, where threats to the United States' national security, economic stability, and technological infrastructure continue to mount, the significance of a resilient cyber supply chain cannot be understated. Through the chapters of this thesis, we have systematically unfolded the complexities of these challenges, validated the concerns, and proposed tangible solutions grounded in research and practicality.

The foundational tenets of this study, laid out in Chapter 1, were the distressing incidents that shook our nation's cyber landscape. Such incidents underscored the need for strategic efforts in bolstering defenses, particularly in the context of the EITaaS Program Office. Chapters 2 and 3 introduced us to the myriad stakeholders and methodological approaches, emphasizing that while there are numerous entities making commendable efforts, a lack of unified strategy often results in fragmented outcomes.

Our H4D project and subsequent explorations, as delineated in Chapters 4 and 5, yielded a validated problem statement and provided deep insights into the very fabric of SBOMs. Recognizing the gaps in the EITaaS SCRM team's capabilities, we proposed pivotal solutions, echoing the NTIA's recommendations and mapping vulnerabilities tailored to the DOD's operational context. These endeavors were further solidified by our SBOM Dashboard prototype, which, as Chapter 6 describes, not only clarified SBOMs for the EITaaS Program Office but also paved the way for a structured, hands-on approach to risk management.

In Chapter 7, our systems dynamic research substantiated the urgent need and efficacy of an SBOM policy within the DAF. Through qualitative and quantitative methodologies, we've showcased that the road to a more secure cyber environment is achievable, economically sensible, and strategically aligned with the organization's larger objectives. Lastly, Chapter 8 delivered actionable recommendations, providing the DOD with a roadmap that ensures SBOMs aren't just a theoretical concept but a practical tool embedded within the DOD's cybersecurity strategies.

In conclusion, the journey of this thesis, much like the cyber landscape, was intricate, challenging, and enlightening. We believe that the insights, solutions, and recommendations presented serve as an invaluable compass for the EITaaS Program Office and, more broadly, for the DOD, guiding them towards a safer, more resilient cyber frontier.

APPENDIX. H4D MISSION MODEL CANVAS

The Mission Model Canvas

Software Supply Chain Visibility
Mission/Problem Description:

Sentries of the Software Supply Chain
Designed by:

12, Oct 2023
Date:

10
Version:

Key Partners 1. Software Stakeholders: 1a. Software Providers: Companies producing the software being analyzed. 1b. Software Repositories: Storage systems for software and components. 1c. Software Supply Chain & SBOM Experts: Professionals versed in software distribution and SBOM specifics. 2. GOV Bodies & Personnel 2a. GOV Intelligence & Cybersecurity: Entities and specialists providing cybersecurity intelligence and expertise. 2b. DOD Chief Information Office, CISA, NTIA: Key U.S. agencies overseeing IT, cybersecurity, and telecom infrastructure. 2c. Other Relevant Federal Agencies: U.S. agencies using, regulating, or interested in the software. 3. Industry Cybersecurity Personnel: Non-government experts offering industry-specific cybersecurity insight. 4. Vulnerability Databases: National Vulnerability Database (NVD): U.S. repository for vulnerability data, essential for software risk assessments.	Key Activities 1. EITaaS SBOM Pilot Program: Launch to gain insights & improve SBOM procedures. 2. Inter-Agency and Industry Collaboration: Teamwork between GOV entities & the private sector. 3. Supply Chain Risk Information Exchange: Facilitating a two-way flow of software supply chain risks between GOV and industry. 4. SBOM Policy Research: Investigating the practicality, benefits, and challenges of establishing a SBOM policy Key Resources 1. Physical: SBOM Repository & Secure Data Center: Central storage and protection for SBOM data. 2. Financial: Pilot & Contract Funding: Budgets for the pilot program and additional contract needs. 3. Human: SBOM Experts & Developers: Personnel specialized in SBOM and SW development. 4. GOV: SBOM Contractor Policy: Mandate for contractors to submit SBOMs. 5. Intellectual: Training: SBOM best practices and visualization tools.	Value Propositions 1. Enhanced SW Security & Reliability. 1a. Bolster software security for 800,000 IT users AF Wide across all career fields, raising the standard of digital tools in use. 1b. Elevate the quality assurance for Software Providers, promoting better software products. 2. Improved Supply Chain Visibility: 2a. Equip EITaaS with insights into their supply chain, reducing risk and potential service interruptions. 2b. Strengthen collaboration between government and industry, synergizing efforts to secure the software supply chain. 3. Data-Driven Decision Making: 3a. Grant AFLCMC leadership and PEOs confidence through data, ensuring software projects meet security standards. 3b. Offer Cyber SC Risk Managers advanced tools and intel, enhancing their operational efficacy. 4. Accountability & Oversight: 4a. Establish clear criteria for COs to ensure contractors uphold software supply chain standards. 4b. Provide a concrete system for evaluating and ensuring the integrity of purchased software.	Buy-in & Support 1. AFLCMC: Backing the EITaaS SBOM pilot initiative. 2. EITaaS Program: Spearheading the SBOM pilot's actual implementation. 3. DOD CIO: Endorsing the pilot. 1d. Congress: Enacting legislation for contractor SBOM submission. 4. U.S. President: Issuing an EO for federal SBOM data collection and analysis. 5. Ongoing Support: Cybersecurity SC Risk Management: Overseeing and facilitating the pilot's execution. Deployment 1. Scaling from MVP: 1a. Incorporate feedback and lessons from MVP stages to shape a robust SBOM pilot program. 1b. Adopt an iterative approach, continuously refining the pilot based on ongoing insights. 2. Success Metrics: 2a. Achieving a comprehensive understanding of SBOM policy's impact. 2b. Garnering substantial data validating the policy's effectiveness and efficiency.	Beneficiaries 1. Internal Beneficiaries: 1a. 800,000 IT users AF wide: Seeking reliable and secure software tools for their diverse tasks. 1b. EITaaS Program: Aiming to implement a robust software supply chain management system for better program outcomes 1c. AFLCMC Leadership: Desiring a transparent and efficient software supply chain. 1d. Cyber Program Executive Officers: Needing clarity and assurance on software sourcing and integrity. 1e. Cyber Supply Chain Risk Managers: Pursuing enhanced risk assessment capabilities. 1f. Cyber Contracting Officers: Requiring clearer guidelines and enforcement mechanisms for software contracts. 2. External Beneficiaries: 2a. Software Providers: Looking for guidance and standards to improve the security and reliability of their offerings.
Mission Budget/Cost 1. Cost Structure: 1a. Setup: SBOM infrastructure & initial software. 1b. Operation: Maintenance, updates, and training. 1c. Improvement: Iterative refinements & feedback analysis. 1d. Advocacy: Policy lobbying & government engagement. 2. Cost Drivers: 2a. Infrastructure: Setup and upkeep. 2b. Personnel: Specialized roles & training. 2c. Development: Ongoing software refinement. 3. Financial Timeline: Start = High initial outlay. Iterative = Periodic feedback-driven costs.		Mission Achievement/Impact Factors 1. IT Users (800,000 AF wide): 1a. Metric: Change in software security breaches and reliability incidents post-SBOM policy. 2. EITaaS Program: 2a. Metric: Reduction in software risk post-SBOM implementation. 3. AFLCMC Leadership & Cyber Program Executive Officers: 3a. Metric: Improvement in program risk visibility after adopting SBOM. 4. Cyber Supply Chain Risk Managers: 4a. Metric: Enhanced task efficiency and effectiveness post-SBOM policy.		

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- AFICC/KA. (2023). *AFBIT lite Air Force contracting spend FY18-22Q4* [Data set]. Air Force Business Intelligence Tool. <https://public.tableau.com/app/profile/afbit/viz/AFBITLiteAirForceContractingSpendFY18-22Q4/CategoryManagement>
- AFLCMC/LG-LZ. (2021). *Air Force Life Cycle Management Center Standard Process for Supply Chain Risk Management (SCRM)*.
- Apple Inc. (2022a). *Finder* (13.5) [Computer software].
- Apple Inc. (2022b). *MacOS Terminal* (2.13) [Computer software].
- Apple Inc. (2022c). *TextEdit* (1.18) [Computer software].
- Austin III, L. (2021). *The Department of Defense releases the president's fiscal year 2022 defense budget*. Department of Defense. <https://www.defense.gov/News/Releases/Release/Article/2638711/the-department-of-defense-releases-the-presidents-fiscal-year-2022-defense-budg/>
- Blank, S. (2009, February 16). *About Steve*. Steve Blank. <https://steveblank.com/about/>
- Blank, S. (2019, September 24). *Steve Blank Mission Model Canvas – The videos*. Steve Blank. <https://steveblank.com/2019/09/24/mission-model-canvas-the-videos/>
- BMNT. (n.d.). *Hacking for defense*. Retrieved August 20, 2023, from <https://www.h4d.us>
- Computer Security Resource Center. (2016, May 24). *Cybersecurity supply chain risk management*. National Institute of Standards and Technology. <https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management>
- Congressional Budget Office. (2020). *The budget and economic outlook: 2020 to 2030*. https://www.bea.gov/sites/default/files/2021-02/gdp4q20_2nd.pdf
- Corporation for Digital Scholarship. (2023). *Zotero* (6.0.26) [Computer software].
- Cybersecurity and Infrastructure Security Agency. (n.d.). *Software Bill of Materials (SBOM) | CISA*. Retrieved October 11, 2023, from <https://www.cisa.gov/sbom>
- Cybersecurity and Infrastructure Security Agency. (2022). *Shields up!* <https://www.cisa.gov/shields-up>
- Davies, M., Devlin, M., & Tight, M. (2010). *Interdisciplinary higher education perspectives and practicalities* (1st ed.). Emerald Group Pub.

- Department of Defense. (n.d.). *Chief information officer*. Retrieved August 20, 2023, from <https://dodcio.defense.gov/>
- Department of Defense. (2021). *Department of Defense budget for fiscal year 2022—Financial summary tables*. https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2022/FY2022_Financial_Summary_Tables.pdf
- Department of the Air Force. (2021). *Fiscal year (FY) 2022 budget estimates—Military personnel appropriation*. Department of the Air Force. <https://www.saffm.hq.af.mil/FM-Resources/Budget/Air-Force-Presidents-Budget-FY22/>
- Department of the Air Force. (2022a). *Enterprise information technology as a service wave one blanket purchase agreement FA8726-22-A-0001 performance work statement*.
- Department of the Air Force. (2022b). *Fiscal year 2022 budget overview*.
- Farrell, B. (2022). *Military cyber personnel: Opportunities exist to improve service obligation guidance and data tracking* (GAO-23-105423). U.S. Government Accountability Office. <https://www.gao.gov/products/gao-23-105423>
- Finkenstadt, D. J., Handfield, R., & Guinto, P. (2022). How firms can plan for risk in a data saturated world: The goals, decisions, signals, data (GDSD) model. *California Management Review Insights*. <https://cmr.berkeley.edu/2022/10/how-firms-can-plan-for-risk-in-a-data-saturated-world-the-goals-decisions-signals-data-gdsd-model/>
- Harper, J. (2023, May 1). Air Force's multibillion-dollar Enterprise IT as a service program cleared for takeoff. *DefenseScoop*. <https://defensescoop.com/2023/05/01/air-forces-multibillion-dollar-enterprise-it-as-a-service-program-cleared-for-takeoff/>
- IBM. (2023). *Cost of a data breach 2023*. <https://www.ibm.com/reports/data-breach>
- J. Hill, interview with author. (2022, October 25). *AFLCMC armament directorate supply chain business tool* [Personal communication].
- Josephson, B., Lee, J.-Y., Mariadoss, B. J., & Johnson, J. (2018). Uncle Sam rising: Performance implications of business-to-government relationships. *Journal of Marketing*. <https://doi.org/10.1177/0022242918814254>
- Kerner, M. (n.d.). *What is software bill of materials (SBOM)?* Retrieved October 11, 2023, from <https://www.techtarget.com/whatis/definition/software-bill-of-materials-SBOM>

- Kirschbaum, J., & Franks, J. (2022). *DOD cybersecurity: Enhanced attention needed to ensure cyber incidents are appropriately reported and shared* (GAO-23-105084). U.S. Government Accountability Office. <https://www.gao.gov/products/gao-23-105084>
- Korbren, B. (2023, February 9). *Updated supply chain resiliency & SCRM resources*. <https://www.dau.edu/blogs/updated-supply-chain-resiliency-scrm-resources>
- LeanIX. (n.d.). *Use case: SBOM to improve software supply chain security*. Retrieved September 8, 2023, from <https://www.leanix.net/en/use-cases/sbom>
- Mataloni, L. (2023, March 30). *Gross domestic product, fourth quarter and year 2022 (third estimate)—GDP by industry, and corporate profits*. <https://www.bea.gov/news/2023/gross-domestic-product-fourth-quarter-and-year-2022-third-estimate-gdp-industry-and#home>
- Mataloni, L., & Aversa, J. (2021). *Gross domestic product, fourth quarter and year 2020 (second estimate)*. Bureau of Economic Analysis. https://www.bea.gov/sites/default/files/2021-02/gdp4q20_2nd.pdf
- Mathiassen, L. (2017). Designing engaged scholarship: From real-world problems to research publications. *Engaged Management ReView*, 1(1).
- Meadows, D. (2009). *Thinking in systems: A primer*. Earthscan.
- MITRE Corporation. (n.d.a). *System of Trust™*. Retrieved October 12, 2023, from https://sot.mitre.org/framework/system_of_trust.html
- MITRE Corporation. (n.d.b). *Who we are*. Retrieved October 12, 2023, from <https://www.mitre.org/who-we-are>
- Muro, A. I. (2022, July 19). *SBOMs 101: What you need to know*. <https://devops.com/sboms-101-what-you-need-to-know/>
- National Cyber Security Centre. (2021, December 10). *Alert: Apache Log4j vulnerabilities*. <https://www.ncsc.gov.uk/news/apache-log4j-vulnerability>
- National Institute of Standards and Technology. (n.d.-a). *National vulnerabilities database (NVD)—Common vulnerabilities and exposures and the NVD Process*. Retrieved October 11, 2023, from <https://nvd.nist.gov/general/cve-process>
- National Institute of Standards and Technology. (n.d.-b). *Provenance—Glossary*. Retrieved October 11, 2023, from <https://csrc.nist.gov/glossary/term/provenance>
- National Institute of Standards and Technology. (2016). *Cybersecurity Supply Chain Risk Management*. <https://csrc.nist.gov/projects/cyber-supply-chain-risk-management>

- National Telecommunications and Information Administration. (2021a). *SBOM at a glance*. https://www.ntia.gov/sites/default/files/publications/sbom_at_a_glance_apr2021_0.pdf
- National Telecommunications and Information Administration. (2021b). *The minimum elements for a software bill of materials (SBOM)*. The United States Department of Commerce. https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
- National Telecommunications and Information Administration, W. G. (2021c). *Survey of existing SBOM formats and standards*. https://ntia.gov/sites/default/files/publications/sbom_formats_survey-version-2021_0.pdf
- Nguyen, P. (2023a). *Homebrew* (4.0.17) [Computer software]. <https://brew.sh>
- Nguyen, P. (2023b). *NPS: Full SBOM demo with dialogue*. <https://www.youtube.com/watch?v=Dy1KM7456jg>
- Office of the Chief Information Officer. (2021, September). *Jason Bonci*. <https://www.safcn.af.mil/About-Us/Biographies/Display/Article/2788272/jason-bonci/https%3A%2F%2Fwww.safcn.af.mil%2FAbout-Us%2FBiographies%2FDisplay%2FArticle%2F2788272%2Fjason-bonci%2F>
- Office of the Under Secretary of Defense for Acquisition and Sustainment. (2021). *Restructuring of the certification program for the contracting functional area*. <https://www.acq.osd.mil/dpap/policy/policyvault/USA000182-21-DPC.pdf>
- Office of the Under Secretary of Defense for Acquisition and Sustainment. (2023). *Supply chain risk management framework: Project report—Phase I*. Department of Defense. https://www.acq.osd.mil/log/LMR/.scrm_report.html/DOD_SCRM_Framework_Report_Phase_I.pdf
- OpenAI. (2023, June 11). *Python SBOM dashboard ChatGPT instruction*. <https://chat.openai.com/share/7b3f9fba-60af-42aa-a97e-2d89a07df15c>
- Parry, G., Guerrero, R., & Deandrade, C. (2022, November 3). *Details of SCBI tool with contracting team* [Personal communication].
- PBS NewsHour. (2021, May 19). *Colonial Pipeline confirms it paid \$4.4 million to hackers*. <https://www.pbs.org/newshour/economy/colonial-pipeline-confirms-it-paid-4-4-million-to-hackers>
- Peter G. Peterson Foundation. (2023, April 24). *The United States spends more on defense than the next 10 countries combined*. <https://www.pgpf.org/blog/2023/04/the-united-states-spends-more-on-defense-than-the-next-10-countries-combined>

- Phillips, L., & Phillips, M. (1993). Facilitated work groups: Theory and practice. *The Journal of Operational Research Society*, 44(6). <https://doi.org/10.1057/jors.1993.96>
- Python Software Foundation. (2023). *Python's integrated development and learning environment* (3.11.3) [Python].
- Ries, E. (2011). *The lean startup: How today's entrepreneurs use continuous innovation to create radically successful businesses: Vol. 3.1*. Crown Business.
- Rodriguez Olivera, F. (2023). *Maven Repository*. <https://mvnrepository.com/artifact/com.zaxxer/HikariCP/4.0.3>
- Schwartz, S. (2021). How a software bill of materials can help guard against supply chain cyberattacks. *Supply Chain Dive*. <https://www.proquest.com/docview/2579471955/abstract/C9827DC478A147FBPQ/1>
- Siangpipop, A. (2022). *Visualizing business intelligence within supply chains: A comparative analysis between the USAF and industry leaders* [Naval Postgraduate School]. <https://dair.nps.edu/bitstream/123456789/4784/1/NPS-LM-23-006.pdf>
- Sterman, J. (2000). *Business dynamics: Systems thinking and modeling for a complex world*. McGraw-Hill Higher Education.
- Townsend, K. (2023, February 28). *Vulnerabilities being exploited faster than ever: Analysis*. <https://www.securityweek.com/vulnerabilities-being-exploited-faster-than-ever-analysis/>
- U.S. Department of Homeland Security. (2023, May 30). *Cybersecurity*. <https://www.dhs.gov/topics/cybersecurity>
- White House. (2021). *Executive order on improving the nation's cybersecurity*. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
- Whitler, K. (2018). Why too much data is a problem and how to prevent it. *Forbes*. <https://www.forbes.com/sites/kimberlywhitler/2018/03/17/why-too-much-data-is-a-problem-and-how-to-prevent-it/?sh=137b072e755f>

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

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



DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE