Pacific Northwest
NATIONAL LABORATORY

PNNL-29642

Attack Scenarios Relating to Army Facility-Related Control Systems: Quantifying the Cost to Secure and Cost Savings of the Army's FRCS Program

January 2020

Jey Castleberry
Carl Baker
Anna Britton
Kristine Arthur-Durrett
Nicholas Thompson
Shadya Rosado Maldonado
Penny McKenzie
Mark Watson
Anna Lipton

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Defense
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov

PNNL-29642

Attack Scenarios Relating to Army Facility-Related Control Systems: Quantifying the Cost to Secure and Cost Savings of the Army's FRCS Program

January 2020

Jey Castleberry
Carl Baker
Anna Britton
Kristine Arthur-Durrett
Nicholas Thompson
Shadya Rosado Maldonado
Penny McKenzie
Mark Watson
Anna Lipton

Prepared for
the U.S. Department of Defense
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Summary

Pacific Northwest National Laboratory (PNNL) analyzed the cyber-threat environment to U.S. Army facilities. This report describes three key factors in securing Army-owned facility-related control systems (FRCS). First, Section 1.0 provides background information about the project. Section 2.0 describes the various types of cyber-attacks. Section 3.0 provides a series of attack scenarios from real-world use cases are described in Section 3. These examples are relevant to the Army because the targeted systems or operating environments are like those used at Army installations. An estimated range for the cost to secure these systems is described in Section 4.0. Finally, the cost savings of preventing these kinds of attacks are described in Section 5.0.

Attack Scenarios. The Office of the Director of National Intelligence's Cyber Threat Framework was used to adapt and modify the FRCS Cyber Adversary Model comprising three sections: FRCS Adversary Tier Hierarchy (ATH), FRCS Cyber Adversarial Stages (CAS), and a FRCS Cyber Activity Profile (CAP). By applying the FRCS Cyber Adversary Model, installations can forecast adversary activities, understand adversaries' motivations and behavior, and better prepare installations' FRCS systems against failures due to differing levels of a cyber-attack. The threat tiers introduced in this paper can be used to analyze the stages of each cyber threat, the preparation activities of the adversary, the engagements of the adversary, the effects or consequences of an attack, and the indicators of compromise of FRCS systems. An overview of the FRCS Cyber Adversary Model process is illustrated in Figure E.1.

FRCS ATH

The FRCS Adversary Tier Hierarchy is a comprehensive and foundational understanding of the posed threats to FRCS on an installation. These capability levels are adapted from the adversary capability levels spreadsheet provided by the Deputy Chief of Staff of G-9 installations. The FRCS ATH defines a threat description tailored from the Cyber Threat Framework for each tier classification. It also provides a high-level functional summary for each tier and assigns a relative cost to the adversary required to participate at each tier.

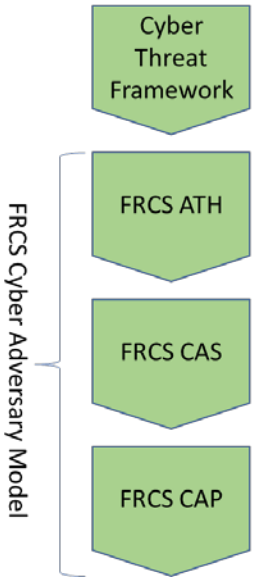
FRCS CAS

The FRCS CAS is used to characterize the stages of a cyber threat to include the preparation activities of the adversary, the engagements of the adversary, the presence of the adversary, and the effects or consequences of an attack on FRCS.

FRCS CAP

The FRCS CAP the standard approach used to characterize specific cyber-attacks, align an adversary capability level, and assign a threat tier level. The FRCS CAP is used to compare specific attacks and adversaries. This method is used in Section 3.0, which describes Army-relevant cyber-attacks.

Below is the description and characterization of the security event known popularly as Black Energy. Additional use cases can be found in Section 3.



Purpose	Outcome
• Informs the FRCS Cyber Adversary Model.	• Provides common lexicon to communicate information about cyber attacks. • Provides criteria for measuring cyber attacks.
• Provides a Threat Description tailored from the Cyber Threat Framework for each Tier Classification.	• Establishes criteria for Objectives, Actions, and Indicators. • Aligns Objective, Actions, and Indicators with Tier Classifications.
• Provides a description for the Cyber Threat Framework Stages for each Tier Classification.	• Establishes criteria for Preparation, Engagement, Presence, and Effect/Consequence for Tier Classification.
• Establishes a methodology for profiling specific cyber attacks.	• Characterized specific cyber attacks. • Assigns a Tier Classification to a specific cyber attack.

Figure Exec.1. FRCS Cyber Adversary Model Process

1. **Cost to Secure**. Two approaches were used to determine the cost to secure. First, the 2017 cost-benefits analysis provided estimates for three unique but overlapping Courses of Action (COAs). Second, the annual labor required to implement a Risk-Management-Framework-based cybersecurity program for FRCS at small, medium, and large installations was estimated in Full-Time Equivalent (FTE) hours.

The 2017 cost-benefits analysis estimated the cost to implement the Risk Management Framework for FRCS on 156 Army installations. The estimates were for three distinct but overlapping COAs.

COA 1: Discover, assess, and remediate cybersecurity vulnerabilities in 100 critical assets (buildings) across 24 installations.

COA 1 Cost: $71.6M

COA 2: COA 1 and any Department of Defense Information Network connected FRCS. It is not known how many FRCS are connected to the Department of Defense Information Network. COA 2 is the sum of COA 1 and half of the COA 3 costs.

COA 2 Cost: $630.4M

COA 3: Discover, assess, and remediate all Army-owned FRCS. This estimate used a population size of 150,000 buildings.

COA 3 Cost: $1,268M

Labor to manage an active cybersecurity program at small, medium, and large installations was estimated. Installation size was determined using models developed during the 2017 cost-

benefits analysis. Table E.1 shows the range, based on number of buildings, used to model Army installations.

Table Exec.1. Installation Size by Number of Buildings

Number of Buildings	Small	Medium	Large
Range	3–999	1,000–2,249	2,250+
Mode	555	1,500	2,250

The level of effort, measured in FTE hours, needed to implement security controls for stand-alone FRCS networks is derived from the staffing requirements to perform the roles and responsibilities outlined in DoDI 8510.01 *Risk Management Framework*. An FTE is defined as 2,000 hours per year.

The roles needed to implement security controls for a stand-alone FRCS network on small, medium, and large installations were identified. Not all roles will be needed at every installation. Specific criteria to choose between two or three FTEs for a small installation or three to four FTEs for a medium installation is not identified in this report.

2. **Cost Savings.** The cost savings of preventing cyber-attacks considered two areas: the Army's Mission Value and the replacement costs of the protected assets (Army-owned FRCS).

Army missions are executed when the perceived benefits exceed the perceived costs. Mission benefits can be assessed in monetary terms, but non-monetary benefits can greatly eclipse the monetary benefits. Army missions are executed to advance U.S. geo-political interests and objectives. These interests and objectives are rarely expressed in monetary terms. Security, support of our allies, reduction in conflict, and international stability are difficult objectives to assign a dollar value to. Likewise, individual facilities, assets, or missions throughout and across the Army hierarchy have qualitative or operational value above and beyond their replacement cost or monetary value. In conjunction with the asset valuation described in this summary, it is recommended that assets be evaluated for qualitative, operational and other non-monetary value. Some relatively low-cost assets can be critical to mission success. A comprehensive valuation of any given asset must include some qualitative assessment of its importance relative to Army missions.

The cost savings of preventing these attacks were determined using known inventory data. The inventory data was used to create a model of 31 buildings and extrapolate that model against the estimated population size of 150,000 buildings.

The estimated maximum value of all FRCS for 150,000 buildings after removing the outliers from the data set is $4,881M. The estimated minimum value is $60M. These numbers were determined using 0.021% of the data from estimated population size.

A method for estimating the asset value and cost to secure FRCS on a given installation is summarized in the Conclusion. Figure E.2 shows a scaled comparison of the estimated costs to secure and the estimated asset valuation for all Army-owned FRCS.

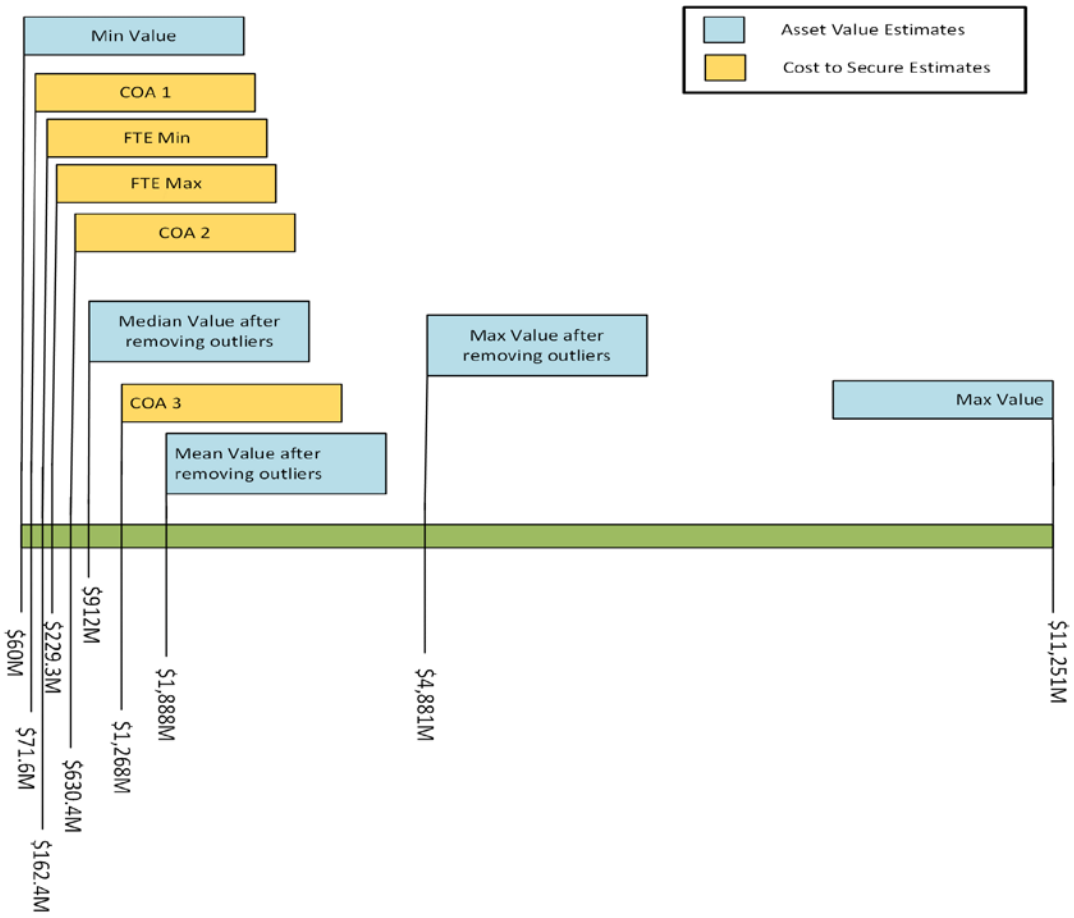


Figure Exec.2. Estimated Costs to Secure and Cost Savings Comparisons

Acronyms and Abbreviations

APT	Advanced Persistent Threat
AR	Army Regulation
ATH	Adversary Tier Hierarchy
CAP	Cyber Activity Profile
CAS	Cyber Adversarial Stages
COA	Course of Action
CTF	Cyber Threat Framework
DoDIN	Department of Defense Information Network
DPW	Department of Public Works
FRCS	Facility-Related Control Systems
FTE	Full-Time Equivalent
ICS	Industrial Control Systems
IT	Information Technology
NIST	National Institute of Security and Technology
ODNI	Office of the Director of National Intelligence
OT	Operational Technology
PII	Personally Identifiable Information
PLC	Programmable Logic Controllers
PNNL	Pacific Northwest National Laboratory
SCADA	Supervisory Control and Data Acquisition
SIS	Safety Instrumented System
USB	Universal Serial Bus

Contents

Figures

Tables

1.0 Introduction

Pacific Northwest National Laboratory (PNNL) analyzed the cyber-threat environment to U.S. Army facilities. This report is intended to provide the reader with an understanding of the nature and extent of the cyber threat environment, the costs of securing against those threats, and the cost savings by securing against those threats. The primary audience is Army Energy Managers and U.S. Department of Army headquarters offices. The information provided will aid the reader in understanding the nature of the threat environment and the risks associated with failure to act. Installation Energy Managers should be motivated to secure facility-related control systems (FRCS) (i.e., Building Control Systems, Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, Operational Technology (OT), Energy Generating Assets, etc.), and Army headquarters staff should understand the need for additional resources and make sure that those resources are available. Management should make risk-based and cost-effective security control investment decisions; addressing security early in an FRCS life cycle can result in adequate security and significant cost savings. Each of the major components is addressed in the following sections.

Section 2 of this document addresses the attack scenarios that may affect Army FRCS. Known previous attacks are characterized and aligned with cyber behavior associated with the FRCS Cyber Adversary Model, which comprises three sections: FRCS Adversary Tier Hierarchy (ATH), FRCS Cyber Adversarial Stages (CAS), and a FRCS Cyber Activity Profile (CAP). The adversary tier levels are derived from the U.S. Department of Defense, Defense Science Board (DoD 2013), and other U.S. government sources and include classifications for advanced persistent threats, cyber terrorists/activists, and insider threats. For a detailed description of the Cyber Adversary Model from Section 2.2, see Appendix A. For a detailed description of the Adversary Characterizations from Section 2.3, see Appendix B.

Section 3 describes attack scenarios taken from real-world use cases. These use cases relate to either Army FRCS equipment or Army FRCS operating environments. All seven uses cases were characterized using the methodology described in Section 2.

Section 4 quantifies the costs of securing these systems using two approaches. Section 4.1 summarizes an Army-wide cost estimate performed in 2017. Section 4.2 addresses cost from the perspective of the roles and responsibilities required at the facility level. For a detailed description of the labor hour estimation from Section 4, see Appendix C.

Section 5 addresses the savings of preventing these attacks. The cost savings are based on an estimate of the asset valuation of all Army-owned FRCS using existing inventory data and extrapolating that data across 150,000 buildings. For a detailed description of the FRCS asset valuation from Section 5, see Appendix D.

2.0 Characterizing Cyber-Attacks

To better inform the Army of the adversary threat landscape to an Army installation, PNNL tailored a commonly accepted technical cyber lexicon from the Cyber Threat Framework (CTF) (ODNI 2018a) that closely aligns with industry definitions and other U.S. government agencies, partners, and stakeholders in discussing adversary activities throughout the adversary threat life cycle. PNNL overlaid Army-provided adversary capability levels onto its tailored CTF. The result was a cyber incident scorecard that can be used to quickly compare and characterize use cases.

2.1 Cyber Threat Framework

CTF is a cybersecurity analytical framework published by the Office of the Director of National Intelligence (ODNI 2018b).[1] According to the Office of the Director of National Intelligence, “its principle benefit being that it provides a common language for describing and communicating information about cyber threat activity” (ODNI 2018b).

As illustrated in Figure 1, the “Stages” layer is the foundation of CTF. The Stages bind the other layers (Objectives, Actions, and Indicators) to time forcing a sequential analysis of cyber threats, shown in Figure 2. Building from Stages, PNNL adapted the CTF lexicon definitions of the four adversary activity stage terms as follows (Zager and Zager ND):

- **Preparation:** Activities undertaken by threat actors, their leadership, and/or sponsors to prepare for conducting malicious cyber activities.
- **Engagement:** Threat actor activities taken before gaining but with the intent to gain unauthorized access to the target.
- **Presence:** Actions taken by the threat actor that establish and maintain conditions allowing the threat actor to perform intended actions.
- **Effect/Consequence:** Outcomes of threat actor actions on a victim's physical or virtual computer or information systems, networks, and/or data stores.
- **Objectives:** The purpose of conducting an action or a series of actions.
- **Actions:** Adversarial activity against a target to achieve an objective.
- **Indicators:** Exemplars of discrete, measurable indicators of compromise, e.g., malware, that indicates an attempt to achieve an objective.

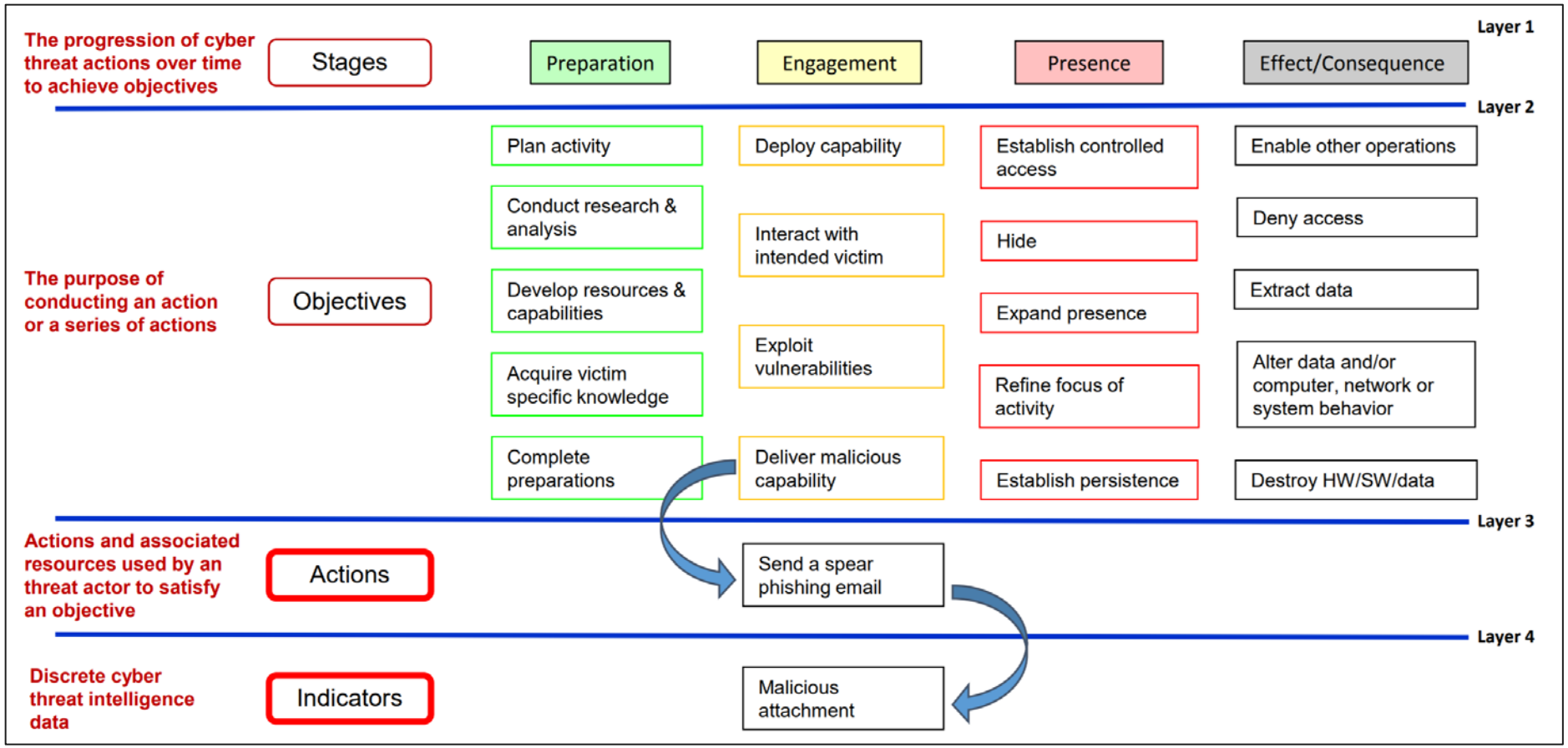


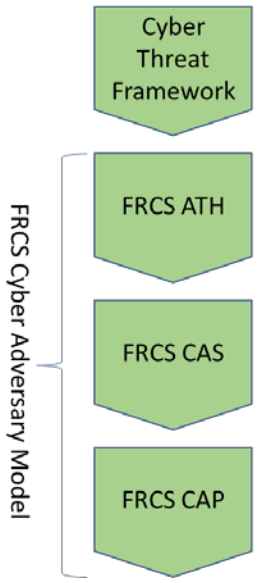
Figure 1. Stages and Objectives of the Cyber Threat Framework Adversary

The FRCS Cyber Adversary Model's hierarchical structure follows a simplified, non-technical threat progression that permits the Army to objectively map diverse models to a commonly accepted standard. Aligning a common approach helps to:

- Establish a shared ontology and enhance information sharing because it is easier to maintain mapping of multiple models to a common reference than directly to each other
- Characterize and categorize threat activity in a straightforward way that can support missions ranging from strategic decision making to analysis and cybersecurity measures and users from generalists to technical experts
- Support common situational awareness across organizations

2.2 FRCS Cyber Adversary Model

CTF was used to adapt and modify the FRCS Cyber Adversary Model that comprises three sections: FRCS ATH, FRCS CAS, and a FRCS CAP. By applying the FRCS Cyber Adversary Model, installations can forecast adversary activities, understand their motivations and behavior, and better prepare installations' FRCS systems against failures caused by cyber-attacks. The threat tiers introduced in this report can be used to analyze the stages of each cyber threat, the preparation activities of the adversary, the engagements of the adversary, the effects or consequences of an attack, and the indicators of compromise of FRCS systems. An overview of the FRCS Cyber Adversary Model process is shown in Figure 2.



Purpose	Outcome
• Informs the FRCS Cyber Adversary Model.	• Provides common lexicon to communicate information about cyber attacks. • Provides criteria for measuring cyber attacks.
• Provides a Threat Description tailored from the Cyber Threat Framework for each Tier Classification.	• Establishes criteria for Objectives, Actions, and Indicators. • Aligns Objective, Actions, and Indicators with Tier Classifications.
• Provides a description for the Cyber Threat Framework Stages for each Tier Classification.	• Establishes criteria for Preparation, Engagement, Presence, and Effect/Consequence for Tier Classification.
• Establishes a methodology for profiling specific cyber attacks.	• Characterized specific cyber attacks. • Assigns a Tier Classification to a specific cyber attack.

Figure 2. FRCS Cyber Adversary Model Process

2.2.1 FRCS Adversary Tier Hierarchy

The FRCS ATH is a comprehensive and foundational understanding of the posed threats to FRCS on an installation. The FRCS ATH defines a threat description tailored from CTF for each tier classification and provides a high-level functional summary for each tier and assigns a relative cost for the adversary required to participate at each tier.

See Appendix A for a detailed description of the FRCS ATH.

2.2.2 FRCS Cyber Adversarial Stages

The FRCS CAP is used to characterize the stages of a cyber threat to include the preparation activities of the adversary, the engagements of the adversary, the presence of the adversary, and the effects or consequences of an attack on FRCS.

See Appendix A for a detailed description of the FRCS CAS.

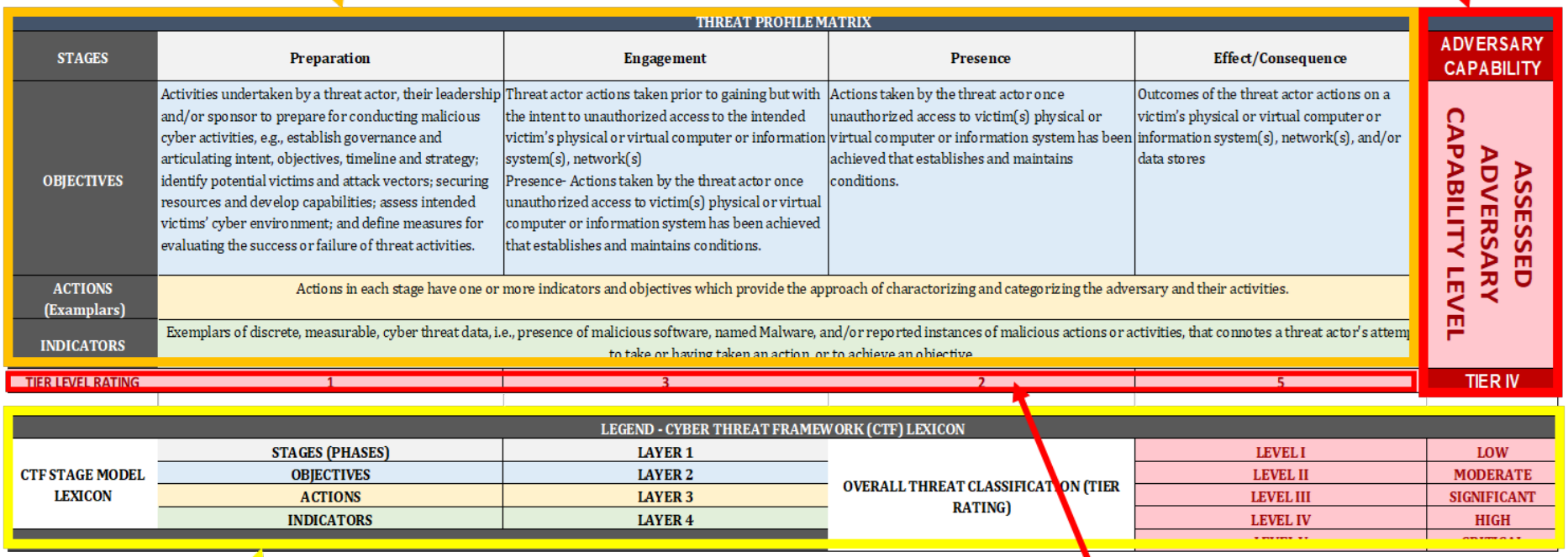
2.2.3 FRCS Cyber Activity Profile

The FRCS CAP in Figure 3 is the standard approach used to characterize specific cyber-attacks, align an adversary capability level, and assign a threat tier level. The FRCS CAP is used to compare specific attacks and adversaries to determine possible threat. This method is used in Section 3.0, which describes Army-relevant cyber-attacks.

See Appendix A for a detailed description of the FRCS CAP.

FRCS CAS: Stage alignment of attack details with Cyber Threat Framework metrics modified for FRCS.

FRCS ATH: Cumulative Tier Classification Determination for attack.



THREAT PROFILE MATRIX

STAGES	Preparation	Engagement	Presence	Effect/Consequence	ADVERSARY CAPABILITY
OBJECTIVES	Activities undertaken by a threat actor, their leadership and/or sponsor to prepare for conducting malicious cyber activities, e.g., establish governance and articulating intent, objectives, timeline and strategy; identify potential victims and attack vectors; securing resources and develop capabilities; assess intended victims' cyber environment; and define measures for evaluating the success or failure of threat activities.	Threat actor actions taken prior to gaining but with the intent to unauthorized access to the intended victim's physical or virtual computer or information system(s), network(s) Presence- Actions taken by the threat actor once unauthorized access to victim(s) physical or virtual computer or information system has been achieved that establishes and maintains conditions.	Actions taken by the threat actor once unauthorized access to victim(s) physical or virtual computer or information system has been achieved that establishes and maintains conditions.	Outcomes of the threat actor actions on a victim's physical or virtual computer or information system(s), network(s), and/or data stores	ASSESSED ADVERSARY CAPABILITY LEVEL
ACTIONS (Examplars)	Actions in each stage have one or more indicators and objectives which provide the approach of charactorizing and categorizing the adversary and their activities.				
INDICATORS	Exemplars of discrete, measurable, cyber threat data, i.e., presence of malicious software, named Malware, and/or reported instances of malicious actions or activities, that connotes a threat actor's attemp to take or having taken an action, or to achieve an objective				
TIER LEVEL RATING	1	3	2	5	TIER IV

LEGEND - CYBER THREAT FRAMEWORK (CTF) LEXICON

CTF STAGE MODEL LEXICON	STAGES (PHASES)	LAYER 1	OVERALL THREAT CLASSIFICATION (TIER RATING)	LEVEL I	LOW
	OBJECTIVES	LAYER 2		LEVEL II	MODERATE
	ACTIONS	LAYER 3		LEVEL III	SIGNIFICANT
	INDICATORS	LAYER 4		LEVEL IV	HIGH

FRCS CAP Legend.

FRCS ATH: Tier Classification Determination for attack by Stage of the attack.

Figure 3. FRCS Cyber Activity Profile

2.3 Characterizing Adversaries

Adversary models are crucial in the field of cybersecurity as they are used to better understand the tactics, techniques, and procedures of varying threats to FRCS. Adversaries have varying degrees of capabilities, and each of the customized models attempts to define the different types of attackers, their skill sets, and the threats they pose to FRCS and Army installations.

The following sections characterize three adversary types relevant to the U.S. Army: advance persistent threats (APTs), cyber terrorists and hacktivists, and insiders. While other adversary types exist, this study focuses on three broad categories and aligns each specific use case to the FRCS CAP described briefly in Section 2.0 and in detail in Appendix A.

See Appendix B for a detailed description of each Adversary Type.

2.3.1 Advanced Persistent Threat

APT actors are recognized in the industry to be the most capable cyber threat archetype, but this is a common misconception. While the FRCS CTF describes APT threat activity elements, analysts and decision makers cannot assume there is one cyber tactic, technique, or procedure that definitively describes APT actor activity. The most common type of APT is the nation state. These are highly resourced and highly skilled organizations that dedicate significant resources to achieving ideological, strategic, or financial goals.

Deterring APTs is difficult and requires an aggressive, well-managed cybersecurity program. Table 1 has high-level recommendations and associated resources for mitigating threats to an installation's FRCS. Defending against APTs requires proactive implementation of recommendations 1–5.

Table 1. Recommended Mitigations

Recommendation	Resources
1. Full Risk Management Framework implementation at a security assurance level that supports the installation's mission.	DoDI 8500.01 DoDI 8510.01 NIST SP 800-53rev4
2. Insider Threat Program.	AR 381-12
3. Active Network Monitoring.	NIST SP 800-137 NIST SP 800-92 NIST SP 800-94
4. Response Team.	ARCYBER
5. Redundant Systems.	Installation responsibility

2.3.2 Cyber Terrorists and Hacktivists

Cyber terrorism is defined as an illicit, politically motivated act by an individual, nation state, or non-state actor that uses computer, network, internet, and information and communication technologies to obstruct political, social, and/or economic operations among a group, organization, or government. Cyber terrorist attacks involve harm against property or persons that causes extreme damage using computers as weapons or targets. Cyber terrorism also

includes acts of online terrorist propaganda, recruitment, and material support of terrorist activities.

Hacktivism is carried out by non-state actors with the intent to "disrupt, disable, or control computer systems, or steal the data they contain" (Denning 2001). Hacktivists support certain political, social, or religious causes, often in opposition of government policies. While both hacktivism and cyber terrorism are politically motivated, computer-generated, and perpetrated against a computer target, they differ significantly in intent and destruction. The intention behind cyber terrorists' attacks is to spread far-reaching terror and destruction, while hacktivists intend to merely disrupt or upset their targets.

Deterring cyber terrorist and hacktivists requires proactive implementation of recommendations 1–3 from Table 1.

2.3.3 Insider Threat

An insider threat is a trusted individual who is currently or was formerly given legitimate, authorized access, privileges, or knowledge to an organization's information systems, data or network. Insider threats can be malicious or non-malicious, resulting from actions that are intended or unintended. The most destructive malicious insider threat can include:

- Espionage
- Terrorism
- Sabotage
- Extortion
- Bribery
- Embezzlement
- Corruption
- Access and dissemination of sensitive and classified information
- Illicit communications.

An insider can include:

- An employee, student, or member of the host institution that has the legitimate access and ability to operate a computer system
- An associate, contractor, business partner, supplier, computer maintenance technician, guest, etc. with business relations with the host institution
- Any individual who has authorization to perform certain activities, such as a customer who accesses their account using the institution's system
- An individual who has been properly identified and authenticated, including a masquerader or an individual an insider has granted access
- An individual who has been coerced by an outsider to perform actions against his/her will
- A former insider who did not have access and credentials revoked upon leaving the institution (Pfleeger 2008).

Deterring cyber terrorist and hacktivists require proactive implementation of recommendations 1–2 from Table 1.

See Appendix B for a detailed description of each Adversary Type.

3.0 FRCS Real-World Use Cases

The use cases in sections 3.1–3.7 describe cyber-attacks using the characterization schema described in Section 2.0. These use cases relate to Army systems by either using the same types of FRCS equipment or operating in environments like Army FRCS. These well-known attacks include examples of APT, cyber terrorism, and insider threat activities.

3.1 APT: Havex

Havex is a remote access trojan. The Havex campaign uses three vectors of delivery: spear phishing, watering-hole attacks, and application infections. Spear-phishing efforts are used to infect victim computers and collect information on energy delivery system environments. Watering-hole attacks target users who visit legitimate websites and are redirected to command and control servers that contain the infected software. Havex is an intelligence-collection tool that is used for espionage and is not usually used for the disruption or destruction of industrial systems. The data collected by Havex aids in efforts to design and develop new malware attacks against energy delivery systems. More information is shown in Table 2.

For specific details regarding this incident see references as annotated in the text below.

Table 2. Havex Attack Summary

Adversary: Russian Information Service (NJCCIC 2017, NCCIC, FBI 2016)	**Adversary Type:** Advanced Persistent Threat	**Adversary Capability Level:** 5
Malware: Havex (ICS-CERT 2014a, ICS-CERT 2014b)	**Threat Vector:** Remote Access Trojan (RAT)	
Target: Havex specifically targets energy grid operators, major electricity generation firms, petroleum pipeline operators, and industrial equipment providers.		
Consequence: Havex is estimated to have affected as many as 2,000 infrastructure sites, a majority of which were in Europe and the United States. Within the energy sector, Havex specifically targets energy grid operators, major electricity generation firms, petroleum pipeline operators, and industrial equipment providers. The Havex malware leverages the Open Platform Communications standard, a protocol used by ICS and SCADA devices across industry that facilitates open connectivity and vendor equipment interoperability.		
Relevance to the Army: ICS/SCADA equipment and vendors used in FRCS environments		

The Havex attack pathway in Figure 4 shows the patterns, cyber events, and behaviors that the adversary takes to ultimately compromise the target systems. There are distinctive patterns to the adversary's methods that can result in easier identification of similar pathways, methods, and malware identification.

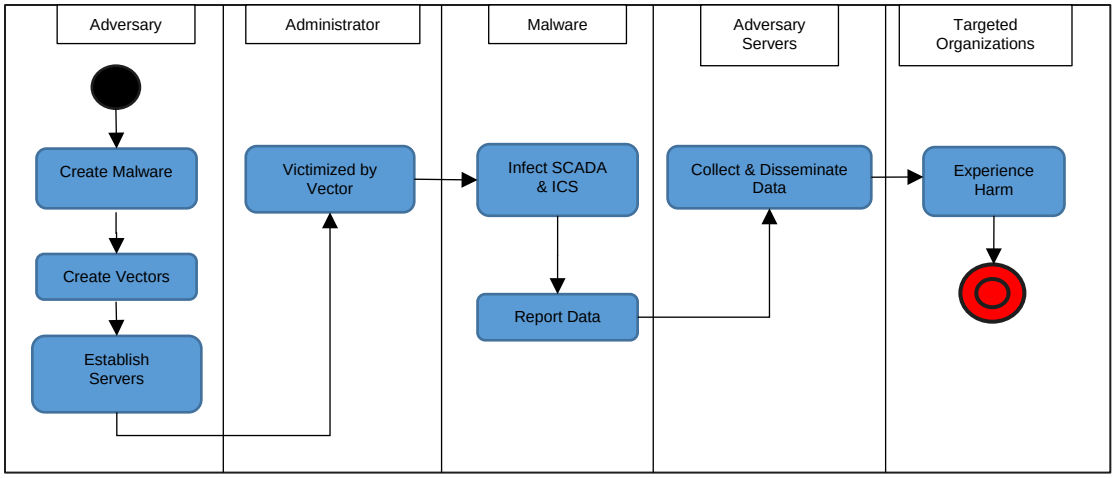


Figure 4. Havex Attack Pathway

Havex CAP provides examples of discrete, measurable, cyber threat information that aligns with the adversary's attempt to take or has taken against the target to reach their goal. The chart provides an understanding of the activities that the adversary takes in preparing their attack, the engagement they take before gaining unauthorized access to systems, the presence within the target systems, and the effect and consequence of the cyber-attack.

Table 3. Havex Cyber Activity Profile Rating—Tier V

CYBER ACTIVITY PROFILE					
STAGES	**Preparation**	**Engagement**	**Presence**	**Effect/Consequence**	ADVERSARY CAPABILITY
OBJECTIVES	Identification of target organization (energy systems)	Gain a foothold within compromise systems	Go undetected and secretly hide within compromised system	Cause damage to energy systems	ASSESSED ADVERSARY CAPABILITY LEVEL
ACTIONS (Exemplars)	Attacker creates malware	Attacker establishes delivery vectors a) Spear Fishing b) Watering Hole c) Vendor compromise Remote access trojan is deployed	System administrator falls victim to delivery vector Data collected and distributed by command and control servers	SCADA and ICS systems are compromised; intellectual property theft; adversary engaged in active intelligence collection	
INDICATORS	No indicators	Security software failed to identify the launch of the remote access trojan	System administrator failed to observe data was leaked	Target and other organizations harmed by unauthorized information release	
THREAT TIER RATING	5	4	5	5	TIER V

LEGEND - CTF LEXICON					
CTF STAGE MODEL LEXICON	STAGES (PHASES)	LAYER 1	OVERALL THREAT CLASSIFICATION (TIER RATING)	LEVEL I	LOW
	OBJECTIVES	LAYER 2		LEVEL II	MODERATE
	ACTIONS	LAYER 3		LEVEL III	SIGNIFICANT
	INDICATORS	LAYER 4		LEVEL IV	HIGH
				LEVEL V	CRITICAL

3.2 APT: Stuxnet

Stuxnet is a computer worm. Stuxnet was designed to target PLCs programmable logic controllers (PLCs) that control the automation of electromechanical processes. This malware was introduced to systems using an infected Universal Serial Bus (USB), so the adversary had to have physical access to the systems. Stuxnet was the first of its kind and caused reputable damage to an Iranian nuclear facility.

For specific details regarding this incident see references as annotated in the text below.

Table 4. Stuxnet Attack Summary

Adversary: Unknown	**Adversary Type:** Advanced Persistent Threat; targeted espionage	**Adversary Capability Level:** 5
Malware: Stuxnet (NJCCIC 2017, Langner 2013)	**Threat Vector:** Remote Access Trojan	
Target: Iranian-owned centrifuges used in uranium enrichment		
Consequence: Stuxnet was used specifically to target centrifuges at Iran's uranium enrichment facility outside Natanz, Iran. It manipulated valves on the centrifuges, increasing and decreasing their speed, putting additional pressure on them, and ultimately damaging the machines until they no longer functioned. When Stuxnet infects a computer, it checks to see if that computer is connected to specific models of PLCs manufactured by Siemens. PLCs are how computers interact with and control industrial machinery like uranium centrifuges. The worm then alters the PLCs' programming, resulting in the centrifuges being spun too quickly and for too long, damaging or destroying the delicate equipment in the process. While this is happening, the PLCs tell the controller computer that everything is working fine, making it difficult to detect or diagnose what's going wrong until it's too late.		
Relevance to the Army: Air-gapped FRCS environments are still vulnerable to USB-delivered espionage. Demonstrate a capability for limited gap jumping and the ability to effectively traverse the information technology (IT) and OT boundary.		

The Stuxnet attack pathway in Figure 6 shows the patterns, cyber events, and behaviors that the adversary took to ultimately compromise the target systems. There are distinctive patterns to the adversary's methods that can result in easier identification of similar pathways, methods, and malware identification.

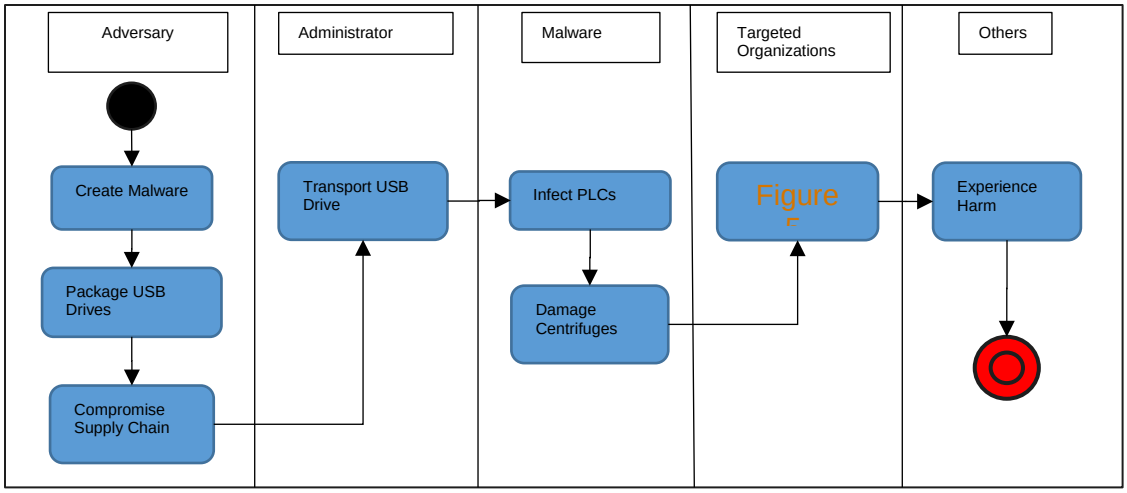


Figure 6. Stuxnet Attack Pathway

The Stuxnet CAP provides examples of discrete, measurable, cyber threat information that aligns with the adversary's attempt to take or has already taken against the target to reach his/her goal. The chart provides an understanding of the activities that the adversary took in preparing the attack, the engagement taken before gaining unauthorized access to systems, the presence within the target systems, and the effect and consequence of the cyber-attack.

Table 5. Stuxnet Cyber Activity Profile Rating—Tier V

STAGES	Preparation	Engagement	Presence	Effect/Consequence	ADVERSARY CAPABILITY
OBJECTIVES	Identification of target organization (Iranian nuclear program centrifuges)	Attacker to inject infected USB drives into Iranian nuclear facility supply chain	Go undetected and spread through the isolated (air-gapped) network	Cause maximum damage to Iranian nuclear program	ASSESSED ADVERSARY CAPABILITY LEVEL
ACTIONS (Exemplars)	Attacker creates malware Attacker packages malware on USB drives potentially destined for Iranian nuclear facility	System administrator falls victim to delivery vector Infected drive used to transport malware into the isolated (air-gapped) network	Malware spreads through isolated network and infects targeted ICS devices (centrifuge PLCs)	Iranian nuclear program harmed and setback functionality of nuclear systems	
INDICATORS	No indicators	No effective mitigations for removal media	Engineers failed to identify ICS devices' drive centrifuges functioning abnormally because of malware injection	Target centrifuges were operating outside normal ranges, leading to breakage of the systems. Inadvertent infection of non-target systems	
THREAT TIER RATING	5	5	5	5	TIER V

LEGEND - CTF LEXICON					
CTF STAGE MODEL LEXICON	STAGES (PHASES)	LAYER 1	OVERALL THREAT CLASSIFICATION (TIER RATING)	LEVEL I	LOW
	OBJECTIVES	LAYER 2		LEVEL II	MODERATE
	ACTIONS	LAYER 3		LEVEL III	SIGNIFICANT
	INDICATORS	LAYER 4		LEVEL IV	HIGH
				LEVEL V	CRITICAL

3.3 APT Use Case: TRISIS/TRITON

TRISIS, also known as TRITON or HatMan, is a malware variant that targets Schneider Electric Triconex Safety Instrumented System (SIS) controllers. TRISIS was designed specifically to interact with SIS controllers. It was deployed manually after a threat actor gained remote access to a SIS engineering workstation to reprogram the SIS controllers. TRITON has been linked to the Central Scientific Research Institute of Chemistry and Mechanics, a technical research organization owned by the Russian government.

For specific details regarding this incident see references as annotated in the text below.

Table 6. XENOTIME Attack Summary

Adversary: XENOTIME (MITRE ND, MITRE 2019)	**Adversary Type:** Advanced Persistent Threat	**Adversary Capability Level:** 4-5
Malware: TRISIS/TRITON	**Threat Vector:** Supply Chain Compromise	
Target: Oil, natural gas, Electric, manufacturing, suppliers/vendors		
Consequence: XENOTIME, the group behind the TRISIS event, previously focused on oil and gas related targeting. In February 2019, Dragos identified a change in XENOTIME behavior: Starting in late 2018, XENOTIME began probing the networks of electric utility organizations in the United States and elsewhere using similar tactics to the group's operations against oil and gas companies. Multiple ICS sectors now face the XENOTIME threat; this means individual verticals—such as oil and gas, manufacturing, or electric—cannot ignore threats to other ICS entities because they are not specifically targeted. Therefore, a key element in defense against sophisticated, expanding threats is understanding threat behaviors and methodologies beyond simply indicators of compromise. Asset owners and operators across ICS should be aware of XENOTIME's tactics, techniques, and procedures (CISA 2019), and consider using an ICS-specific detection capability while also implementing defensive recommendations discussed below.		
Relevance to the Army: Safety systems, such as SIS, in FRCS environments are vulnerable to changes in set points on the remainder of the process control system that could be changed to conditions that would result in the process shifting to an unsafe condition. Demonstrate a capability for limited gap jumping and the ability to effectively traverse the IT/OT boundary.		

The XENOTIME attack pathway in Figure 7 shows the patterns, cyber events, and behaviors that the adversary took to ultimately compromise the target systems. There are distinctive patterns to the adversary's methods that can result in easier identification of similar pathways, methods, and malware identification.

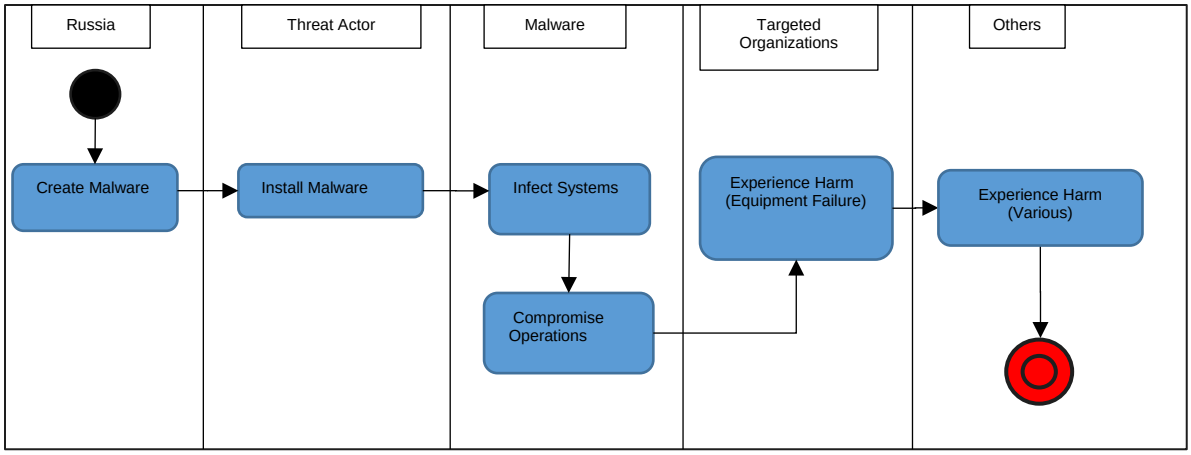


Figure 7. XENOTIME Attack Pathway

XENOTIME CAP provides examples of discrete, measurable cyber threat information that aligns with the adversary's attempt to take or has acted against the target to reach its goal. The chart provides an understanding of the activities that the adversary took in preparing their attack, the engagement the adversary took before gaining unauthorized access to systems, the presence within the target systems, and the effect and consequence of the cyber-attack.

Table 7. TRISIS/TRITON Cyber Activity Profile Rating—Tier V

CYBER ACTIVITY PROFILE					
STAGES	**Preparation**	**Engagement**	**Presence**	**Effect/Consequence**	ADVERSARY CAPABILITY
OBJECTIVES	Identification of target systems (oil, natural gas, electric, manufacturing, vendors and suppliers)	Attacker establishes foothold in the corporate network	Go undetected, spread through the corporate network, and gain access to the OT network	Compromise of various oil, natural gas, manufacturing, and other operations leading to economic and other harms	ASSESSED ADVERSARY CAPABILITY LEVEL
ACTIONS (Exemplars)	External scanning, network enumeration, and open source research of victims	Attacker's agent obtains access to targeted systems, harvests credentials for access to IT/OT systems and installs malware	Reconnaissance, lateral movement, escalate privileges, and maintain presence in the target environment. SIS controllers report bogus data	Plant operations are compromised, leading to potential equipment damage and risk to operator safety	
INDICATORS	No Indicators	Failure to use common network intrusion detection software. Attempted authentication with stolen credentials and brute force entry	Failure to prioritize detection and defense across Windows systems in both IT and OT		
THREAT TIER RATING	5	5	4	5	TIER V

LEGEND - CTF LEXICON					
CTF STAGE MODEL LEXICON	STAGES (PHASES)	LAYER 1	OVERALL THREAT CLASSIFICATION (TIER RATING)	LEVEL I	LOW
	OBJECTIVES	LAYER 2		LEVEL II	MODERATE
	ACTIONS	LAYER 3		LEVEL III	SIGNIFICANT
	INDICATORS	LAYER 4		LEVEL IV	HIGH
				LEVEL V	CRITICAL

3.4 APT Use Case: Black Energy

Black Energy malware was designed to be delivered to an ICS system using spear phishing campaigns to conduct reconnaissance that specifically targets owners and operators. Black Energy was first a distributed denial of service tool and evolved to include modules for the exploitation of vulnerabilities in networked ICS and a data collection tool.

For specific details regarding this incident see references as annotated in the text below.

Table 8. Black Energy Attack Summary

Adversary: Russian Hacking Group known as "Sandworm" (MITRE 2017a)	**Adversary Type:** Advanced Persistent Threat	**Adversary Capability Level:** 5
Malware: Black Energy Malware (MITRE 2017b)	**Threat Vector:** Remote Access Trojan	
Target: Energy utility networks that support FRCS, ICS, and energy delivery systems		
Consequence: The attack focuses on industrial control systems and energy delivery systems similar to FRCS used on Army installations		
Relevance to the Army: The targeted utility and the Army use the same FRCS and energy delivery systems.		

The Black Energy attack pathway shows the patterns, cyber events, and behaviors that the adversary took to ultimately compromise the target systems. There are distinctive patterns to the adversary's methods that can result in easier identification of similar pathways, methods, and malware identification.

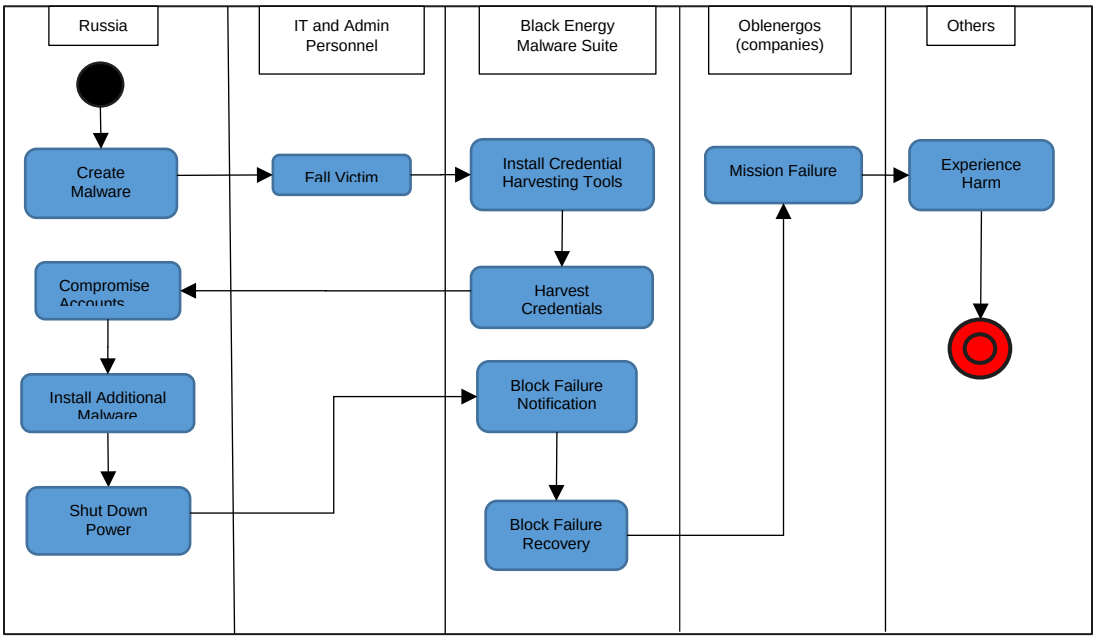


Figure 8. Black Energy Attack Pathway

Black Energy CAP provides examples of discrete, measurable cyber threat information that aligns with the adversary's attempt to take or has acted against the target to reach its goal. The

chart provides an understanding of the activities that the adversary took in preparing the attack, the engagement the adversary took before gaining unauthorized access to systems, the presence within the target systems, and the effect and consequence of the cyber-attack.

Table 9. Black Energy Cyber Activity Profile Rating—Tier V

CYBER ACTIVITY PROFILE					
STAGES	**Preparation**	**Engagement**	**Presence**	**Effect/Consequence**	**ADVERSARY CAPABILITY**
OBJECTIVES	Identification of Target (owners and operators of utility company)	Attacker establishes foothold into the utility network	Go undetected, spread through the corporate network and gain access to the OT network.	Compromise of utility operations leading to dangers to public lives and utility operations.	**ASSESSED ADVERSARY CAPABILITY LEVEL**
ACTIONS (Exemplars)	Create credential harvesting tools. Create specific targeting malware. Create spear phishing emails to specifically target owners and operators.	Attacker's installs credential harvesting tools and installed Kill disk, UPS and serial-to-ethernet disabling tools.	Reconnaissance, lateral movement, escalate privileges, and maintaining presence in the target environment.	Utility operations are compromised, leading to power shut down through HMI, failure notification route blocked, recover routes blocked, DDoS of phone systems	
INDICATORS	No indicators	Failure to use common network intrusion detection software. Lack of training to recognize phishing emails.	Failure to prioritize detection and defense against phishing emails	Operator station not operating in normal state, reboot unsuccessful, manual override of operations to restore functions	
THREAT TIER RATING	**4**	**5**	**4**	**5**	**TIER V**

LEGEND - CYBER THREAT FRAMEWORK (CTF) LEXICON					
CTF STAGE MODEL LEXICON	**STAGES (PHASES)**	**LAYER 1**	**OVERALL THREAT CLASSIFICATION (TIER RATING)**	**LEVEL I**	**LOW**
	OBJECTIVES	**LAYER 2**		**LEVEL II**	**MODERATE**
	ACTIONS	**LAYER 3**		**LEVEL III**	**SIGNIFICANT**
	INDICATORS	**LAYER 4**		**LEVEL IV**	**HIGH**
				LEVEL V	**CRITICAL**

3.5 Cyber Terrorist/Hacktivist Use Case: Ardit Ferizi

Ardit Ferizi, aka Th3Dir3torY, was sentenced to 20 years in prison after pleading guilty to accessing a protected computer without authorization in order to provide material support to the Islamic State of Iraq and the Levant through obtained information. Ferizi gained administrator-level access to a server of a victim company's website in the United States and culled personally identifiable information (PII) of approximately 1,300 United States military and government personnel. He provided this PII to Junaid Hussain, aka Abu Hussain al-Britani, a member of the Islamic State of Iraq and the Levant, with the intent to cause harm to these individuals through targeted attacks (DOJ 2016a).

For specific details regarding this incident see references as annotated in the text below.

Table 10. Ardit Ferizi Attack Summary

Adversary: Ardit Ferizi	**Adversary Type:** Activist/Terrorist	**Adversary Capability Level:** 2-3
Malware: None	**Threat Vector:** SQL Injection	
Target: U.S. military and government personnel		
Consequence: Members of Islamic State of Iraq and the Levant posted names, derived from data provided by Ferizi, as a target list putting U.S. military and government personnel at risk.		
Relevance to the Army: Demonstrates the vulnerability of protected systems to determined adversaries.		

Ardit Ferizi's attack pathway shows the patterns, cyber events, and behaviors that the adversary took to ultimately compromise the target systems. There are distinctive patterns to the adversary's methods that can result in easier identification of similar pathways, methods, and malware identification.

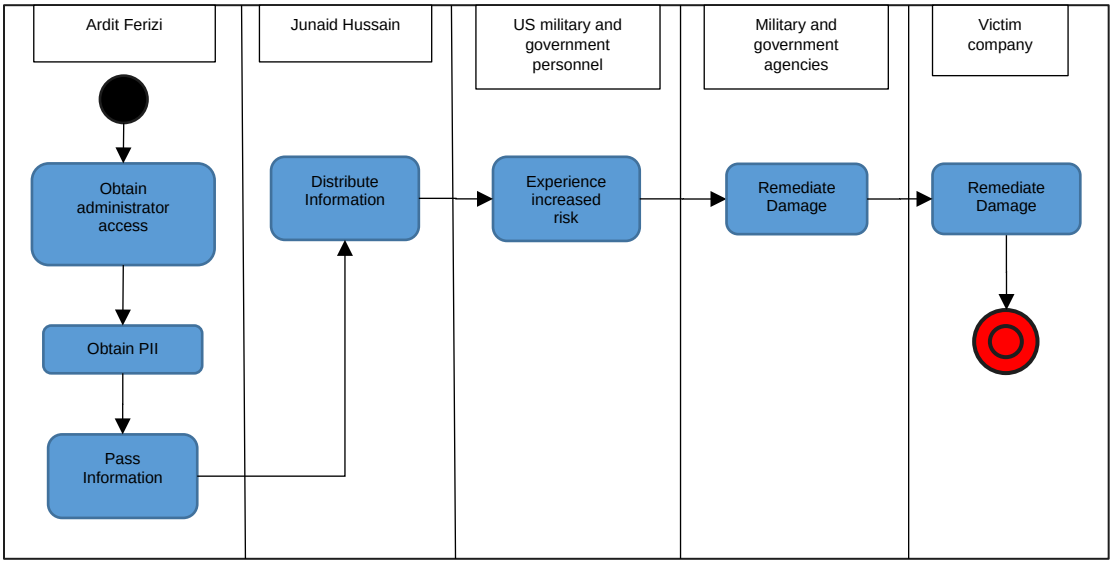


Figure 9. Ardit Ferizi Attack Pathway

Ardit Ferizi's CAP provides examples of discrete, measurable cyber threat information that aligns with the adversary's attempt to take or has acted against the target to reach its goal. The chart provides an understanding of the activities that the adversary took in preparing its attack, the engagement taken before gaining unauthorized access to systems, the presence within the target systems, and the effect and consequence of the cyber-attack.

Table 11. Ardit Ferizi Cyber Activity Profile Rating—Tier III–IV

CYBER ACTIVITY PROFILE					
STAGES	**Preparation**	**Engagement**	**Presence**	**Effect/Consequence**	ADVERSARY CAPABILITY
OBJECTIVES	Identification of target	Attacker gains access to server hosting PII	To steal as much PII as possible	Compromise military and government personnel PII	ASSESSED ADVERSARY CAPABILITY LEVEL
ACTIONS (Exemplars)	Secure credentials for access to systems	Attacker steals PII of U.S. military and government personnel information from compromised server	Deliver target list to terrorist group	Create terror and insecurity of military and government personnel	
INDICATORS	No indicators	Failure to secure compromised server	Failure to prevent data exfiltration	Expend resources to increase security, remediate damaged reputation. Experience increased risk of harm, safety concerns, expend resources to increase security	
THREAT TIER RATING	2	2	2	2	TIER II

LEGEND - CTF LEXICON					
CTF STAGE MODEL LEXICON	STAGES (PHASES)	LAYER 1	OVERALL THREAT CLASSIFICATION (TIER RATING)	LEVEL I	LOW
	OBJECTIVES	LAYER 2		LEVEL II	MODERATE
	ACTIONS	LAYER 3		LEVEL III	SIGNIFICANT
	INDICATORS	LAYER 4		LEVEL IV	HIGH
				LEVEL V	CRITICAL

3.6 Cyber Terrorist/Hacktivist Use Case: Hamid Firoozi

Hamid Firoozi, employed by the Iran-based companies ITSecTeam and Mersad Company and sponsored by Iran's Islamic Revolutionary Guard Corps, repeatedly obtained unauthorized access to the SCADA systems of the Bowman Dam in Rye, New York between August 28, 2013 and September 18, 2013. Firoozi could see the status and operation of the dam regarding water levels and temperature and the status of the sluice gate for controlling water levels and flow rates. Firoozi was only prevented from manipulating and controlling the sluice gate because the gate had been manually disconnected for maintenance at the time (DOJ 2016b).

For specific details regarding this incident see references as annotated in the text below.

Table 12. Hamid Firoozi Attack Summary

Adversary: Hamid Firoozi	**Adversary Type:** Activist/Terrorist	**Adversary Capability Level:** 3-4
Attack Vector: Distributed Denial of Service	**Threat Vector:** BotNet	
Target: Bowman Dam		
Consequence: This use case is a near miss and should not be considered an example of a properly implemented risk mitigation strategy. The intrusion occurred when the sluice gate was manually disconnected for maintenance. Luckily, the intrusion was detected before the sluice gate was reconnected.		
Relevance to the Army: The Army uses these same kinds of FRCS/OT systems.		

Hamid Firoozi's attack pathway shows the patterns, cyber events, and behaviors that the adversary took to ultimately compromise the target systems. There are distinctive patterns to the adversary's methods that can result in easier identification of similar pathways, methods, and malware identification.

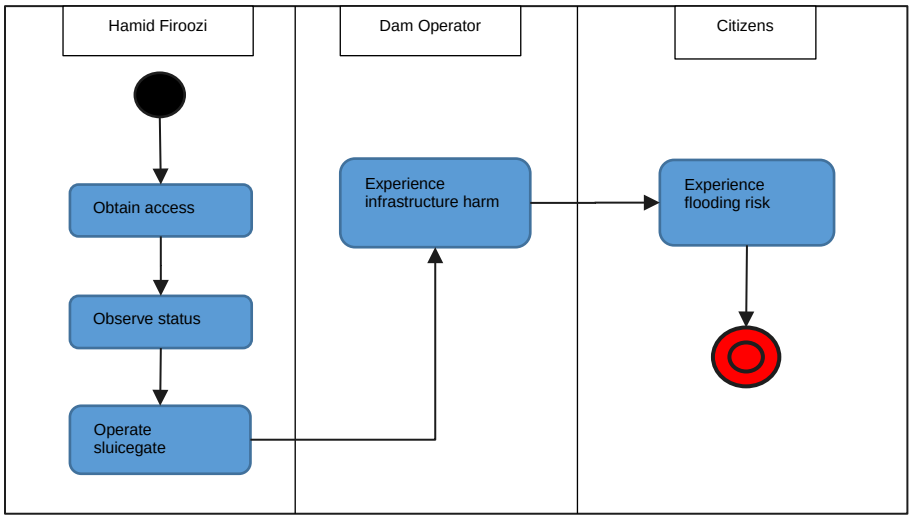


Figure 10. Hamid Firoozi Attack Pathway

Hamid Firoozi's CAP provides examples of discrete, measurable cyber threat information that aligns with the adversary's attempt to take or has acted against the target to reach its goal. The

chart provides an understanding of the activities that the adversary took in preparing the attack, the engagement taken before gaining unauthorized access to systems, the presence within the target systems, and the effect and consequence of the cyber-attack.

Table 13. Hamid Firoozi Cyber Activity Profile Rating—Tier III–IV

CYBER ACTIVITY PROFILE					
STAGES	**Preparation**	**Engagement**	**Presence**	**Effect/Consequence**	ADVERSARY CAPABILITY
OBJECTIVES	Identify potential infrastructure vulnerabilities	Secure control of infrastructure	Manifest control of infrastructure	Infrastructure and other damage (flooding)	ASSESSED ADVERSARY CAPABILITY
ACTIONS (Exemplars)	Secure tools required for access	Access SCADA systems	Observe dam operational status	Assume control of dam operations	
INDICATORS	No indicators	No indicators	Remote connections	Unauthorized operation of dam controls	
THREAT TIER RATING	2	3	1	1	TIER III - IV

LEGEND - CTF LEXICON					
CTF STAGE MODEL LEXICON	STAGES (PHASES)	LAYER 1	OVERALL THREAT CLASSIFICATION (TIER RATING)	LEVEL I	LOW
	OBJECTIVES	LAYER 2		LEVEL II	MODERATE
	ACTIONS	LAYER 3		LEVEL III	SIGNIFICANT
	INDICATORS	LAYER 4		LEVEL IV	HIGH
				LEVEL V	CRITICAL

3.7 Insider Threat Use Case: Xu Jiaqiang

Xu Jiaqiang, a Chinese national formerly of Beijing, pled guilty to economic espionage and trade secret theft for his connection to the theft of proprietary source code from his former employer. Xu worked as a developer for a U.S. company where he had access to proprietary software and its source code. Xu voluntarily resigned from the company and began communicating with two undercover law enforcement officers posing as a financial investor and project manager. Xu sent the proprietary code to the officers.

For specific details regarding this incident see references as annotated in the text below.

Table 14. Xu Jiaqiang Attack Summary

Adversary: Xu Jiaqiang (DOJ 2017)	**Adversary Type:** Insider Threat	**Adversary Capability Level:** 0
Malware: Insider Threat	**Threat Vector:** Code Theft	
Target: U.S. Company		
Relevance to the Army: This could pose a problem in supply chain risks in proprietary code for FRCS/OT systems on Army installations.		

Xu Jiaqiang's attack pathway shows the patterns, cyber events, and behaviors that the adversary took to ultimately compromise the target systems. There are distinctive patterns to the adversary's methods that can result in easier identification of similar pathways, methods, and malware identification.

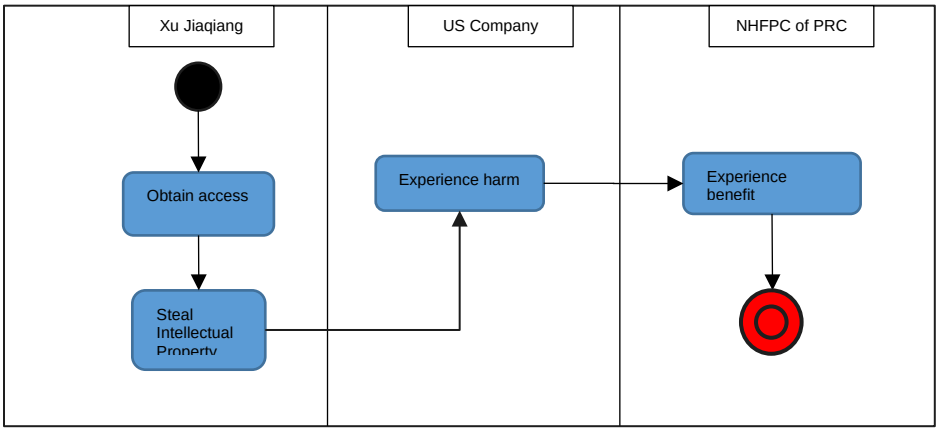


Figure 11. Xu Jiaqiang Attack Pathway

Xu Jiaqiang's CAP provides examples of discrete, measurable cyber threat information that aligns with the adversary's attempt to take or has acted against the target to reach its goal. The chart provides an understanding of the activities that the adversary took in preparing the attack, the engagement taken before gaining unauthorized access to systems, the presence within the target systems, and the effect and consequence of the cyber-attack.

Table 15. Xu Jiaqiang Cyber Activity Profile Rating—Tier I

CYBER ACTIVITY PROFILE					
STAGES	**Preparation**	**Engagement**	**Presence**	**Effect/Consequence**	**ADVERSARY CAPABILITY**
OBJECTIVES		Profit from release of proprietary code	Profit from release of proprietary code	Profit from release of proprietary code	ASSESSED ADVERSARY CAPABILITY LEVEL
ACTIONS (Exemplars)	Insider obtains access to proprietary code	Insider agrees to sell code			
INDICATORS	Possible indicators of Compromise (spending, erratic behavior, data access, etc).	Few	Unauthorized information release may be detected	Target organization harmed by unauthorized information release	
THREAT TIER RATING	**1**	**1**	**1**	**1**	**TIER I**

LEGEND - CYBER THREAT FRAMEWORK (CTF) LEXICON					
CTF STAGE MODEL LEXICON	**STAGES (PHASES)**	**LAYER 1**	**OVERALL THREAT CLASSIFICATION (TIER RATING)**	**LEVEL I**	**LOW**
	OBJECTIVES	**LAYER 2**		**LEVEL II**	**MODERATE**
	ACTIONS	**LAYER 3**		**LEVEL III**	**SIGNIFICANT**
	INDICATORS	**LAYER 4**		**LEVEL IV**	**HIGH**
				LEVEL V	**CRITICAL**

4.0 Estimated Cost to Secure Systems

The Army's capability to protect FRCS requires Army Energy and U.S. Department of Defense management commitment to implement and maintain cost-effective cybersecurity based on risk management of perceived threats that result in unacceptable risk to FRCS critical assets.

This section provides a brief description of the return on investment implementing a stand-alone FRCS network and first-year cost estimate for implementing security controls to protect the stand-alone FRCS. While implementation cost can greatly vary depending on a FRCS size, complexity, and scope of services, the provided cost estimate ranges based on subject matter expertise take into consideration the various skill sets needed to implement a FRCS secure stand-alone network. This work is based on previous work for Army DCS G-9.

The cost estimates in Section 4.1 and 4.2 are not cumulative to the Army. Both estimates are presented to reinforce the complexity of the problem when securing FRCS.

4.1 Total Cost of Implementing the Risk Management Framework from the 2017 Cost-Benefit Analysis

In 2017, a cost estimate was performed to implement the Risk Management Framework for FRCS on 150 Army installations. The estimates were for three distinct but overlapping courses of action (COA).

COA 1: Discover, assess, and remediate cybersecurity vulnerabilities in 100 critical assets (buildings) across 24 installations.

COA 1 Cost: $71.6M

COA 2: COA 1 and any DoDIN-connected FRCS. Not knowing how many systems are connected to the Department of Defense Information Network (DoDIN), we assume half of the facilities in COA 3 will be found to either reside on the DoDIN or use the same physical transport medium. Therefore, we assume all the costs included in COA 1 and approximately half of the costs of COA 3.

COA 2 Cost: $630.4M

COA 3: Discover, assess, and remediate all Army-owned FRCS. This estimate used a population size of 150,000 buildings.

COA 3 Cost: $1,268.0M

See Appendix C for a list of criteria and assumptions used in the 2017 cost-benefit analysis.

4.2 Full-Time Equivalent Estimation to Implement Risk Management Framework Security Control Policies per Installation

This section addresses the staffing requirements associated with implementing the security controls for a stand-alone FRCS network at an installation. The level of effort, measured in full-

time equivalent (FTE) hours, needed to implement security controls for stand-alone FRCS networks is derived from the staffing requirements to perform the roles and responsibilities outlined in DoDI 8510.01 *Risk Management Framework*. An FTE is defined as 2,000 hours per year.

Table 16 shows the roles needed to implement security controls for a stand-alone FRCS network on small, medium, and large installations. Not all roles will be needed at every installation. Specific criteria to choose between two or three FTEs for a small installation or three to four FTEs for a medium installation is not identified in this report. The installation models were taken from the 2017 cost-benefit analysis work and validated through the Deputy Chief of Staff G-9 office. While Deputy Chief of Staff G-9 recognizes that these models were not perfect, they serve as a consistent measure for ongoing FRCS cyber estimates.

Table 16. FTE Roles Alignment to Army Installations

	Roles	**Army Installation FTEs by Size**			
		Small (2 FTEs)	Medium (3 FTEs)		Large 5 (FTEs)
A	Project Manager	A	A	A	A
B	Information Assurance Manager				B
C	Information System Security Officer	C	C	C	C
D	Security Engineer	D	D	D	D
E	System Administrator			E	E

4.3 Determine a Rough Estimate for an Installation's Cost to Secure

This section helps the reader determine how many FTEs are needed on a specific installation based on the model detailed in Appendix D. See Appendix D for more information on the installation size models used in this report.

Step 1: Using Table 17, determine whether your installation is small, medium, or large.

Table 17. Installation Size by Number of Buildings

Number of Buildings	**Small**	**Medium**	**Large**
Range	<999	1,000-2,249	2,250+
Mode	555	1,500	2,250

Step 2: Using Table 16, determine how many FTEs and what roles are needed to secure the assessed installations FRCS.

A dollar amount can be determined using the General Services Administration estimate of $226.18 per hour for Analyst 2 contractors and the installation models described in Appendix C (GSA ND). Table 18 shows that the total number of FTEs needed to secure 155 installations is between 359-507.

Table 18. FTE Range for All Department of Public Works Cybersecurity Personnel Needed

Installation Size	Number of Installations	FTEs Required IAW Table 9	Total FTEs
Small	125	2–3	250–375
Medium	23	3–4	69–92
Large	8	5	40
		Result:	359–507 FTEs

The total cost estimate for Department of Public Works (DPW) cybersecurity personnel needed can be determined by multiplying the FTE range from Table 18 by the General Services Administration Analyst 2 labor rate.

$$CybersecurityPersonnelCostMIN = 359\ FTEs * \$226 = \$162{,}397{,}240 \quad (1)$$

$$CybersecurityPersonnelCostMAX = 507\ FTEs * 226 = \$229{,}346{,}520$$

Figure 12 shows the labor range in dollars for all FTEs needed by the Army.

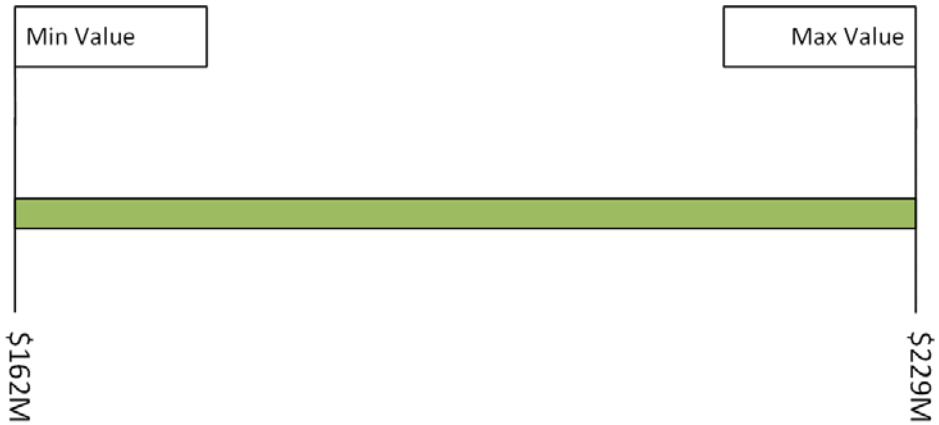


Figure 12. Estimated FTEs in Dollars

Figure 13 summarizes the calculation to estimate the number of FTEs and annual cost to secure FRCS for a given installation. Installation managers can use Figure 14 to estimate the number of annual labor hours and annual cost to secure an installation's FRCS.

(# of FTEs)*(2,000) : (# of FTEs)*(2,000)*($226)

_____ : _____

Annual Labor Hours | Annual Cost

Figure 13. Equation to Estimate FTEs and Annual Cost of Installation Securing FRCS

For example, a manager of a small installation of only 800 buildings determines that three FTEs are needed to secure his/her FRCS. The number of FTEs would be used in Figure 13 as demonstrated in Figure 14.

(# of FTEs)*(2,000) : (# of FTEs)*(2,000)*($226)

3 * 2,000 = 6,000 : 3 * 2,000 * 226 = $1,356M

Annual Labor Hours | Annual Cost

Figure 14. Example of Installation-Level Annual Labor and Annual Cost Estimate

5.0 Estimated Cost Savings of Preventing Cyber-Attacks

For an installation, the consequences of a cyber-attack on FRCS can be costly and negatively affect the installation's mission. This section attempts to determine the value of the Army's FRCS. First, the value of the installation's mission is qualitatively determined by the reader. Then, the cost of a cyber-attack is quantified by estimating the total FRCS asset valuation for 150,000 Army-owned buildings. The information provided is based on an inventory of three installations.

5.1 Mission Value

Army missions are executed when the perceived benefits exceed the perceived costs. Mission benefits can be assessed in monetary terms, but non-monetary benefits can greatly eclipse the monetary benefits. Army missions are executed to advance U.S. geo-political interests and objectives. These interests and objectives are rarely expressed in monetary terms. Security, support of our allies, reduction in conflict, and international stability are difficult objectives to assign a dollar value. Likewise, individual facilities, assets, or missions throughout and across the Army hierarchy have qualitative or operational value beyond their replacement cost or monetary value. In conjunction with the asset valuation described in the balance of this section, it is recommended that assets be evaluated for qualitative, operational, and other non-monetary value. Some relatively low-cost assets can be critical to mission success. A comprehensive valuation of any given asset must include some qualitative assessment of its importance relative to Army missions. As a factor in the resource determination of an FRCS cybersecurity program, consider the qualitative mission value or the cost of mission failure or degradation due to the impact a cybersecurity attack could have on a critical facility.

5.2 Asset Valuation

PNNL used the inventory data from 31 buildings to estimate the total asset valuation of FRCS for an estimated 150,000 Army-owned buildings. The 150,000-building estimate was provided to PNNL by the Army. The inventory data set is not an ideal representation of Army-owned FRCS given the sample size is only 0.021% of the estimated population size.

The known inventory devices were searched in vulnerability and exposure databases to determine if known vulnerabilities existed. Nineteen unique vulnerabilities were found for the data set of 129 devices. The search criteria were limited to the specific make and model of the device. Other attributes such as operating system, software libraries, major applications, device firmware, and protocols were not researched. It is highly likely that 19 unique vulnerabilities for the sample data set is a lower-bound estimate.

The inventory data set contained 129 devices, of which 89 were unique devices. The cost to replace each device was determined using market research. Table 19 shows the minimum, maximum, median, and average device values for the data set after removing the outliers.

Table 19. Device Values per Building for the Sample Data Set with the Outliers Removed

	Minimum	Maximum	Median	Average
Sample Data Set	$400	$32,540	$6,075	$7,710

A model of buildings found on Army installations was constructed using the inventory data. The model in Figure 15 shows the minimum, median, mean, and maximum values of the FRCS in 150,000 buildings for all data and for the data set after outliers have been removed. Outliers were determined by identifying building FRCS values that were two standard deviations from the data set's mean value.

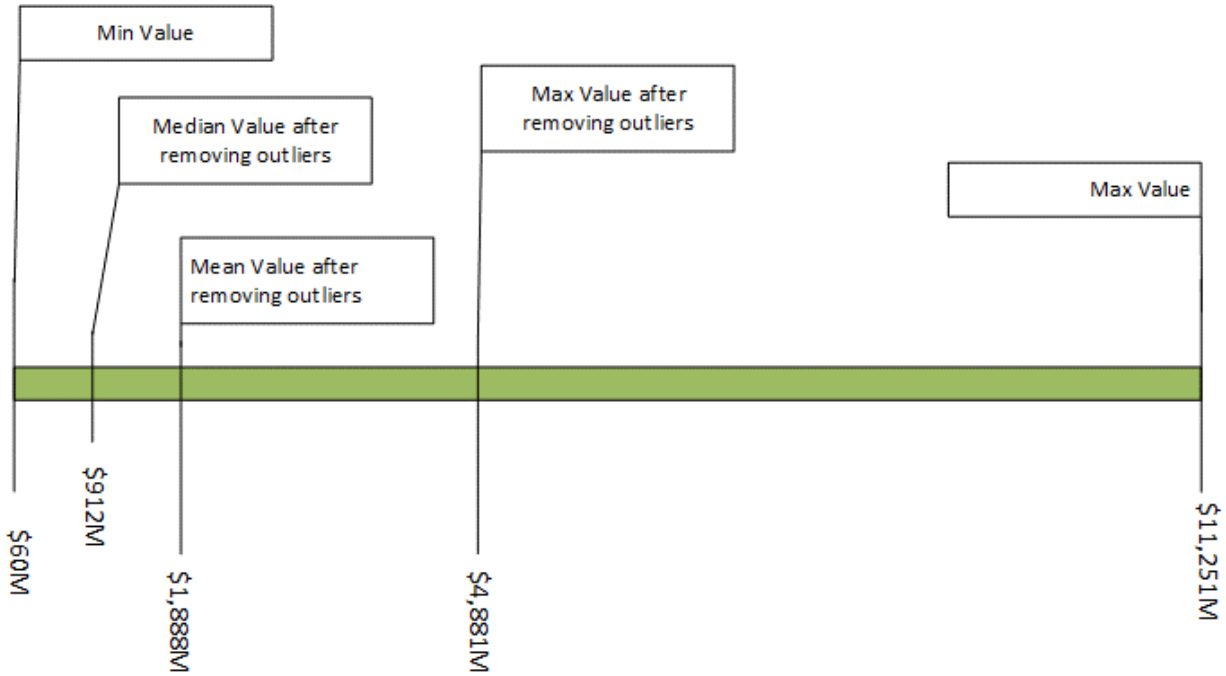


Figure 15. Estimated Minimum, Maximum, Median, and Mean Values of the Total FRCS in 150,000 Buildings

The estimated maximum value of all FRCS for 150,000 buildings after removing the outliers from the data set is $4,881M. The estimated minimum value did not change. These numbers were determined using 0.021% of the data from the estimated population size.

For use in resource planning, it is recommended to use the asset valuation estimates with the outliers removed. The minimum value of all Army FRCS is estimated at $60M. The maximum value of all Army FRCS is estimated at $4,881M.

5.3 Determine a Rough Estimate for an Installation's Asset Valuation

This section helps the reader determine a rough FRCS asset valuation for a specific installation based on the analysis of known inventory data detailed in Appendix D. Figure 16 presents Steps 1-4 as an equation the reader can use to determine minimum, likely, and maximum FRCS values for a given installation.

Step 1: Determine the number of buildings on the installation.

Step 2: Multiply the number from Step 1 by $400 to determine the minimum value of FRCS for the assessed installation.

Step 3: Multiply the number from Step 1 by $7,710 to determine the most likely value of FRCS for the assessed installation.

Step 4: Multiply the number from Step 1 by $32,540 to determine the maximum value of FRCS for the assessed installation.

Step 5: Consider the value of the installation's mission and how FRCS in critical facilities support that mission.

(# of BLDG)*(400) : (# of BLDG)*(7,710) : (# of BLDG)*(32,540)

_____: _____: _____

MIN Likely MAX

Figure 16. Equation to Estimate the Range of FRCS Value for a Given Installation

Building on the example in Section 4.3, the same installation manager estimates the value of all FRCS assets in the 800 buildings on their installation as demonstrated in Figure 17.

(# of BLDG)*(400) : (# of BLDG)*(7,710) : (# of BLDG)*(32,540)

800 * 400 = $320,000 : 800 * 7,710 = $6,168,000 : 800 * 32,540 = $26,032,000

MIN Likely MAX

Figure 17. Example Estimate of FRCS Value for 100 Buildings

6.0 Conclusion

Cyber-attacks on organizations using the same equipment or similar operating environments as Army FRCS are happening right now. Known vulnerabilities exist on equipment used by the Army. It is not known whether those vulnerabilities have been mitigated by a compensating control at the installation level.

The list of inventory data was searched in vulnerability and exposure databases to determine if known vulnerabilities existed. Nineteen unique vulnerabilities were found for the 129 devices. The search criteria were limited to the specific make and model of the device. Other attributes such as operating system, software libraries, major applications, device firmware, and protocols were not researched. Therefore, this number is a lower-bound estimate.

Readers can estimate the cost to secure in FTEs using the process described in Section 4.3. Figure 16 summarizes the equation for determining the number of FTEs needed on a given installation and notional cost in dollars using General Services Administration's labor rates. The number of FTEs can be determined using Table 18 from Section 4.2.

$$\frac{(\#\ \text{of FTEs})*(2{,}000)}{\text{Annual Labor Hours}} : \frac{(\#\ \text{of FTEs})*(2{,}000)*(\$226)}{\text{Annual Cost}}$$

Figure 18. Equation to Estimate the FTEs and Annual Cost of Securing FRCS for a Given Installation

Readers can estimate the asset value of all FRCS on a given installation by using the process described in Section 5.3. Figure 19 summarizes the equation for estimating the value of all FRCS for a given installation.

$$\frac{(\#\ \text{of BLDG})*(400)}{\text{MIN}} : \frac{(\#\ \text{of BLDG})*(7{,}710)}{\text{Likely}} : \frac{(\#\ \text{of BLDG})*(32{,}540)}{\text{MAX}}$$

Figure 19. Equation to Estimate the Range of FRCS Value for a Given Installation

All estimates to secure Army FRCS are included in Table 20. The 2017 cost-benefit analysis only covers the discovery, assessment, and remediation of FRCS assets and the initial Risk Management Framework authority to operate. The FTE estimates do not cover hardware, software, or other security services that may be needed to fully implement a cybersecurity program.

Table 20. Summary of Cost to Secure Estimates

	Name	Estimate (in millions)
2017 CBA	COA 1	$71.6
	COA 2	$630.4
	COA 3	$1,268.0
FTEs	FTE Min	$162.4
	FTE Max	$229.3

The estimated minimum value of all FRCS devices in 150,000 Army-owned buildings is $60M. The absolute maximum value for FRCS is estimated at $11,251M, with a likely maximum value of $4,888M. These values do not capture the value of the mission at each installation.

Figure 20 compares all cost to secure estimates from Section 4 with the FRCS asset valuation estimates from Section 5. All the costs to secure estimates are below the likely maximum value of FRCS assets.

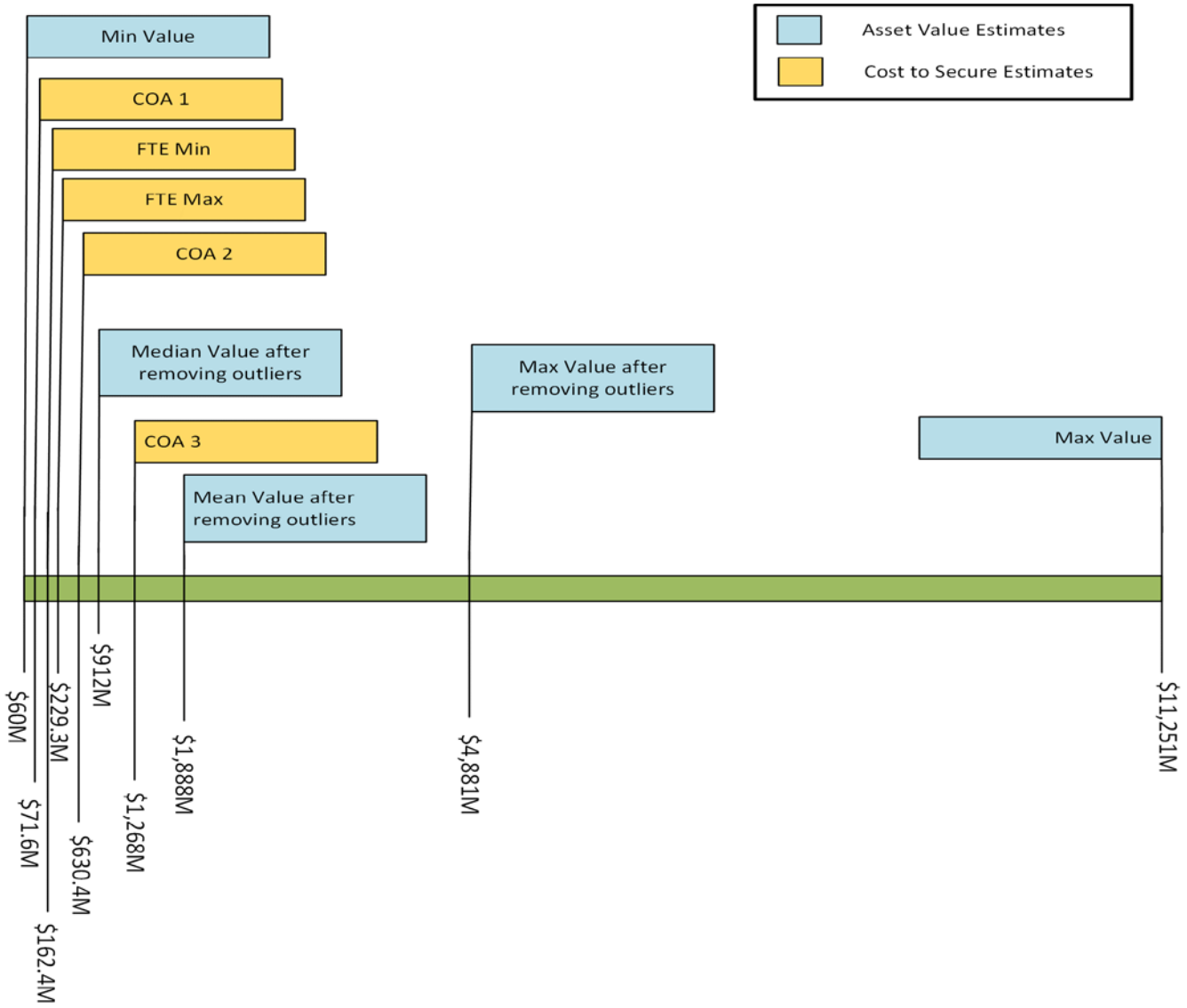


Figure 20. Comparison of FRCS Asset Valuation and Cost to Secure Estimates

7.0 References

CISA. 2019. “HatMan—Safety System Targeted Malware (Update B),” MAR-17-352-01. Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security. Accessed January 22, 2020 at https://www.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf

Denning DE. “Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.” Chapter 8 in (J. Arquilla and D. Ronfeldt (eds) *Networks and Netwars. The Future of Terror, Crime, and Militancy*.” RAND Corporation, Santa Monica, CA.

DoD. 2013. *Resilience Military Systems and the Advanced Cyber Threat*, Task Force Report. Defense Science Board, U.S. Department of Defense, January 2013. Accessed January 22, 2020 at https://dsb.cto.mil/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf

Dogrul M, A. Aslan, and E Celik. 2011. “Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism.” In *Proc. Of 3rd International Conference on Cyber Conflict*.

DOJ. 2016a. “ISIL-Linked Hacker Sentenced to 20 Years in Prison.” Department of Justice, U.S. Attorney’s Office. Accessed January 22, 2020 at https://www.justice.gov/usao-edva/pr/isil-linked-hacker-sentenced-20-years-prison

DOJ. 2016b. “Manhattan U.S. Attorney Announces Charges against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities.” Department of Justice, U.S. Attorney’s Office. Accessed January 22, 2020 at https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated

DOJ. 2017. “Chinese National Pleads Guilty to Economic Espionage and Theft of a Trade Secret from U.S. Company.” Department of Justice, U.S. Attorney’s Office. Accessed January 22, 2020 at https://www.justice.gov/usao-sdny/pr/chinese-national-pleads-guilty-economic-espionage-and-theft-trade-secret-us-company

Pfleeger CP. 2008. "Reflections on the Insider Threat." In (eds. Stolfo SJ, Bellovin SM, Hershkop S, Keromytis AD, Sinclair S, and Smith S.) *Insider Attack and Cyber Security: Beyond the Hacker*, pp. 5-16. Springer, Boston.

GSA. ND. “Authorized Federal Supply Schedule Price List: Professional Engineering Services.” General Services Administration. Accessed January 22, 2020 at https://www.gsaadvantage.gov/ref_text/GS23F0081K/GS23F0081K_online.htm

ICS-CERT. 2014a (rev 2018). “ICS Focused Malware,” ICS Advisory, ICSA-14-178-01. Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security. Accessed January 22, 2020 at https://www.us-cert.gov/ics/advisories/ICSA-14-178-01

ICS-CERT. 2014b (rev 2018). “ICS Focused Malware,” ICS Advisory, ICSA-14-178-02A (update to ICS-CERT 2014a). Cybersecurity and Infrastructure Security Agency, U.S.

Department of Homeland Security. Accessed January 22, 2020 at https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-176-02A.

Langner R. 2013. *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. The Langner Group. Accessed January 22, 2020 at https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

MITRE. 2017a. "Sandworm Team." Modified March 2019. Accessed January 22, 2020 at https://attack.mitre.org/groups/G0034/

MITRE. 2017b. "BlackEnergy." Modified June 2019. Accessed January 22, 2020 at https://attack.mitre.org/software/S0089/

MITRE. 2019. "TEMP.Veles." Created April 16, 2019, Updated April 29, 2019. Accessed January 22, 2020 at https://attack.mitre.org/groups/G0088/

MITRE. ND. "Groups." Accessed January 22, 2020 at https://attack.mitre.org/groups/

NCCIC and FBI. 2016. "GRIZZLY STEPPE—Russian Malicious Cyber Activity," JAR-16-20296A. Joint Analysis Report from the U.S. National Cybersecurity and Communications Integration Center and U.S. Federal Bureau of Investigation. Accessed January 22, 2020 at https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

NJCCIC. 2017. "Havex." New Jersey Cybersecurity and Communications Integration Cell. Accessed January 22, 2020 at https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/havex

NJCCIC. 2017. "Stuxnet." New Jersey Cybersecurity and Communications Integration Cell. Accessed January 22, 2020 at https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet.

ODNI. 2018a. A Common Cyber Threat Framework Lexicon of Concepts and Definitions, July 17, 2018. Office of the Director of National Intelligence. Accessed January 22 22, 2020 at https://www.odni.gov/files/ODNI/documents/features/Cyber_Threat_Framework_Lexicon_20180718.pdf

ODNI. 2018b. A Common Cyber Threat Framework: A Foundation for Communication." Office of the Director of National Intelligence. ODNI, 13 Mar. 2017. Accessed January 22, 2020 at https://www.dni.gov/files/ODNI/documents/features/Threat_Framework_A_Foundation_for_Communication_short_version.pdf

Rogers M. 2003. "The Psychology of Cyber-Terrorism." Chapter 4 in (ed: A. Silke) *Terrorists, Victims and Society: Psychological Perspectives on Terrorism and Its Consequences*. John Wiley & Sons LTD.

Zager R. and J. Zager. ND. "ODNI Common Cyber Threat Framework: A New Model Improves Understanding and Communications." *Small Wars Journal*.

Appendix A – Detailed Description of FRCS Cybersecurity Profile

To better inform the Army of the adversary threat landscape to an Army installation, Pacific Northwest National Laboratory (PNNL) tailored a commonly accepted technical cyber lexicon (ODNI 2018a) from the Cyber Threat Framework (CTF) that closely aligns with industry definitions and other U.S. government agencies, partners, and stakeholders in discussing adversary activities throughout the adversary threat life cycle.

The adversary threat landscape addresses the attack scenarios that may affect Army facility-related control systems (FRCS). Known previous attacks are characterized and aligned with cyber behavior associated with the FRCS Cyber Adversary Model presented here. The adversary tier levels described in this appendix are derived from the Department of Defense, Defense Science Board (DoD 2013). The follow-on adversarial stages aligned with cyber threat descriptions and the cyber activity profile presented in this section are tailored from the Director of National Intelligence Cyber Threat Framework (CTF) (ODNI 2017).

A Common Cyber Threat Framework: A Foundation for Communication (Cyber Threat Framework) is a cybersecurity analytical framework published by the Office of the Director of National Intelligence. The Office states that, “its principle benefit being that it provides a common language for describing and communicating information about cyber threat activity” (Zager and Zager ND). The Cyber Threat Framework stage model creates a four-layer hierarchy.

As illustrated in Figure A.1, the Stages layer is the foundation of the Cyber Threat Framework. Building from Stages, PNNL adapted the CTF lexicon definitions of the four adversary activity stage terms as follows (Zager and Zager ND):

- **Preparation:** Activities undertaken by a threat actor, his/her leadership, and/or sponsor to prepare for conducting malicious cyber activities, e.g., establish governance and articulating intent, objectives, and strategy; identify potential victims and attack vectors; secure resources and develop capabilities; assess intended victim's cyber environment; and define measures for evaluating the success or failure of threat activities.
- **Engagement:** Threat actor activities taken before gaining but with the intent to gain unauthorized access to the intended victim's physical or virtual computer or information systems, networks, and/or data stores.
- **Presence:** Actions taken by the threat actor once unauthorized access to victim’s physical or virtual computer or information system has been achieved that establishes and maintains conditions or allows the threat actor to perform intended actions or operate at will against the host physical or virtual computer or information system, network, and/or data stores.
- **Effect/Consequence:** Outcomes of threat actor actions on a victim's physical or virtual computer or information systems, networks, and/or data stores.

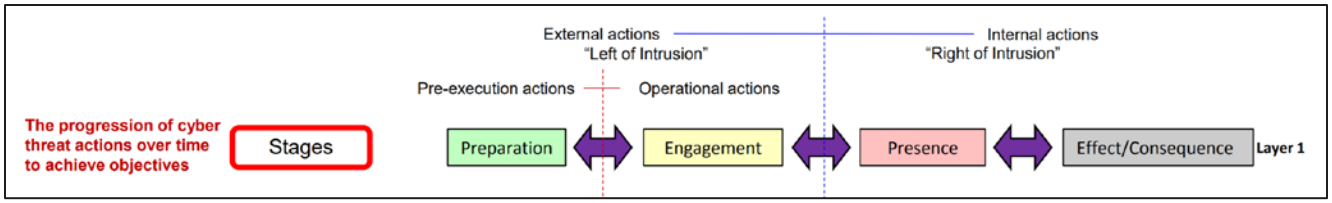


Figure A.1. Cyber Threat Framework Adversary Stage Activity

The Stages bind the other layers (Objectives, Actions, and Indicators) to time, forcing a sequential analysis of cyber threats, as shown in Figure A.2. The four stages are divided into major divisions, Left of Intrusion and Right of Intrusion, in Figure A.1. Although not expressly stated, the boundary between Left of Intrusion and Right of Intrusion (which occurs between Preparation and Engagement) is Intrusion. Intrusion is an important threat transition because pre-intrusion defensive interventions are preventative while post-intrusion defenses are remedial. Similarly, Left of Intrusion is divided into two distinct phases: Pre-Execution actions, which occur in the Preparation Stage, and Operational Actions, which occur during the Engagement Stage.

Adversary characteristics can be identified by the tactics, techniques, and procedures that are used when launching a cyber-attack. A correlation of adversary tactics, techniques, and procedures information can be shown to align with deployed networked devices managed by the Department of Public Works. This section outlines identified adversarial cyber-enabled attack scenarios based on known characteristics of archetype threat activities (i.e., advanced persistent threats, terrorist/hacktivism, and insider threats). Recognizing the stages, objectives, actions, and indicators associated with Cyber Threat Framework Adversary Stage Activity in Figure A.2 can better protect the Army's mission by applying cybersecurity controls and procedures to assets that are critical to an installation's operational readiness.

The FRCS Cyber Adversary Model's hierarchical structure follows a simplified, non-technical threat progression that permits the Army to objectively map diverse models to a commonly accepted standard. Aligning a common approach helps to:

- Establish a shared ontology and enhance information sharing because it is easier to maintain mapping of multiple models to a common reference than directly to each other
- Characterize and categorize threat activity in a straightforward way that can support missions ranging from strategic decision making to analysis and cybersecurity measures and users from generalists to technical experts
- Support common situational awareness across organizations

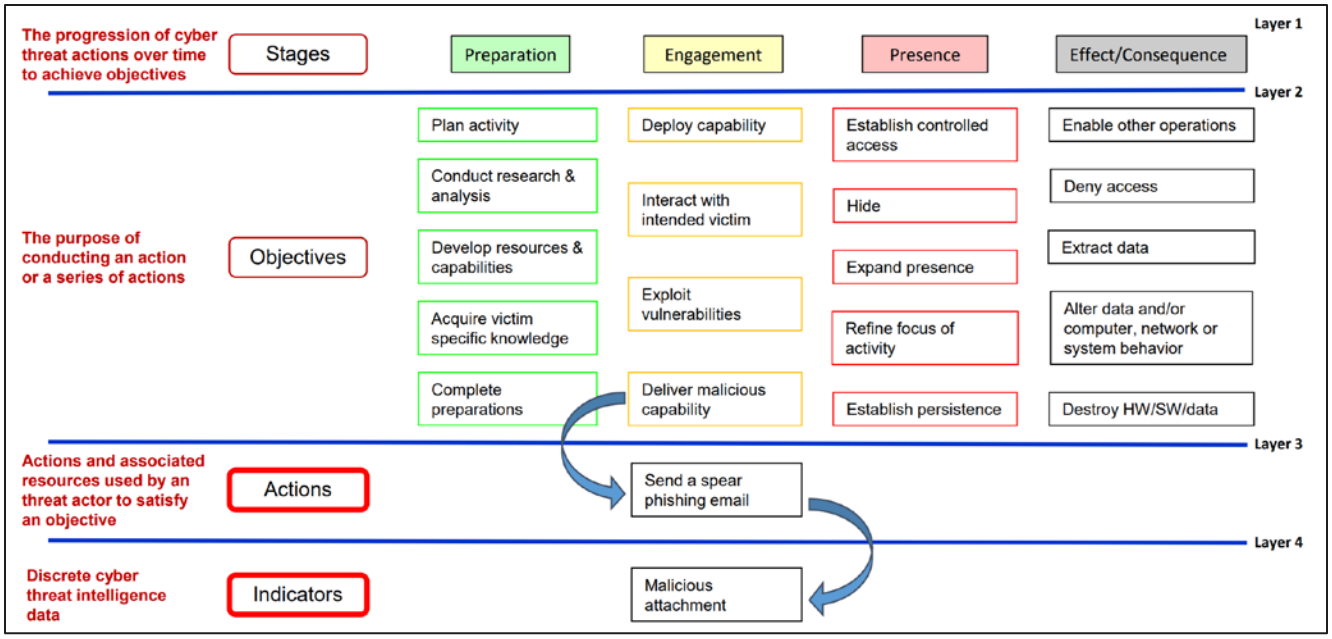


Figure A.2. Cyber Threat Framework Stage Model

Rather than defining “cybersecurity” or “cyberspace,” the Cyber Threat Framework defines cyber threats (activities), how these threats progress over time, and the consequences of these threats.

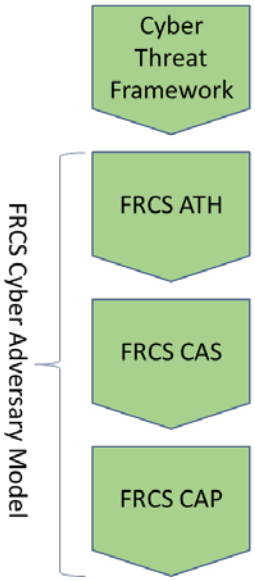
A.1 Caveats

The Cyber Threat Framework abstracts cyber threats from particular technologies, focusing on the attacker’s methodologies, not specific malware vulnerabilities (Zager and Zager ND).

The Cyber Threat Framework acknowledges that cyber threats can result from users being persuaded by threat actors to act on behalf of threat actors (Zager and Zager ND). In the Cyber Threat Framework, users are the nascent agents of the threat actors, waiting to fall victim to psychological manipulation (Zager and Zager ND).. The Cyber Threat Framework supports the characterization and categorization of cyber threat information using standardized language. The Cyber Threat Framework categorizes the activity in increasing layer” of detail (1–4) as available in the intelligence reporting.

A.2 FRCS Cyber Adversary Model

The Cyber Threat Framework was used to adapt and modify the FRCS Cyber Adversary Model comprising three sections: FRCS Adversary Tier Hierarchy, FRCS Cyber Adversarial Stages, and a FRCS Cyber Activity Profile. By applying the FRCS Cyber Adversary Model, installations can forecast adversary activities, understand the adversary’s motivations and behavior, and better prepare installations’ FRCS against failures due to differing levels of a cyber-attack. The threat tiers introduced in this report can be used to analyze the stages of each cyber threat, the preparation activities of the adversary, the engagements of the adversary, the effects or consequences of an attack, and the indicators of compromise of FRCS systems. Figure A.3 describes the cyber adversary model process used to characterize the attack scenarios in Section 3.0.



Purpose	Outcome
• Informs the FRCS Cyber Adversary Model.	• Provides common lexicon to communicate information about cyber attacks. • Provides criteria for measuring cyber attacks.
• Provides a Threat Description tailored from the Cyber Threat Framework for each Tier Classification.	• Establishes criteria for Objectives, Actions, and Indicators. • Aligns Objective, Actions, and Indicators with Tier Classifications.
• Provides a description for the Cyber Threat Framework Stages for each Tier Classification.	• Establishes criteria for Preparation, Engagement, Presence, and Effect/Consequence for Tier Classification.
• Establishes a methodology for profiling specific cyber attacks.	• Characterized specific cyber attacks. • Assigns a Tier Classification to a specific cyber attack.

Figure A.3. FRCS Cyber Adversary Model Process

A.3 FRCS Adversary Tier Hierarchy

The FRCS Adversary Tier Hierarchy is a comprehensive and foundational understanding of the posed threats to FRCS on an installation. Table A.1 provides a threat description tailored from the CTF for each tier classification. Table A.1 also provides a high-level functional summary for each tier and assigns a relative cost to the adversary required to participate at each tier. The objectives of the adversary are outlined throughout each tier with defined knowledge and tools that an adversary uses in its attack. The actions include the target resources that an adversary incorporates throughout the attack life cycle. The indicators provide definitions of the access that an adversary needs to gain a foothold and the traversal pathway that the adversary will take to identify and gain access to FRCS systems.

Table A.1. FRCS Adversary Tier Hierarchy

FRCS Adversary Tier Hierarchy (ATH)					
			Objectives	Actions	Indicators
Tier Classification	**Threat Description**	**Function**	**Attack Methods (Knowledge and Tool)**	**Target Resource (Technology and Process Knowledge)**	**Access Needs and Motivation (Foothold and Traversal)**
Level V	State-sponsored, nation state Tiers V encompass threat actors who can go beyond malicious software inserted through Internet access, and instead, create and identify vulnerabilities in otherwise well-protected systems.	Creates vulnerabilities using full spectrum (Billions)	If desired, surgical attacks targeting a specific facility, process, or function are possible. Often, the payload is designed to target low-level processes, making it difficult to disrupt or identify.	Established successful mechanism for gap jumping in addition to capabilities to cross the FRCS boundary. In many cases, the gap jumping may involve targeting the supply chain, for example, that eliminates the need to cross the FRCS boundary. Conducts sophisticated supply chain operations that result in the introduction of implants into the most hardened government and military facilities, cause a disruption or delay to mission-critical systems or affects mission readiness.	The threat actor exploits the physics of the technology and processes to cause catastrophic damage.
Level IV	Tier IV encompasses actors who can adapt and use available malicious software to gain a foothold in otherwise well-protected systems.	Discovers unknown vulnerabilities (billions)	Demonstrated capability to conduct FRCS attacks against a variety of targets (i.e., countries, sectors, technologies, etc.)	Highly capable of determining and understanding the technology, people, and processes in use at a target facility.	Demonstrate a capability for limited gap jumping and the ability to effectively traverse the FRCS boundary. May also rely on supply chain operations, such as targeting FRCS systems during upgrade and maintenance cycles in order to introduce implants.
Level III					

FRCS Adversary Tier Hierarchy (ATH)					
			Objectives	Actions	Indicators
Tier Classification	**Threat Description**	**Function**	**Attack Methods (Knowledge and Tool)**	**Target Resource (Technology and Process Knowledge)**	**Access Needs and Motivation (Foothold and Traversal)**
Level II	Tier III actors employ a broad range of software capabilities to penetrate FRCS systems and employ exploits through internet access. A major distinction between Tiers II and III is scale—Tier III threat actors implement asymmetric tactics, techniques, and procedures, characterized by well-organized groups. Tier III actors aim to cause deliberate damage.	Discovers unknown vulnerabilities (Millions)	Some capability for the disruption of FRCS environment exists. In many cases, the target of interest is widely deployed, resulting in widely distributed but surgical attacks. Rely on the use of commercially available tools and exploit kits (e.g., Metasploit, Glegg's SCADA+)	Able to conduct enough reconnaissance on and off the target environment.	Possess some capability to successfully traverse the FRCS boundary, but cyber operations are likely to originate from the IT side, using traditional exploitation methods (e.g., spear phishing, escalation of privileges, etc.)

FRCS Adversary Tier Hierarchy (ATH)					
			Objectives	Actions	Indicators
Tier Classification	Threat Description	Function	Attack Methods (Knowledge and Tool)	Target Resource (Technology and Process Knowledge)	Access Needs and Motivation (Foothold and Traversal)
	Tier II actors employ a broad range of software capabilities to penetrate FRCS systems and effect exploits through internet access. Tier II actors have the potential to cause inadvertent damage.	Exploits pre-existing known vulnerabilities (tens of thousands)	Disruption and destructive capabilities can focus on specific industrial control systems (ICSs) or supervisory control and data acquisition (SCADA) equipment or their associated communication protocols, but the actual attacks involve the manipulation of legitimate functions (as in Level 1). For example, malware may be designed that puts ICS equipment into upgrade mode, but no malicious firmware is developed to brick the device. Some functionality is lost as a result of the attack, but it may be recoverable.	Cyber concept of operations reflects some understanding of the ICS/SCADA mechanics in place, but manipulation or exploitation of these devices occurs with little understanding of the consequence or impact.	Initial infection vectors typically include spear phishing attacks to gain access to information technology infrastructure after which implants are used to target ICS/SCADA infrastructure/components that are available within the information technology space.
Level I	Tier I actors	Exploits pre-existing known	Manipulation of FRCS equipment	Capable of determining what	Access capabilities are very limited and may be

FRCS Adversary Tier Hierarchy (ATH)					
			Objectives	Actions	Indicators
Tier Classification	Threat Description	Function	Attack Methods (Knowledge and Tool)	Target Resource (Technology and Process Knowledge)	Access Needs and Motivation (Foothold and Traversal)
	have some ability to change pre-existing malicious code, and their actions may be characterized by pursuit of specific objectives to exploit known vulnerabilities. Low-tier actors can employ some very sophisticated tools and techniques developed and exposed by others.	vulnerabilities (tens of thousands)	is possible, but these attacks generally involve the manipulation of legitimate engineering or operator functions (e.g., opening breakers from a human-machine interface designed for that function).	is deployed in the target space but display little to no understanding of the technology, systems, processes, or physics used. Reconnaissance efforts on target are extensive and often include publicly available network enumeration and credential collection tools.	dependent on publicly available exploitation kits or malware. Initial infection vector primarily originates from a spear phishing campaign on the network.
Level 0	Actors may not currently possess the sophisticated tools, techniques, or skill necessary to execute a cyber-attack that could cause an unknown or unpredictable widespread or significant impact to FRCS systems. Tier 0 actors are driven as much by the desire to brag about their success in executing an attack as they are to cause specific damage.	Opportunity (tens of thousands)	Some knowledge of information technology or web hacking but no ICS-specific knowledge.	Some knowledge of information technology or general digital equipment but no ICS-specific knowledge.	Access capabilities, if present, are restricted to the information technology domain.

Level V: State-sponsored, nation state: encompasses threat actors who can go beyond malicious software inserted through internet access and instead create and identify vulnerabilities in otherwise well-protected systems.

Level IV: Encompasses actors who can adapt and use available malicious software to gain a foothold in otherwise well-protected systems.

Level III: Encompasses actors who employ a broad range of software capabilities to penetrate FRCS systems and employ exploits through internet access. These threat actors implement asymmetric tactics, techniques, and procedures, characterized by well-organized groups, and aim to cause deliberate damage.

Level II: Encompasses actors who employ a broad range of software capabilities to penetrate FRCS systems and effect exploits through internet access and have the potential to cause inadvertent damage.

Level I: Encompasses actors who have some ability to change pre-existing malicious code; their actions may be characterized by pursuit of specific objectives to exploit known vulnerabilities. Low-tier actors can employ some very sophisticated tools and techniques developed and exposed by others.

Level 0: Encompasses actors that may not currently possess the sophisticated tools, techniques, or skill necessary to execute a cyber-attack that could cause an unknown or unpredictable widespread or significant impact to FRCS systems. Tier 0 actors are driven as much by the desire to brag about their success in executing an attack as they are to cause specific damage.

A.4 FRCS Cyber Adversarial Stages

The FRCS Cyber Activity Profile in Table A.2 can be used to characterize the stages of a cyber threat to include the preparation activities of the adversary, the engagements of the adversary, the presence of the adversary, and the effects or consequences of an attack on FRCS. The definitions are outlined to include each step taken to compromise an FRCS.

Table A.2. FRCS Cyber Adversarial Stages

	FRCS Cyber Adversarial Stages			
Tier Classification				
Level V	Warehousing malicious cyber capabilities in/on threat actor internally owned or externally acquired storage locations, whether as electronic media or physical hardware (i.e., removable media, bundled hardware/firmware/software corrupted through a cooperative supply chain) for future deployment, and issuing final instructions to	Electronic or physical activities that expose malicious content to the intended victim that results in a physical or electronic presence but which does not activate the	Steps taken by the threat actor (electronically or physically) to preserve, obfuscate, or increase his/her footprint or capabilities on a victim's computers, information systems, and/or	Permanently, completely, and irreparably damage a victim's physical or virtual computer or information systems, networks, and/or data stores, e.g., system administrators discover permanent, unexplained damage to portions of the information system, system users discover data/files have been

Tier Classification	FRCS Cyber Adversarial Stages			
	those that will conduct the planned malicious activity	malicious content, e.g., send an email to the intended victim with malicious attachment or distribute removable media containing malware.	networks, e.g., additions to or modification of the existing operating system or enterprise capabilities, such as Windows software services, Master Boot Record, or the implant of additional malicious software.	inappropriately corrupted or deleted.
Level IV	Steps taken by the threat actor before gaining access to an intended victim's computers, information systems, networks, and/or data stores, but just before execution of the planned cyber activity, to gather through physical/electronic observation (i.e., port scanning) or social media surveys, the latest details on the activities, characteristics, resources and perceived vulnerabilities of the intended victim to validate/confirm final planning assumptions	Steps taken to leverage deficiencies, vulnerabilities, gaps, and/or shortfalls (e.g., zero-day exploits, malicious SQL injections, cross-site scripting) in the intended victim's computers, networks, and/or information systems to try to gain unauthorized access.	Steps taken by the threat actor confirm the existence and validity of the intended victim's data, information, and/or system capabilities, and/or identify additional potential victims and their data, computers, and/or information systems, and that the available malicious tools/processes will achieve the intended outcome/results.	
Level III	Steps taken by the threat actor to secure the requisite resources (funding, people), and acquire the capabilities (technology, processes, tools, infrastructure) and partnerships necessary for conducting the planned cyber threat activity and for ascertaining its success/ failure in achieving the desired objectives/outcomes	Steps taken to leverage deficiencies, vulnerabilities, gaps, and/or shortfalls (e.g., zero-day exploits, malicious SQL injections, cross-site scripting) in the intended victim's computers,	Steps taken by the threat actor confirm the existence and validity of the intended victim's data, information, and/or system capabilities, and/or identify additional potential victims and their data, computers, and/or information	Steps taken by the threat actor to change the behavior/outcomes/and interaction (violate the integrity) of the victim's computer(s), information system(s), and/or network(s).

Tier Classification		FRCS Cyber Adversarial Stages		
		networks, and/or information systems to try to gain unauthorized access.	systems, and that the available malicious tools/processes will achieve the intended outcome/results.	
Level II	Steps taken by a threat actor before conducting malicious cyber activity to define intent; establish policy limitations; identify funding; coordinate intended activities; establish initial objectives and parameters for measuring progress/success toward meeting them; and the steps taken to update plans, activities, and requirements based on insights gained during the eventual victim engagement	Steps taken to position malicious content for operational employment, e.g., place corrupted firmware in commercial products.	Activities (automated or manual) intended to gain unauthorized control (violate the confidentiality) of the intended victim's computers, information systems, and/or networks to allow the threat actor to direct or conduct enabling or malicious activity.	Steps taken by the threat actor to temporarily deny, degrade, disrupt, or destroy access to, or to encrypt for ransom (violate the availability) a victim's physical or virtual computer or information system, network, communications capabilities, and/or data stores.
Level I	Opportunistic/Plan activity	Steps taken to position malicious content for operational employment, e.g., place corrupted firmware in commercial products.	Activities (automated or manual) intended to gain unauthorized control (violate the confidentiality) of the intended victim's computers, information systems, and/or networks to allow the threat actor to direct or conduct enabling or malicious activity.	Measurable cyber threat activities that indicate, identify, and/or establish a foundation for (to include the conduct of effects assessments) subsequent actions against a victim's data, computers and/or information systems, e.g., establish a command and control node or hop point, incorporate the victim's computer/information systems in a botnet, or exfiltrate user password and/or credentials. Analytic judgments or assessments are not included.

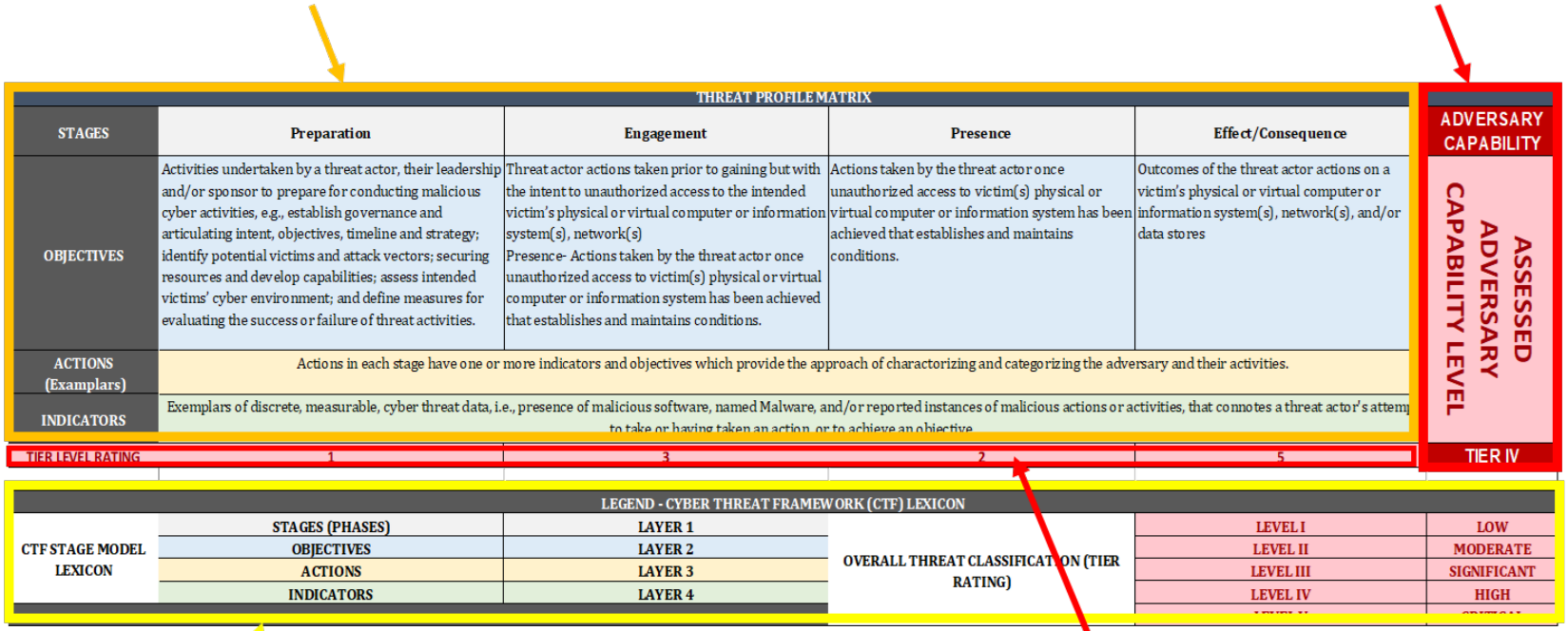
A.5 FRCS Cyber Activity Profile

Using the FRCS Cyber Activity Profile template in Figure A.4 is an important process to identify the stages that an adversary will take to compromise critical systems on an installation and a tool to provide documented evidence of each stage of an attack. Additionally, definitions are

included in each stage of the FRCS cyber adversary process so that when personnel input information into the FRCS cyber adversary profile datasheet, this information can provide an understandable profile that can be used by any installation no matter the size. It is commonly known that understanding the adversary allows users to better protect their systems. Some attacks cannot be predicted, but installation managers can use this type of intelligence to be better prepared for future attacks. The FRCS cyber adversary profile is a scorecard for cyber-attacks to easily compare the levels of sophistication among varying cyber incidents.

FRCS CAS: Stage alignment of attack details with Cyber Threat Framework metrics modified for FRCS.

FRCS ATH: Cumulative Tier Classification Determination for attack.



THREAT PROFILE MATRIX					
STAGES	Preparation	Engagement	Presence	Effect/Consequence	ADVERSARY CAPABILITY
OBJECTIVES	Activities undertaken by a threat actor, their leadership and/or sponsor to prepare for conducting malicious cyber activities, e.g., establish governance and articulating intent, objectives, timeline and strategy; identify potential victims and attack vectors; securing resources and develop capabilities; assess intended victims' cyber environment; and define measures for evaluating the success or failure of threat activities.	Threat actor actions taken prior to gaining but with the intent to unauthorized access to the intended victim's physical or virtual computer or information system(s), network(s) Presence- Actions taken by the threat actor once unauthorized access to victim(s) physical or virtual computer or information system has been achieved that establishes and maintains conditions.	Actions taken by the threat actor once unauthorized access to victim(s) physical or virtual computer or information system has been achieved that establishes and maintains conditions.	Outcomes of the threat actor actions on a victim's physical or virtual computer or information system(s), network(s), and/or data stores	ASSESSED ADVERSARY CAPABILITY LEVEL
ACTIONS (Examplars)	Actions in each stage have one or more indicators and objectives which provide the approach of charactorizing and categorizing the adversary and their activities.				
INDICATORS	Exemplars of discrete, measurable, cyber threat data, i.e., presence of malicious software, named Malware, and/or reported instances of malicious actions or activities, that connotes a threat actor's attem to take or having taken an action, or to achieve an objective				
TIER LEVEL RATING	1	3	2	5	TIER IV

LEGEND - CYBER THREAT FRAMEWORK (CTF) LEXICON					
CTF STAGE MODEL LEXICON	STAGES (PHASES)	LAYER 1	OVERALL THREAT CLASSIFICATION (TIER RATING)	LEVEL I	LOW
	OBJECTIVES	LAYER 2		LEVEL II	MODERATE
	ACTIONS	LAYER 3		LEVEL III	SIGNIFICANT
	INDICATORS	LAYER 4		LEVEL IV	HIGH

FRCS CAP Legend.

FRCS ATH: Tier Classification Determination for attack by Stage of the attack.

Figure A.4. FRCS Cyber Activity Profile Template

A.6 References

DoD. 2013. *Resilience Military Systems and the Advanced Cyber Threat*, Task Force Report. Defense Science Board, U.S. Department of Defense, January 2013. Accessed January 22, 2020 at https://dsb.cto.mil/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf

ODNI. 2018a. A Common Cyber Threat Framework Lexicon of Concepts and Definitions, July 17, 2018. Office of the Director of National Intelligence. Accessed January 22 22, 2020 at https://www.odni.gov/files/ODNI/documents/features/Cyber_Threat_Framework_Lexicon_20180718.pdf

ODNI. 2018b. A Common Cyber Threat Framework: A Foundation for Communication." Office of the Director of National Intelligence. Accessed January 22, 2020 at https://www.dni.gov/files/ODNI/documents/features/Threat_Framework_A_Foundation_for_Communication_short_version.pdf

ODNI. Cyber Threat Framework. 2017. Office of the Director of National Intelligence. Accessed January 22, 2020 at https://www.dni.gov/index.php/cyber-threat-framework

Zager R. and J. Zager. ND. “ODNI Common Cyber Threat Framework: A New Model Improves Understanding and Communications.” *Small Wars Journal*.

Appendix B – Adversary Characteristics

Adversary models are crucial in the field of cybersecurity as they are used to better understand the tactics, techniques, and procedures of varying threats to facility-related control systems (FRCSs). Adversaries have varying degrees of capabilities and each of the customized models define the different types of attackers, their skill sets, and the advantages and disadvantages that pose different setbacks to FRCS and installations.

B.1 Advanced Persistent Threat

Cyber activity characterization of an advanced persistent threat (APT) actor's behavior varies across the cyber-attack continuum. While adversary capabilities and motivation (e.g., ideology) can vary, APTs, terrorists, or a lone wolf can all emulate high-critical threat activity. APT actors are recognized in the industry as the most capable cyber threat archetype, but this is a misconception. Because of the complexity of sense-making tasks across multiple cyber systems, specifically cyber archetype attribution within the cyber operational environment, the authors created FCRS-specific models to serve as the foundation for future automation and augmentation within analysis workflows, cybersecurity organizational function, decision making, and information sharing. While the FCRS Cyber Threat Framework describes APT threat activity elements, analysts and decision makers cannot assume there is one cyber tactic, technique, and procedure that definitively describes APT actor activity; rather, a culmination of data provides the evidence to convey threat activity impact and assessed cyber archetype attribution (lone wolf, terrorist, or APT).

B.1.1 Methods

Strategic and operational trend analysis reporting, typically the output of a cyber threat intelligence organizational function, serves as a primary source for APT adversary capability assessments. Like state actors, cyber APT actors typically warehouse and maintain advanced cyber campaign capabilities. In some instances, APT actor groups maintain hybrid forces consisting of state actor and non-state actor associated (criminal elements and terrorists) resources. In this example, organizations might observe threat behaviors across Tiers 1-5. However, APTs work to achieve their goals at the lowest levels to save effort, time, and funding. Simply put, an APT would not waste a zero-day attack when a known attack vector would achieve the same objective.

B.1.2 Profile and Motivation

APT actor motivations are most often observed through non-cyber means but can inform an organization's cyber defense strategy. Unlike the terrorist or lone wolf cyber archetype, APT actor objectives and intent are often characterized over time and their signatures are observed forensically. While cyber archetype intent is difficult to observe, considering external cyber operational environment factors (e.g., geopolitics and business intelligence considerations) infuses additional rigor into cyber risk management planning. These signatures can also serve as early indicators and warnings for specific APT activity detection and asset risk prioritization.

Certain indicators summarized in Tiers 3–5 of the FRCS Adversary Tier Hierarchy, for instance, describe some examples of an APT-related actor activities. Because cyber threat actors typically conduct parallel processes, the FRCS Adversary Tier Hierarchy serves as a reference

guide for assessing cyber archetype attribution and likelihood of threat impact based on a culmination of multiple data elements.

Rather than focusing on cyber archetype attribution, the authors focus on describing examples of cyber threat activities unique to each actor for future FCRS adversary capability assessments.

B.1.3 Deterrence

APTs can be delayed and detected. They can even be mitigated against with redundant systems and mature recovery plans. However, APTs cannot be deterred.

B.2 Cyber Terrorists and Hacktivists

Cyber terrorism is frequently misunderstood, often because it lacks a concise, agreed-upon definition. Further complicating matters, hacktivist attacks and other cyber crimes are often mislabeled as cyber terrorism, and thus the establishment of a clear definition is necessary before examining the topic in full. *Cyber terrorism* can be defined as an illicit, politically motivated act by an individual, nation-state, or non-state actors that uses computer, network, internet, and information and communication technologies to obstruct political, social, and/or economic operations among a group, organization, and/or government (FBI 2007, Rogers 2003). These acts are intended to intimidate or coerce civilians and governments and create significant disturbances or fear, involving the same motivation found in traditional terrorism (Tafoya 2011). Cyber terrorist attacks involve harm against property or persons or cause enough damage to generate widespread fear and terror while also using computers as weapons or as targets (Dogrul et al. 2011, Cavelty MD 2008, Theohary and Rollins 2015). Cyber terrorism can take the form of attacks against hospitals, schools, businesses, homes, and financial institutions, attacks against critical infrastructure (including financial services sector, the electrical grid, dams, water treatment facilities, electoral systems, etc.), or the dissemination of personally identifiable information for malicious political or ideological causes. A real-world example of such an attack occurred when an attacker gained access to the supervisory control and data acquisition system of a New York dam. Upon gaining control, the individual was able to acquire information on the status and operation of the dam. The attacker was unable to control the dam's sluice gate only because the system was under maintenance (DOJ 2018). Put simply, cyber terrorism intends to generate fear and terror in civilians, cause economic damage, and/or destroy public and private infrastructure (Hua and Bapna 2012, Denning 2001).

If the definition of cyber terrorism is expanded to include broader terrorist activities that use the internet, acts such as online propaganda, recruitment, and material support of terrorist activities can also be considered cyber terrorism. Thus, the definition of cyber terrorism may also include not only cyber terrorist attacks themselves but also the wide-ranging use of the internet by terrorists (Dogrul et al. 2011).

Cyber-attacks are separate from cyber terrorism, mainly in terms of intent and destruction. A cyber-attack can include cyber terrorist and hacktivist attacks but also include the actions taken by cyber criminals. Cyber-attacks can include a large range of activities that use information and communications technology to achieve malicious goals, often with a financial or ideological motivation (Theohary and Rollins 2015).

Cyber terrorism differs from information warfare in that cyber terrorism involves premeditated, politically motivated attacks against systems, programs, and data by sub-national or clandestine

agents or other individuals who perpetuate malicious acts against innocent targets (Theohary and Rollins 2015). Information warfare is a planned attack by nations or agents against information and computer systems, programs, and data that causes enemy losses. While information warfare involves certain targets in war, cyber terrorism is intended to cause terror and damage to all those in a targeted locality (Dogrul et al. 2011, Theohary and Rollins 2015). Unlike cyber terrorism, cyber warfare targets military or other strategic assets with civilian harm being labeled as collateral damage (Rogers 2018).

Hacktivism is another term that is often incorrectly used interchangeably with cyber terrorism. Hacktivism intends to "disrupt, disable, or control computer systems, or steal the data they contain" (Denning 2001) while also supporting a certain political, social, or religious cause, often in opposition to government policies. Hacktivism is carried out by non-state actors with the goal of disrupting targets in order to bring awareness to their ideological cause and differs from cyber terrorism in this regard. Hacktivism can thus be thought of as an "aggressive form of contentious politics and civil disobedience" (Denning 2001) where the intent is to upset, embarrass, disrupt, or inconvenience the target (Webber and Yip 2018). Hactivism can include activities such as web sit-ins, virtual blockades and distributed denial of services attacks, automated email bombs, web hacks, computer break-ins, computer viruses, and worms (Plachkinova and Vo 2019). Hacktivist activities intend merely to disrupt or upset their target without extensive damage in order to further their ideological goals. While both hacktivism and cyber terrorism are politically motivated, computer-generated, and perpetrated against a computer target, they differ significantly in intent and destruction (Kenney 2015). For example, cyber terrorism intends to cause extensive damage to infrastructure in order to further ideological goals and spread fear among civilians or coerce governments. The intention behind the cyber terrorists' attack is to achieve a political, social, or religious goal and the effect must be damaging enough to create fear that is comparable to traditional terrorist acts (Kenney 2015).

Hacktivism and cyber terrorism represent two separate categories, but the boundaries between them remain somewhat vague. An individual can be both hacktivist and cyber terrorist, for example, and definitional differences may cause one to label an attack as hacktivism while others may label it as cyber terrorism. This problem is exacerbated by the fact that cyber terrorism lacks a universally accepted definition (Theohary and Rollins 2015). The comparatively benign acts by hackers have often been incorrectly identified as cyber terrorism. We must distinguish between the potential and actual damage created by cyber terrorists from the acts of hacktivists who merely intend to disrupt rather than spread widespread panic, fear, and destruction (Weimann 2005).

B.2.1 Methods

Terrorist organizations use the internet to commit a wide variety of terrorist activities, such as creating plans for future attacks; raising and laundering funds; spreading propaganda; communicating with other members; sharing information and knowledge with other terrorist groups; implementing command and control; conducting research; recruiting new members (UNODC 2012); creating international support; and gathering intelligence (Theohary and Rollins 2015, Weimann 2005). The internet is an effective platform for conducting these activities because of its anonymity, connectivity, ease of access, potential for large-scale damage, psychological impact, media attention (Weimann 2005), the capability for wide advertising and public relations, the ability to attack varying targets on a global scale, and the potential impact on vulnerable infrastructure (Rogers 2003).

Because cyber-attacks typically require fewer people and fewer resources and because of their ability to target a large number of victims, cyber terrorism may be a more attractive route than traditional terrorism (Albahar 2019, MacDonald 2015). Cyberspace also allows terrorists to remain anonymous and absent from the physical location of the attack and provides a large pool of poorly protected targets. Thus, they can launch remote, anonymous attacks with greater ease (Seissa et al. 2017). These remote attacks require less physical training, psychological investment, mortality risks, and travel, which then may lead to an increased ability to recruit members (Weimann 2005, MacDonald 2015). Because of their ability to use proxy servers and IP-change-methods, cyber terrorists can easily conceal their identities from government agents, complicating the ability to trace and arrest them (Hua and Bapna 2012. When the attack is followed through, it can be executed quickly and without any physical barriers or checkpoints to evade (Dogrul et al. 2011, Weimann 2005).

Cyberspace allows terrorists to achieve a far-reaching audience and provides access to a larger number of targets (Klein 2015). Traditional terrorist acts, such as bombings, are restrained to specific physical locations, while cyber terrorists can potentially create much larger and damaging effects (Dogrul et al. 2011). One of the key components of terrorism is the fear generated by the attacks. By bringing as much attention as possible to the attacks, the terrorists' message can be heard by a wide audience (Rogers 2003). Because they are given a wider audience and a larger scope of attack, cyber terrorists may gain greater leverage when attempting to achieve their political goals compared to traditional terrorists (Dogrul et al. 2011). Cyber terrorism has an increased ability to directly affect a large number and variety of people, potentially leading to more extensive media coverage and thus a greater spread of their agenda (Weimann 2005).

B.2.2 Profile and Motivation

Because of the difficulties in identifying and creating a profile of the cyber terrorist, it is necessary to look at the broader profile of terrorists in general to draw conclusions. However, there is currently no consensus on a singular, general terrorist profile. Motivations for becoming a terrorist and carrying out terrorist acts, as well as the personality traits of terrorists, vary significantly among individual offenders. Some studies have posited that terrorists are action-oriented, aggressive, and tend to seek excitement and stimulation. Such individuals rely on externalization and splitting. Externalization involves looking outside oneself to find the source of problems, while splitting is the tendency to split and project weaknesses that the individual dislikes onto others. Terrorists and terrorist groups tend to be motivated by future outcomes, looking to the future rather than the past or present. Because the present is often tumultuous for their group, looking to the future outcomes of changing government policy, gaining sovereign independence, or achieving other goals greatly reinforces their actions (Rogers 2003).

Terrorists tend to be highly motivated by their religion or ideology and a sense of injustice. They generally want to enact mass damage in order to attract the largest amount of media attention and spread their message to a large audience. Some studies have indicated that terrorist membership is influenced by radicalism, perceived disenfranchisement, a need for excitement and thrill, and a need for meaningfulness and glory. This gives the individuals a sense of identity as part of a larger, important group (Rogers 2018).

Bandura's social cognitive theory states that individuals tend not to participate in behavior that violates their moral standards, as violating their morals would cause self-condemnation and self-sanctions. Self-regulatory mechanisms (known as moral disengagement) will not operate until activated, and thus there are many ways that moral reactions can be divorced from the immoral

behavior. Terrorists must use moral disengagement to justify their violent attacks and use mechanisms to conduct such disengagement. These mechanisms include vilifying the victim ("the victim deserves the attack"), dehumanizing the victim (stereotyping), describing actions in euphemistic language (such as "defeating one's enemies"), claiming a moral purpose ("it is the will of God" or "I will enact revenge"), misconstruing consequences ("no innocents will be affected"), and diffusing responsibility through group membership (Rogers 2003).

Terrorists generally do not suffer from mental illness in a way that is distinguishable from the normal population (Rogers 2018). Terrorists are often mislabeled as psychopaths or mentally unstable, when they are often calculating, rational, and neurotypical (Rogers 2003). Thus, terrorists often have a level of psychological instability that is comparable to the general population. Even in instances where a terrorist shows evidence of mental illness, this is insufficient as a sole causal explanation for their attacks (Corner and Gill 2017).

Psychopathy is often thought of as a disorder experienced by terrorists. Psychopathy can be broken into two conditions: clinical illness and personality disorder. One with clinical illness is unable to distinguish right from wrong, while those with a personality disorder can. Based on this information, it can be determined that most terrorists are not psychotic. Moreover, terrorists are very rarely sociopathic, and there is currently no evidence that conclusively shows any antisocial tendencies among terrorists. By their communities, terrorists are sometimes regarded as heroes who receive popular support. These individuals often believe they are prosocial and benefiting society, and thus they are often altruistic rather than antisocial, psychopathic, or sociopathic Hua and Bapna 2012.

Socioeconomic and educational backgrounds of terrorists are varied (Rogers 2018). Many terrorists have high levels of education, including university and professional backgrounds (Alzoubaidi et al. 2016). Most terrorists likely come from middle-class backgrounds, and one study found that Palestinian support for terrorism against Israeli civilians was found more commonly in professionals than in laborers and more common among individuals with secondary education than in illiterate individuals. Another study found that 71 percent of self-identified terrorists had some form of college education and 43 percent had professional backgrounds. These findings may indicate that terrorists tend to be highly educated and knowledgeable about information and communications technology (Hua and Bapna 2013).

It should be noted that these characterizations are those of traditional terrorists, and therefore, further research must be conducted to determine if cyber terrorists' profile and motivation match those of traditional terrorists.

B.2.3 Deterrence

Deterrence theory assumes that all people are rational agents who make rational decisions to maximize benefits and minimize costs. When the benefits of an illicit activity outweigh the cost of punishment, the individual will decide to commit the criminal act. Thus, deterrence theory posits that deterring criminal behavior involves increasing the perceived costs of committing the criminal behavior and decreasing the benefits. This theory indicates that increasing punishment should theoretically deter terrorists. However, punishment may not be an effective deterrence for terrorists or even ordinary criminals. Instead, increasing the probability of being tracked and captured could prove to be a better deterrent. Moreover, it may be incorrect to assume that all potential criminals are rational and make pure cost-benefit analyses when making decisions. Cyber criminals' perception of the probability of identification and the probability of punishment

is likely skewed and more complicated than expected (Hua and Bapna 2012). These matters all complicate deterrence of cyber terrorist activities.

While cyber terrorists likely fear punishment, such punishment can only occur if the offender can be identified, traced, and prosecuted. If cyber terrorists do not think they will be identified, then they will not be deterred by increased punishment severity. The major effects of deterrence are perhaps more affected by identification probability rather than punishment severity. Therefore, increasing the ability to track and identify cyber terrorists is likely a better deterrent than increasing punishment (Hua and Bapna 2012). However, tracking terrorists is also difficult, perhaps more so than increasing penalty severity. Cyber terrorists have three main methods to avoid tracking: spoofing media access control and IP addresses; using a public internet; and using proxy servers (Hua and Bapna 2012).

Before meaningful progress can be made, national and international laws must be coordinated to make hacking and cyber terrorist attacks universally forbidden in every country. International laws, norms, and definitions do not adequately address cyber terrorism and exasperate the effects through the creation of a gray area that can be abused by cyber terrorists. However, before such coordination can take place, there must be a common, agreed-upon definitions of cyber threats and cyber terrorism (Dogrul et al. 2011).

B.2.4 Social Learning

Social learning theory suggests that individuals learn deviant behavior from others through association, definitions, differential reinforcement, and imitation. These mechanisms of social learning theory are used by cyber terrorist groups to assist in attacks and recruitment (Awan 2017). Because hacking and terrorism are included in the category of deviance, differential association can be used to understand such deviant acts (Rogers 2018).

Cyber terrorist groups use a flattened hierarchical model with a loose, decentralized network of people with flexible structures and associations. They are reliant on social connections for the coordination and completion of attacks, and affiliations are flexible and dynamic and consist of many different members conducting different attacks and for a variety of motives (Rogers 2018).

B.3 Insider Threats

An insider is a trusted individual who is currently or was formerly given legitimate, authorized access, privilege, or knowledge to an organization's information system, data, or network. An insider threat represents the destructive acts an insider may commit (Greitzer et al. 2008, Probst et al. 2010). These acts result in breeches of confidentiality, data integrity, system integrity, system survivability, identity management, accountability, etc. (Neumann 2010). In 2015, 92 percent of organizations claimed they had experienced data security incidents in the past 12 months, 74 percent of which were conducted by insiders (Liu et al. 2018).

Insider threats can be either malicious or non-malicious, resulting from actions that are intended or unintended, respectively. The more destructive insider threat abuse can include such acts as espionage, terrorism, sabotage, extortion, bribery, embezzlement, and corruption, while other abuses can include "copyright violations, negligent use of classified data, fraud, unauthorized access to sensitive information, and illicit communications with unauthorized recipients" (Greitzer et al. 2008). Whether the threat is intentional or unintentional, the insider will likely deviate from typical behavior (Liu et al. 2018). It should be noted that non-malicious insider

activity makes up the majority of threats, while malicious insiders are the small minority (Pfleeger 2008).

An insider can include:

- An employee, student, or member of the host institution that has the legitimate access and ability to operate a computer system
- An associate, contractor, business partner, supplier, computer maintenance technician, guest, etc. with business relations with the host institution
- Any individual who has authorization to perform certain activities, such as a customer who accesses his or her account using the institution's system
- An individual who has been properly identified and authenticated, including a masquerader or an individual an insider has granted access
- An individual who has been coerced by an outsider to perform actions against his or her will
- A former insider who did not have access and credentials revoked upon leaving the institution (Pfleeger 2008)

Malicious insiders intentionally abuse their privileged access to their organization's network, system, and data, and these abuses affect the confidentiality, integrity, and/or availability of the organization's information and information and communications technology infrastructures. Malicious insiders' attacks can range from data manipulation, data destruction, data theft, fraud, blackmail, and embezzlement. They may steal credit card information, sell intellectual property, or release sensitive, classified, or other protected information. Sometimes the precursor to malicious attacks are non-malicious or benign incidents (Willison and Warkentin 2013). Another type of insider is the masquerader who impersonates an individual with legitimate access using a compromised computer or stolen credentials (Liu et al. 2018).

An insider threat can also be a legitimate user who unintentionally makes a mistake. Unintentional insiders may commit attacks because of carelessness, lack of motivation, or poor training. Four characteristics of unintentional and non-malicious insider security violations include intentional behaviors, self-benefiting without malicious intent, voluntary rule-breaking, and potential to cause damage. Some examples include those who fail to shred sensitive documents, encrypt data, make data backups, change passwords, or choose strong passwords. These insiders may be knowingly breaking security rules but without malicious intent (Willison and Warkentin 2013).

B.3.1 Methods

Insiders tend to differ from external attackers in their attack signatures. Insiders can obtain physical access to their victim systems, eliminating the need to use specialized attack methods. Moreover, intrusion detection systems can detect many external attack patterns but often cannot detect the more subtle insider attacks (Schultz 2002).

An insider attacker must have the capability, motive, and opportunity to commit the attack—commonly referred to as the *CMO Model*. Another model states that insiders must have the skills, knowledge, resources, authority, and motives to attack (Schultz 2002). If any of these factors are missing, the insider will not successfully complete the attack. Thus, thwarting one or all these factors could prove to be effective in deterring insider threats.

Moreover, one study on insiders found that most attacks observed were technologically unsophisticated, with 61 percent using simple methods such as user commands, information exchanges, and exploitation of physical security. The remaining 39 percent used sophisticated methods such as using scripts and programs, autonomous agents, toolkits, flooding methods, probing, scanning, and spoofing (Wall 2013).

In the same study, 87 percent of insiders performed undetected technical precursors (action, event, or condition that uses computer or electronic media before the act) before their attack. Technical precursors included downloading and using hacker tools, failing to create backups, failing to document systems and software, accessing coworkers' or customers' systems without authorization, sharing passwords or requesting others' passwords, accessing the system after termination, unacceptable internet access during work, and setting up and using backdoor accounts (Moore et al. 2008).

B.3.2 Profile and Motivation

Identifying a unified profile of the insider attacker is likely not possible because of the variance in motivation and psychological dispositions (Pfleeger 2008). However, most malicious insiders show personal dispositions that influence their likelihood of committing sabotage. These predispositions can help explain why, although they are in the same conditions, some employees turn to malicious acts while others do not (Moore et al. 2008). Attackers often commit deviant online behaviors to make a statement. Thus, any unusual behavior markers, such as threating statements or the spamming of anonymous messages, can be understood as key indicators of a potential attack (Schultz 2002).

Personal predispositions of malicious insiders have included serious mental health disorders, including alcohol and drug addiction, panic attacks, spousal abuse, etc.; poor social skills and decision making, including bullying, intimidation, personality conflicts, unprofessional behavior, personal hygiene issues and dress code violations; inability to follow rules; aggressive or violent behavior; sexual harassment; lying about qualifications; maladaptive reactions to stress, financial, and personal issues; strong or inappropriate reactions to sanctions; escalation of work conflicts; and a history of rule breaking, including arrests, hacking, security violations, and harassment incidents; and abuse of travel, time, and expenses. All malicious insiders will likely show the influence of at least one personal predisposition (Moore et al. 2008, Greitzer and Hohimer 2011).

Despite these precursors, organizations routinely ignore warning signs. Ninety-seven percent of malicious insiders were brought to the attention of supervisors and coworkers because of troubling behavior patterns, while 80 percent in another study showed troubling behavior, including truancy, tardiness, conflicts with coworkers, and poor performance (Moore et al. 2008).

A number of suggested psychological indicators may be used to identify insiders. These indicators must be tested to demonstrate validity. A disgruntled employee will appear to be dissatisfied with his or her position, discontented about being underpaid or not being promoted, and may be a bad fit for his or her current job. The disgruntled employee may have an adverse reaction to criticism, reacting inappropriately and personally and becoming hostile or defensive. The employee may not acknowledge or admit to mistakes and may conceal errors (Greitzer and Hohimer 2011).

Additionally, malicious insiders may have anger management issues and may have pent up hostility that they have difficulty controlling. They may also seem detached, uninterested in group communication, withdrawn, and may not attend meetings. Insiders often will not abide by rules, authority, or policies because of a feeling of being above the rules. They will likely have received corrective actions because of poor performance and may be unable to handle personal stress or strain. Malicious insiders may also have difficulty separating their personal lives and conflicts from work. They may display aggressive, argumentative behavior toward others and may be unable or unwilling to keep up their commitments. Finally, malicious insiders may display excessive and unexplained absenteeism and truancy (Greitzer and Hohimer 2011).

Malicious insiders may show higher levels of neuroticism according to the Big Five Personality framework, which includes five dimensions of personality (Openness to experience, Conscientiousness, Agreeableness, Extraversion, and Neuroticism). Low agreeableness, low conscientiousness, and high neuroticism are the most highly correlated with insider threat risk (Yang et al. 2018), although a separate study discovered that the majority of insider attackers also score highly on introversion (Schultz 2002, Alahmadi et al. 2015). Neuroticism causes one to experience negative and unstable emotions more frequently than non-neurotic individuals and therefore show lower levels of self-esteem and higher pessimism. Neurotic individuals also tend to cope poorly with stress. Low conscientiousness also indicates an inability to self-regulate, leading to an inability to cope with stress, control impulses, and regulate emotions. Malicious insiders may also show low levels of agreeableness, indicating a low interest in cooperating with others and a general unfriendliness, suspiciousness, and a greater self-interest. The sub-dimensions of agreeableness can also be used to indicate an insider risk. Low scores on trust, sympathy, morality, and altruism may indicate a higher likelihood to become involved in conflicts, while low scores on anxiety and vulnerability may indicate a motivation and adaptability at work. Low scores on dutifulness indicate one who disregards rules (Yang et al. 2018).

The Dark Triad may be more useful in determining antisocial behavior, measuring Machiavellianism, narcissism, and psychopathy. Machiavellianism indicates a cynical, unprincipled individual who believes that manipulation is necessary for success. Narcissistic individuals show high levels of grandiosity, entitlement, and feelings of superiority (Yang et al. 2018). The need for admiration, a lack of empathy, and unwarranted self-importance have all been found in malicious insider attackers (Alahmadi et al. 2015). Psychopathy includes behaviors related to impulsivity, antisocial acts, selfishness, and insensitivity. All three of the Dark Triad traits are relevant to malicious insiders and each influences malicious intent (Yang et al. 2018).

Motivations for insiders are varied and include making an unintentional mistake; attempting to accomplish tasks through workarounds; attempting to force the system into doing an action it is not designed for; unintentionally going beyond the authorized limit; checking the system for vulnerabilities with or without the intent to report them; viewing data for fun; committing an attack for the purpose of expressing disgruntlement; testing the system for technical challenge; committing an act with the intent to cause harm for fame, greed, capability, etc. (Pfleeger 2008). Despite the differences in intent, the outcomes of each action can be equally damaging (Probst et al. 2010).

Most malicious insiders who commit sabotage are disgruntled. In one study, 57 percent of insiders were perceived as disgruntled, while 84 percent were motivated by revenge, and 92 percent committed their attack after a negative work-related event, including termination, disputes, demotion, or transfer (Moore et al. 2008). Feelings of disgruntlement in employees

can be caused by “unpleasant task, little autonomy, coercive control, low pay, few benefits, little prestige, and very limited opportunities for advancement” (Dang 2014). These strains are then separated into the categories of mismatching expectations (including perceived lack of monetary reward, benefits, prestige, and opportunity for advancement) and job dissatisfaction (coercive control and insecurity, excessive workload, complicated procedures). Additionally, sanction pressure where employees feel they are under too harsh, erratic, or excessive supervision and discipline can lead to disgruntlement. Employee conflict, including insults, ridicule, gossip, threats, coercive behavior, and physical assaults likewise contribute to strain. Disgruntlement is considered a major psychological indicator of an insider threat (Dang 2014).

Other precursors to insider attacks are unmet expectations and stressful events. Unmet expectations include insufficient salary and bonus, lack of promotion, restriction of online activities, limitations on company resources, violations of privacy, weakened authority or responsibilities, unfair work requirements, and bad coworker relationships (Moore et al. 2008).

Stressful events, such as organizational sanctions, lead to a higher probability of insider sabotage. Ninety-seven percent of malicious insiders were found to have experienced one or more stressful events before their attack. The majority attacked after they were terminated or suspended. Stressful events also included poor performance evaluations, sanctions for bad behavior, suspension for absenteeism, demotion for poor performance, limited responsibilities and online privileges, disagreements about salary or bonuses, no offer of severance package, new hire of supervisor, or personal issues such as death in the family or divorce (Moore et al. 2008).

One study found that most malicious insider attacks were committed on the job with financial gain being the primary motivation. Another study conducted from 1996 to 2002 found that most malicious insider attacks were triggered by a negative work-related incident (Wall 2013).

B.3.3 Deterrence

Current methods of insider threat mitigation tend to focus on detecting malicious behavior and then identifying and disciplining the offender. Tools are forensic in nature and are employed after the exploit has occurred, which gives no information on the threat indicators of insiders (Greitzer and Frincke 2010). Instead, monitoring employee behavior, enacting psychological screening before hiring employees, and delivering effective trainings may be more effective in the deterrence of insiders, although each is not without potential disadvantages.

Greitzer and Frincke propose combining traditional monitoring (such as workstation or internet activity monitoring) with organizational and social data to determine motives and predict future actions, which may lead to early identification of threats. This method, however, may be viewed as intrusive and thus may lead to disgruntlement among high-risk employees. Less invasive methods that do not use personal data may reduce the risk. It has been shown that overly intrusive security measures could lead to employee dissatisfaction, lower productivity, lower commitment, and frustration. However, too little attention and monitoring can also increase potential insider activity. This situation can be referred to as the “trust trap” where the organization’s trust toward individuals increases, which then creates a false sense of security and thus reduced vigilance toward the potential risk (Greitzer and Frincke 2010).

Psychological reactance theory states that individuals who have a perception of being externally controlled will react by reasserting control. Regaining control may be done through sabotage and other destructive acts. Individuals who feel powerless may intend to damage or harm the

organization as a means of revenge against what they perceive as unwarranted monitoring. Posey et al. (2011) found that the stress of computer monitoring had a positive and direct link to internal computer abuse.

Deciding what level of monitoring is acceptable, or whether it should be conducted at all, is an important factor in deterring insider threats. Some cases of increased monitoring have not led to any difference in identified incidents. In other cases, attackers understood the monitoring system and how to exploit it. Employment screening may be an alternative, although it is likely to lead to false positives where innocents may be identified as threats. Insider threat identification must therefore be context driven (Probst et al. 2010). Because of the lack of substantive research, it is unclear whether monitoring is an adequate solution to identifying insider threats. Thus, we do not know if monitoring is a successful deterrent (Pfleeger 2008).

If monitoring is introduced without advance notice and without transparency, the potential for negative backlash is increased. Thus, if monitoring is to be implemented, the process must be entirely disclosed, explained, and managed fairly in order to minimize distrust and frustration by employees. Maintaining mutual trust is absolutely necessary (Greitzer and Frincke 2010).

The following data should not be included in insider monitoring because of legal and ethical concerns: arrest records; use of employee assistance programs; life events such as marriage, birth, divorce, or death; and health events and medical records. Psychosocial factors that can be used include: tools used in staff performance evaluations; competency and disciplinary tracking; timecard records; proximity card records; and pre-employment background checks (Greitzer and Frincke 2010).

Deterrence and identification are better options than arrest and investigation because of the relative freedom a company has in monitoring employee behavior compared to the abilities of law enforcement. Companies can monitor employee behavior as long as there is reasonable purpose, while law enforcement must have probable cause and a search warrant. Psychological screening before hiring an employee may help identify potential insiders. However, invasive psychological evaluations that are in depth enough to detect potential insiders would likely be uncomfortable to non-attackers. Moreover, this kind of evaluation takes time away from evaluating one’s suitability to the organization (Pfleeger 2008).

Improvements in identifying at-risk individuals could include pre-employment screening on personality and past and current behavior; mitigating predisposition through expectation setting to minimize probability of unmet expectations; enabling intervention techniques; improving awareness of behavior changes and intervention and counseling approaches; documenting problematic behaviors and procedures to respond to problematic behaviors; creating an organizational climate that is conductive to coworker intervention; creating online environments to mitigate work-related stress; and improving reinforcement of organizational rules and policies (Greitzer and Frincke 2010).

Combining cybersecurity audit data with demographic and organizational data about the employee is one method of predicting attacks instead of merely detecting them. Such data can include annual performance review; performance awards/recognition; background checks and clearance information; assessments of managers and peers about behavior including disgruntlement, stress, and anger; physical security access; and attendance and time reporting records. Of course, prediction instead of detection comes with the risk of false positives and false negatives. Once an organization has an understanding of the insider threat in complete detail, mitigating the threat and defusing the situation can involve intervention by supervisors,

coworkers, family, and friends that can lead to counseling, support groups, or medical assistance (Greitzer and Frincke 2010).

Other methods of deterrence include the reinforcement of good behaviors (Pfleeger 2008). Making security policies easy to follow is necessary in mitigating insider threats. Compliance is difficult to achieve because of individual tolerance limits for interruptions in workflow. Thus, successful policies must show the value of security rather than just requiring it without question (Probst et al. 2010). Every employee should receive comprehensive training on security and information technology practices to reduce the risk of non-malicious and unintentional insider threats (Greitzer and Frincke 2010). The best plan for deterring insiders is ultimately maintaining an organization where employees are satisfied and treated fairly (Greitzer and Frincke 2010).

It should be noted that, although security training can be an effective deterrent, it can also give insiders the skills, resources, and knowledge necessary to commit a successful attack. By using company resources, security loopholes can be discovered and exploited by insiders Willison and Warkentin (2013).

Sanctions against insiders can be technical, including the restriction of system privileges or access. Non-technical sanctions include demotion, termination, or reprimand. Although these sanctions are intended to deter future threats, they can unintentionally create escalation of disgruntlement. Whether these sanctions deter or escalate the insider depends on the personal disposition of the insider (Moore et al. 2008). Ensuring a fair distribution of sanctions for policy violations is one method for reducing this probability for abuse. Educating employees on the reason for monitoring and developing a set of procedures for monitoring can assist in reducing abuse as long as the consequences are evenly and fairly implemented (Posey et al. 2011). Organizational injustice represents perceived unfairness in outcomes (distributive injustice), procedures determining outcomes (procedural injustice), and treatment received by others (interactional injustice). These organizational injustices can contribute to strain, which then increases the likelihood to engage in deviant behaviors. If organizational injustice leads to criminal behavior, then implementing organizational justice may assist in mitigating criminal behavior (Dang 2014).

Examining theories in the fields of the social sciences may provide valuable insight into the deterrence of insiders. Specifically, general deterrence theory, the theory of planned behavior, and general strain theory will be discussed.

General deterrence theory focuses on punishment severity, certainty, and celerity. While implementing security systems was found to motivate abuses by insiders in one study, another found no deterrence effect on the intention to commit an attack. Regardless, it was found that deterring effects of severe, certain, and swift punishment did not have the desired effect (Dang 2014).

The theory of planned behavior suggests that for a crime to occur, the offender must have both motive and opportunity. When the likelihood of punishment is high and sanctions are severe, insiders may be deterred when their motives are weak (Probst et al. 2010).

General strain theory posits that there are three types of stressful life events that may promote criminal behavior. These three strains are the prevention of meeting positive goals, the removal of positive stimuli, and the presence of negative stimuli. Because careers in information systems are often high stress, these professionals may be susceptible to the strains that encourage white-collar criminality (Dang 2014).

Other recommendations include clearly enforcing policies; periodic security awareness training; monitoring and responding to suspicious behaviors; anticipating and mitigating workplace issues; securing the physical environment; enforcing strict password and account policies; using additional caution with system administrators and privileged users; logging, monitoring, and auditing online actions of employees; immediately deactivating computer access after termination; creating secure backup and recovery plans; and developing insider response plans (Greitzer and Frincke 2010).

B.4 References

Alahmadi B, P Legg, and J Nurse. 2015 "Using Internet Activity Profiling for Insider-Threat Detection. In *Proc. of 12th International Workshop on Security in Information Systems*.

Albahar M. 2019 “Cyber Attacks and Terrorism: A Twenty-First Century Conundrum.” *Science and Engineering Ethics*. 25(4):993-1006.

Alzoubaidi AR, D Prodan-Palade, and S Ekici. 2016. *Countering Terrorist Recruitment in the Context of Armed Counter-Terrorism Operations*. IOS Press.

Awan I. 2017. “Cyber-Extremism: ISIS and the Power of Social Media.” *Society*, 54:138-149.

Cavelty MD. 2008. “Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate.” *Journal of Information Technology & Politics*. 4(1):19-36.

Corner E and P Gill. 2017. “Is there a Nexus between Terrorist Involvement and Mental Health in the Age of the Islamic State?” *Combating Terrorism Center*. 10(1).

Dang D. 2014. "Predicting Insider's Malicious Security Behaviours: A General Strain Theory-Based Conceptual Model." In *Proceedings of the International Conference on Information Resources Management (CONF-IRM)*, Ho Chi Minh City.

Denning DE. “Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.” Chapter 8 in J. Arquilla and D. Ronfeldt (eds), *Networks and Netwars. The Future of Terror, Crime, and Militancy*.” RAND Corporation, Santa Monica, CA.

Dogrul M, A. Aslan, and E Celik. 2011. “Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism.” In *Proc. Of 3rd International Conference on Cyber Conflict*.

DOJ. 2018. *Report of the Attorney General’s Cyber Digital Task Force*. Office of the Deputy Attorney General, U.S. Department of Justice.

FBI. 2007. *Terrorism 2002-2005*. U.S. Federal Bureau of Investigation, U.S. Department of Justice.

Greitzer F and D Frincke. 2010. "Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation." In (eds. Probst CW, Hunker J, Bishop M, and D Gollman) *Insider Threats in Cyber Security*, pp. 85-113. Springer, Boston.

Greitzer F and R. Hohimer. 2011. "Modeling Human Behavior to Anticipate Insider Attacks." *Journal of Strategic Security,* 4(2):25-48.

Greitzer FL, A P Moore, DM Cappelli, DH Andrews, LA Carroll, and T D Hull. 2008. "Combating the Insider Cyber Threat." *IEEE Security & Privacy,* 6(1):61-64.

Hua J and S Bapna. 2012. “How Can We Deter Cyber Terrorism?” *Information Security Journal A Global Perspective*. 21(2):102-114.

Hua J and S Bapna. 2013. "The Economic Impact of Cyber Terrorism." *The Journal of Strategic Information Systems,* 22(2):175-186.

Kenney M. 2015. “Cyber-Terrorism in a Post-Stuxnet World.” *Orbis*. 59(1).

Klein JJ. 2015 "Deterring and Dissuading Cyberterrorism." *Journal of Strategic Security*. 8(4):23-38.

Liu L, O De Vel, Q-L Han, J Zhang, and Y Xiang. 2018. "Detecting and Preventing Cyber Insider Threats: A Survey." *IEEE Communications Surveys & Tutorials,* 20(2):1397-1417.

MacDonald S. 2015. “Assessing and Responding to the Cyberterrorism Threat.” In ed. MN Ogun, *Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses*, pp. 200-209. IOS Press.

Moore A, D Cappelli, and R Trzeciak. 2008. "The ‘Big Picture’ of Insider IT Sabotage Across US Critical Infrastructures," pp. 17-52. In (eds. Probst C, Hunker J, Gollmann D, and Bishop M) *Insider Attack and Cyber Security*. Springer, Boston.

Neumann P. "Combatting Insider Threats." 2010. In (eds. Probst C, Hunker J, Gollmann D, and Bishop M) *Insider Threats in Cyber Security*, pp. 17-41. Springer, Boston.

Pfleeger CP. 2008. "Reflections on the Insider Threat." In (eds. Stolfo SJ, Bellovin SM, Hershkop S, Keromytis AD, Sinclair S, and Smith S.) *Insider Attack and Cyber Security: Beyond the Hacker*, pp. 5-16. Springer, Boston.

Plachkinova M and A. Vo. 2019. “Hactivism and Its Impact on Society.” In *AMCIS 2019Proc.*

Posey C, B Bennett, T Roberts, and P Benjamin. 2011. "When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse," *Journal of Information System Security,* 7(1):24-47.

Probst CW, J Hunker, D Gollmann, and M Bishop. 2010. "Aspects of Insider Threats." In (eds. Probst C, Hunker J, Gollmann D, and Bishop M) *Insider Threats in Cyber Security*, pp. 1-15. Springer, Boston.

Rogers M. 2003. “The Psychology of Cyber-Terrorism.” Chapter 4 in *Terrorists, Victims and Society: Psychological Perspectives on Terrorism and Its Consequences*, ed: A. Silke. John Wiley & Sons LTD.

Rogers M. 2018. “Cyber Terrorism.” Chapter 22 in (ed. Andrew Silke) *Routledge Handbook of Terrorism and Counterterrorism*.

Schultz EE. 2002. "A Framework for Understanding and Predicting Insider Attacks." *Computers & Security,* 21(6):526-531.

Seissa IG, J Ibrahim, N-Z Yahaya. 2017. “Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review.” *International Journal of Science and Research*, pp. 180-186.

Tafoya WL. 2011. “Cyber Terror.” *FBI Law Enforcement Bulletin*. U.S. Department of Justice.

Theohary CA and JW Rollins. 2015. *Cyberwarfare and Cyberterrorism: In Brief*. Congressional Researc Service Report Prepared for Members and Committees of Congress.

UNODC. 2012. *The Use of the Internet for Terrorist Purposes*. United Nations Office on Drugs and Crime. Vienna.

Wall DS. 2013. "Enemies within: Redefining the Insider Threat in Organizational Security Policy." *Security Journal,* 26,(2):107-124, 2013.

Webber C and M Yip. 2018. “The Rise of Chinese Cyber Warriors: Towards a Theoretical Model of Online Hacktivism.” *International Journal of Cyber Criminology*. 12(1):230-254.

Weimann G. 2005. “Cyberterrorism: The Sum of All Fears?” *Studies in Conflict & Terrorism*. 28:129-149.

Willison R. and M. Warkentin. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse." *MIS Quarterly,* 37(1): 1-20.

Yang G, L Cai, A Yu, J Ma, D Meng, and Y Wu. 2018. "Potential Malicious Insiders Detection Based on a Comprehensive Security Psychological Model." In *Proc. of IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService)*.

Appendix C – Total Estimated Cost of Implementing the Risk Management Framework

In 2017, a cost estimate to implement the Risk Management Framework for facility-related control systems (FRCS) on 150 Army installations was conducted. The estimates were for three distinct but overlapping courses of action (COA).

C.1 COA 1: Critical Assets Only

COA 1: Discover, assess, and remediate cybersecurity vulnerabilities in 100 critical assets (buildings) across 24 installations.

Assumptions:

- Assessment base reviewed 100 critical assets located at 24 installations
- 4 per installation
- Critical infrastructure 1,650 based on 90 systems
- Remediation based on Federal Risk and Authorization Management Program metrics
- The Federal Risk and Authorization Management Program is a government-wide program that provides a standardized measure of cloud service providers. Federal agencies are required to use cloud services approved by the Federal Risk and Authorization Management Program.

COA 1 - Critical Assets	Million $		
	FY18	FY19	FY20
Critical Assets (Level 1 Discovery & Assess & Remedia	$19.4		
Critical Assets (Level 1 Discovery & Assess & Remediate)		$ 19.4	
Critical Infrastructure - 1650 (Level 1 Discover & Assess)			$ 20.8
FRCS Certification (critical only)		6.0	6.0
Total	$19.4	$ 25.4	$ 26.8

Overnight Costs	
	Critical Assets
Critical Assets	($ Mil.)
Total Inventory for Critical Installations	0.30
Total Remediation Cost:	$ 38.5
Total Critical Certification:	$ 12.0
Critical Infrastructure -1650	$ 20.8
Total Critical Assets	71.6

Figure C.1. COA 1 Critical Assets

C.2 COA2: Critical Assets and Department of Defense Information Network Facing Systems

COA 2: COA 1 and any Department of Defense Information Network (DoDIN)-connected FRCS.

Assumptions

- Not knowing how many systems are connected to DoDIN, we assume half of COA 3 will be found to either reside on DoDIN or use the same physical transport medium. Thus, we assume all the costs included in COA 1 and approximately half of the costs of COA 3.
- ES2 – Utility/water; FRD Tier 1; and FRD Tier 2 include separate inventory and assessment teams for each installation. This assumes a 3-person team completing 16 installations per year.
- Network architecture changes use Cisco Adaptive Security Appliance logical segmentation.
- Above baseline service sustainment based on a quote for contract service sustainment from a Dugway Proving Grounds Network Enterprise Center. Two personnel needed to meet the skillset required for FRCS systems.

COA 2 - COA 1 + DODIN facing systems					Million $				
	FY18	**FY19**	**FY20**	**FY21**	**FY22**	**FY23**	**FY24**	**FY25**	**FY26**
Critical Assets (Level 1 Discovery & Assess & Remediate	$19.4								
Critical Assets (Level 1 Discovery & Assess & Remediate)		$ 19.4							
Critical Infrastructure - 1650 (Level 1 Discover & Assess)			$ 20.8						
FRCS Certification (Critical Only)		6.0	6.0						
ES2 - Utility/Water (Level 1 Discovery & Assess)			31.7	31.7	31.7	31.7	31.7		
Tier 1 FRD				5.5	5.5	5.5	5.5	5.5	
Tier 2 FRD					5.5	5.5	5.5	5.5	5.5
Dedicated Assessor Teams (CPT/IO/Contract)									
Contract Augmentation (Inventory)									
Remediation - DODIN facing	11.8	11.8	11.8	11.8	11.8	11.8	11.8	11.8	11.8
Network Architecture Changes (DODIN portion)	39.7	39.7	39.7	39.7					
Monitoring Solution									
Above Baseline Service Sustainment	1.4	1.4	4.9	4.9	4.9	4.9	4.9		
Certifications DODIN Facing	17.9	17.9	17.9						
Recertification									
Lifecycle Replacement									
Total by Year	90.1	96.1	132.8	93.5	59.3	59.3	59.3	22.7	17.2

Overnight Costs	
Critical Assets + DODIN Facing Assets	Critcal Assets + DODIN ($ Mil.)
Total Inventory for Critical Installations:	0.30
Total Remediation Cost:	$ 38.5
Critical Infrastructure - 1650	$ 20.8
FRCS Certification (Critical Only):	$ 12.0
ES2 - Utility/Water (Level 1 Discovery & Asses	$ 158.3
Tier 1 FRD	27.3
Tier 2 FRD	27.3
Remediation (non-critical asset)	105.9
Network Architecture Changes	158.7
Monitoring Solution	
Above Baseline Service Sustainment	27.4
Certification	53.8
Recert	
Lifecycle Replacement	
Total Critical Assets	**630.4**

Figure C.2. COA 2 – COA 1 + DoDIN-Facing Systems

C.3 COA 3: All Army-Owned Systems

COA 3: Discover, assess, and remediate all Army-owned FRCS. This estimate used a population size of 150,000 buildings.

Assumptions – Assessment

- Remaining assessments valued all the noncritical assets
- Assessments assumed 2 hours per building per team
- Separated into small, medium, and large installations based on square footage
- Extrapolated to 156 installations

Assumptions – Remaining Remediation

- Based Federal Risk and Authorization Management Program certification – meets requirements of Risk Management Framework
- Remove COA 1 remediation and divided by 9 years

Assumptions – Recertification

- Recertified every third year
- Assumed 10 types of manufacturers for 12 systems be certified
- The Lifecycle Replacement line item is based on Army Regulation 25-1 guidance to replace common-use information technology every 3 years. The number of common-use servers and workstations was estimated at 40 per base to account for 12–15 unique systems per installation with 1 server and 2–3 workstations per unique system.

COA 3 - All Systems	Million $								
	FY18	FY19	FY20	FY21	FY22	FY23	FY24	FY25	FY26
Critical Assets (Level 1 Discovery & Assess & Remediate)	19.4								
Critical Assets (Level 1 Discovery & Assess & Remediate)		19.4							
Critical Infrastructure - 1650 (Level 1 Discover & Assess)			20.8						
FRCS Certification (critical only)		6.0	6.0						
ES2 - Utility/Water (Level 1 Discovery & Assess)			31.7	31.7	31.7	31.7	31.7		
Tier 1 FRD				10.9	10.9	10.9	10.9	10.9	
Tier 2 FRD					10.9	10.9	10.9	10.9	10.9
Dedicated Assessor Teams (CPT/IO/Contract)	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
Contract Augmentation (Inventory)	11.5	11.5	11.5	11.5	11.5	11.5	11.5	11.5	11.5
Remediation	23.5	23.5	23.5	23.5	23.5	23.5	23.5	23.5	23.5
Network Architecture Changes	79.4	79.4	79.4	79.4					
Monitoring Solution			1.2	1.2	1.2	1.2	1.2		
Above Baseline Service Sustainment	2.4	2.4	8.7	8.7	8.7	8.7	8.7		
Certifications (non-critical)	35.9	35.9	35.9						
Recertification				19.9	19.9	19.9	19.9	19.9	19.9
Lifecycle Replacement								5.1	5.1
Total by Year	172.6	178.6	219.1	187.3	118.8	118.8	118.8	82.5	71.5

	Costs ($ Mil.)
Total Inventory for Critical Installations:	0.3
Remediation for Critical Assets	38.5
Critical Infrastructure - 1650 (Level 1 Discover & Assess	20.8
FRCS Certification	12.0
ES2 - Utility/Water (Level 1 Discovery & Assess)	158.3
Tier 1 FRD	54.6
Tier 2 FRD	54.6
Dedicated Assessor Teams (CPT/IO/Contract)	4.6
Contract Augmentation (Inventory)	103.5
Remaining Remediation	211.8
Network Architecture Changes	317.5
Monitoring Solution	5.9
Above Baseline Service Sustainment	48.2
Certification (non-critical)	107.6
Recert	119.6
Lifecycle Replacement	10.3
Total	1,268.0

Figure C.3. COA 3 All Systems

Appendix D – Full-time Equivalent Cost Estimate

Pacific Northwest National Laboratory (PNNL) used a seven-step process to determine a range in labor hours for the implementation of the security controls in NIST SP 800-53rev4. Supplemental controls were not assessed. The estimates were based on a trained, experienced professional conducting the work using mature processes and, where applicable, established technologies, such as the Assured Compliance Assessment Solution. Figure D.1 shows the process used to determine the full-time equivalent (FTE) cost in labor needed to implement the assessed security controls for small, medium, and large installations.

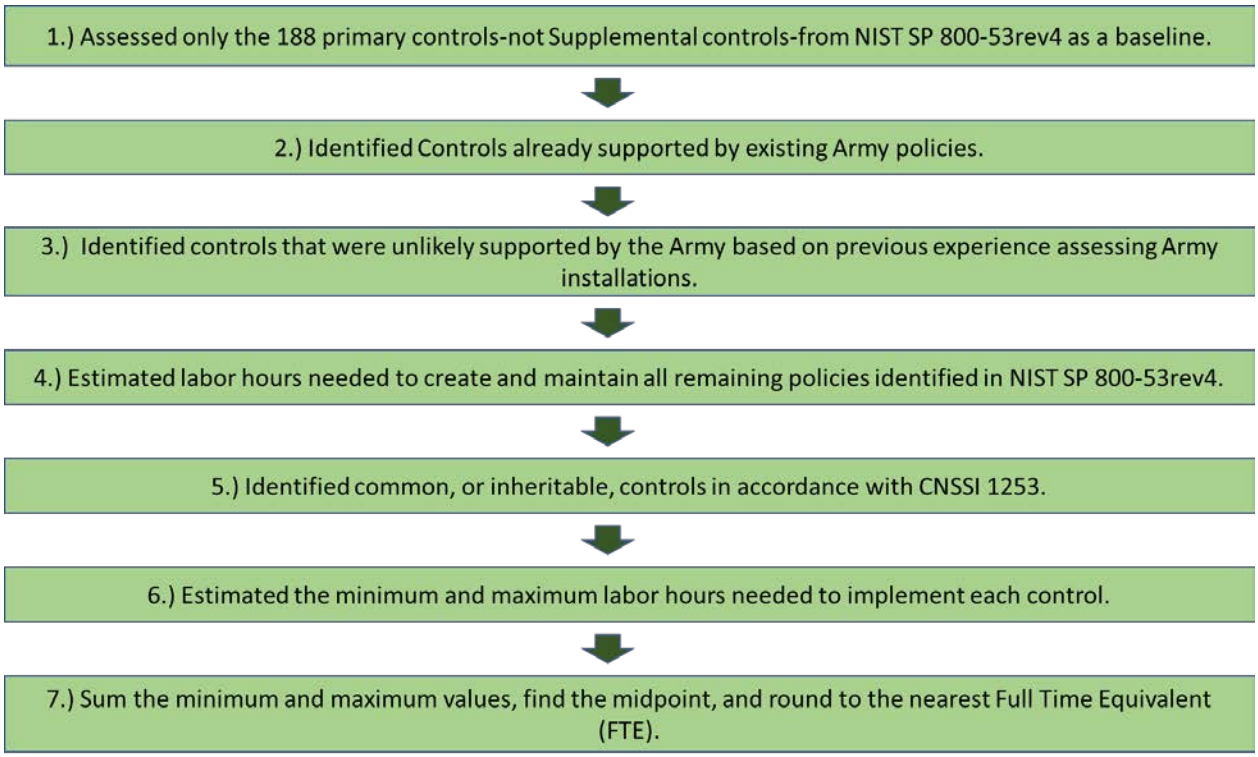


Figure D.1. The Seven-Step Process PNNL Used to Make Full-time Equivalent Determinations per Installation Category

PNNL used the installation size categorizations from the 2017 cost-benefit analysis for implementing the Risk Management Framework on 150 Army installations. The size categories are based on an installation's number of buildings. The 2017 cost-benefit analysis assigned a common number, or mode, of buildings per category and range of buildings for each category; see Figure D.1. These size categorizations were the model PNNL used to determine how to implement security controls applicable to each device.

Table D.1 Mode (Common Number) and Range of Buildings per Category

Number of Buildings	Small	Medium	Large
Range	3–999	1,000–2,249	2,250+
Mode	555	1,500	2,250

Based on previous inventories conducted by PNNL in support of the Army, PNNL assumed that all installations would have a minimum of 17 systems supported in whole or in part by the installation's Department of Public Works. These systems can include intrusion detection systems, fire alarm systems, substations, mass notification, and energy management and control systems. Table D.2 lists the types of major systems found on Army installations. PNNL assumes this list is not comprehensive and that other systems not included in this study are currently in use at Army installations. PNNL further acknowledges that the systems not included in this study will be included in an installation's implementation of the Risk Management Framework.

Table D.2. List of System Types Found on Army Installations

System Type
Mass Notification System
Intrusion Detection System
Fire Alarm System
Energy Management Control System
Water/Wastewater System
3 MW Photovoltaic System
1MW/hr Battery System
Computer-Aided Dispatch
Closed Circuit Television
Gasification System
HVAC
Smart Metering
Smart Lighting
Water Treatment/Wastewater System
MEDCOM Equipment
Test Equipment for Chemical and Biological Labs
RDECOM Equipment

A subset of security controls was assessed using the installation models described above. The subset was used to determine an average minimum and maximum number of labor hours needed to implement the assessed security controls. The averages were used to estimate the total labor hours needed to implement all remaining security controls. Table D.3 shows the estimates made for policy and procedure creation and maintenance for Risk Management Framework security control families.

Table D.3. Policy FTE Estimates for Risk Management Framework Security Control Families

No.	Title	Trained SME		Novice		Policy		Procedures		Total	Annual Review / Revision
AC-1	Access Control Policy and Procedures	4	Access Control, including Auth/Auth requirements, includes subject matters to include AD, MFA, and more which require a clearer understanding of standards and connecting NIST guidelines (e.g., 800-63-3)	16	Complicated set up documents, including NIST, OMB Memos, and White House Directives which would take a new individual some time to understand and map	4	Once understood, defining a policy is relatively easy—depending on how you structure policy	20	Detailing exhaustive procedures around account management processes will be cumbersome and require adequate time to accomplish	28–40 hours	2

No.	Title	Trained SME		Novice		Policy		Procedures		Total	Annual Review / Revision
AT-1	Security Awareness and Training Policy and Procedures	2	Requirements for standard users, privileged users, Department of Defense (DoD) phishing requirements, etc.	8	Understanding what DoD desires and what you will have to answer to (e.g., Data Call) will take minimal time	2	Once understood, defining a policy is relatively easy, depending on how you structure policy	16	Training is diverse (computer-based, in-person, simulations) and will require time to develop	20–26 hours	2
AU-1	Audit and Accountability Policy and Procedures	2	Self-explanatory	8	Minor time required to understand oversight requirements	2	Once understood, defining a policy is relatively easy, depending on how you structure policy	12	Procedures generally dictate automatic processes and/or defined audit data flows	16–22 hours	2

No.	Title	Trained SME		Novice		Policy		Procedures		Total	Annual Review / Revision
CA-1	Security Assessment and Authorization Policy and Procedures	8	Ensuring understanding of site processes for authority to operate will still take some time to accomplish	20	Understanding the ATO process, in accordance with how a given Authorizing Official may wish to deviate, will take additional effort	8	Once understood, defining a policy is relatively easy, depending on how you structure policy	20	As a “more important” set of documents to confirm the processes and how they relate to Department of Defense oversight, will take substantial effort	36–48 hours	2
CM-1	Configuration Management Policy and Procedures	2	Self-explanatory	8	Minor time required to understand oversight requirements	2	Once understood, defining a policy is relatively easy, depending on how you structure policy	12	Config. Mgmt specific processes are relatively easy to document and maintain	16–22 hours	2

No.	Title	Trained SME		Novice		Policy		Procedures		Total	Annual Review / Revision
CP-1	Contingency Planning Policy and Procedures	2	Self-explanatory	8	Minor time required to understand oversight requirements	2	Once understood, defining a policy is relatively easy, depending on how you structure policy	12	Contingency planning processes are relatively easy to document and maintain	16–22 hours	2

No.	Title	Trained SME		Novice		Policy		Procedures		Total	Annual Review / Revision
IA-1	Identification and Authentication Policy and Procedures	4	A good understanding of IA and AC will take minor time to make sure all requirements are met	16	Understanding how this control family relates to AC and the mgmt. of Identifiers and Authenticators (and combination of DoD requirements) will take a strong level of understanding	4	Once understood, defining a policy is relatively easy, depending on how you structure policy	16	Detailing exhaustive procedures around org. and non-org users, as well as processes for distributing Identifiers/ Authenticators, will be cumbersome and require adequate time to accomplish	24–36 hours	2

No.	Title	Trained SME		Novice		Policy		Procedures		Total	Annual Review / Revision
IR-1	Incident Response Policy and Procedures	4	The IR process, including the IR Plan, will help direct the needs	16	Understanding the scope of IR as it relates to a cyber program, including escalation, reporting, and other requirements, will take substantial time	4	Once understood, defining a policy is relatively easy, depending on how you structure policy	20	Often iterative in nature; detailed explicit processes/requirements as dictated by DoD require important revision upfront	28–40 hours	2
MA-1	System Maintenance Policy and Procedures	2	Self-explanatory	8	Minor time required to understand oversight requirements	2	Once understood, defining a policy is relatively easy, depending on how you structure policy	12	Maintenance-specific processes are relatively easy to document and maintain	16–22 hours	2

No.	Title	Trained SME		Novice		Policy		Procedures		Total	Annual Review / Revision
PE-1	Physical and Environmental Protection Policy and Procedures	2	Self-explanatory	8	Minor time required to understand oversight requirements	2	Once understood, defining a policy is relatively easy, depending on how you structure policy	12	P&E-specific processes are relatively easy to document and maintain	16–22 hours	2
PL-1	Security Planning Policy and Procedures	4	An understanding of what this entails will take minimal time to accomplish	16	SSPs, ISA/MOU, and other formal documentation requirements will take effort to understand	4	Once understood, defining a policy is relatively easy, depending on how you structure policy	16	Ensuring processes are in place that help structure the formality and documentation that is meant for AO and other oversight review requires close attention	24–36 hours	2

No.	Title	Trained SME		Novice		Policy		Procedures		Total	Annual Review / Revision
PS-1	Personnel Security Policy and Procedures	2	Self-explanatory	8	Minor time required to understand oversight requirements	2	Once understood, defining a policy is relatively easy, depending on how you structure policy	12	Physical-security-specific processes are relatively easy to document and maintain	16–22 hours	2
RA-1	Risk Assessment Policy and Procedures	2	Self-explanatory	8	Minor time required to understand oversight requirements	2	Once understood, defining a policy is relatively easy, depending on how you structure policy	16	Risk assessment, including vulnerability management, is a cumbersome process that requires detailed steps to implement actionable processes	20–26 hours	2

No.	Title	Trained SME		Novice		Policy		Procedures		Total	Annual Review / Revision
SA-1	System and Services Acquisition Policy and Procedures	2	Self-explanatory	8	Minor time required to understand oversight requirements, including contractual acquisition resources	2	Once understood, defining a policy is relatively easy, depending on how you structure policy	12	S&S-acquisition-specific processes are relatively easy to document and maintain	16–22 hours	2
SC-1	System and Communications Protection Policy and Procedures	2	Self-explanatory	8	Minor time required to understand oversight requirements	2	Once understood, defining a policy is relatively easy, depending on how you structure policy	12	System and comms specific processes are relatively easy to document and maintain	16–22 hours	2

No.	Title	Trained SME		Novice		Policy		Procedures		Total	Annual Review / Revision
SI-1	System and Information Integrity Policy and Procedures	2	Self-explanatory	8	Minor time required to understand oversight requirements	2	Once understood, defining a policy is relatively easy, depending on how you structure policy	12	System & info. integrity specific processes are relatively easy to document and maintain	16–22 hours	2
PM-1	Information Security Program Plan	4	Usually dictated by a DoD Cyber Security Program Plan or other similar document; this will take minor time	20	Understanding the needs to encompass a holistic cyber program will need detailed understanding and preparation	2	Once understood, defining a policy is relatively easy, depending on how you structure policy	16	Cyber program procedures, while not used often, require accuracy and proper alignment with DoD oversight expectations	22–38 hours	2
									Totals:	346–488 hours	34

This assessment of security controls is specific to the devices known to be used by the Department of Public Works (DPW). This assessment does not cover the information technology systems supported by the Network Enterprise Center. The following security controls were excluded from the assessment based on previous inventory experience by the PNNL team and knowledge of current Army policy: AC-17 Remote Access; AC-18 Wireless Access; AC-10 Access Control for Mobile Devices; AC-22 Publicly Accessible Content; and SC-19 Voice Over Internet Protocol. See Table D.4 for a justification for each control excluded from the assessment.

Table D.4. Security Controls Not Assessed for Applicability

Number	Title	Justification
AC-17	Remote Access	Not supported by current Army policy
AC-18	Wireless Access	Not supported by current Army policy
AC-19	Access Control for Mobile Devices	Not supported by current Army policy
AC-22	Publicly Accessible Content	Not supported by current Army policy
SC-19	Voice over Internet Protocol	PNNL assumes DPW will not be tasked with supporting a Voice over Internet Protocol system

PNNL identified security controls that are likely already supported by existing Army policies and processes. The following security controls were excluded from the assessment based on previous inventory experience by the PNNL team and knowledge of current Army policy: AC-8 System Use Notification; AT-2 Security Awareness Training; AT-4 Security Training Records; CM-11 User-Installed Software; MA-2 Controlled Maintenance; MA-3 Maintenance Tools; MA-4 Non-Local Maintenance; MA-5 Maintenance Personnel; MA-6 Timely Maintenance; MP-1 Media Protection Policy and Procedures; MP-2 Media Access; MP-3 Media Marking; MP-4 Media Storage; MP-5 Media Transport; MP-6 Media Sanitization; MP-7 Media Use; PE-2 Physical Access Authorizations; PE-3 Physical Access Control; PE-4 Access Control for Transmission Medium; PE-8 Visitor Access Records; PE-3 Fire Protection; PS-3 Personnel Screening; PS-4 Personnel Termination; and PS-5 Personnel Transfer. See Table D.5 for a justification of each control already implemented by existing Army policy, program, or process.

Table D.5. Security Controls Implemented by Existing Army Policy

Number	Title	Control Types Implemented by...
AC-8	System Use Notification	Covered by existing Army policy. Installations should verify that these policies are being applied to DPW-owned systems.
AT-2	Security Awareness Training	Covered by existing Army program.
AT-4	Security Training Records	Covered by existing Army program.
CM-11	User-Installed Software	Covered by existing Army policy. Typically prohibited by End User License Agreement or Facility-Related Control System (FRCS) device warranty.
MA-2	Controlled Maintenance	Covered by Base Ops contract. Each installation should verify maintenance practices with the Base Ops contractor.

Number	Title	Control Types Implemented by...
MA-3	Maintenance Tools	Covered by Base Ops contract. Each installation should verify maintenance practices with the Base Ops contractor.
MA-4	Non-Local Maintenance	Covered by Base Ops contract. Each installation should verify maintenance practices with the Base Ops contractor.
MA-5	Maintenance Personnel	Covered by Base Ops contract. Each installation should verify maintenance practices with the Base Ops contractor.
MA-6	Timely Maintenance	Covered by Base Ops contract. Each installation should verify maintenance practices with the Base Ops contractor.
MP-1	Media Protection Policy and Procedures	Covered by existing Army policies regarding media.
MP-2	Media Access	Covered by existing Army policies regarding media.
MP-3	Media Marking	Covered by existing Army policies regarding media.
MP-4	Media Storage	Covered by existing Army policies regarding media.
MP-5	Media Transport	Covered by existing Army policies regarding media.
MP-6	Media Sanitization	Covered by existing Army policies regarding media.
MP-7	Media Use	Covered by existing Army policies regarding media.
PE-2	Physical Access Authorizations	Covered by existing Army policies.
PE-3	Physical Access Control	Covered by existing Army policies.
PE-4	Access Control for Transmission Medium	Covered by existing Army policies.
PE-8	Visitor Access Records	Covered by existing Army policies.
PE-13	Fire Protection	Covered by existing fire protection program.
PS-3	Personnel Screening	Covered by existing Army policies and processes for onboarding and offboarding personnel.
PS-4	Personnel Termination	Covered by existing Army policies and processes for onboarding and offboarding personnel.
PS-5	Personnel Transfer	Covered by existing Army policies and processes for onboarding and offboarding personnel.

Table D.6 shows the estimates and average values used for controls not individually assessed to determine a labor hour range for all security controls by installation size.

Table D.6. Remaining Security Control Labor Estimates (Hours)

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
AC-2	Account Management	42	104	31	78	21	52	
AC-3	Access Enforcement	42	104	31	78	21	52	
AC-4	Information Flow Enforcement	4	12	4	12	4	12	For DPW systems, information flow enforcement is limited to the implementation, configuration, and maintenance of routers, proxies, and firewalls. Information flow enforcement is limited to source, destination, and service (port).
AC-5	Separation of Duties	42	104	31	78	21	52	
AC-6	Least Privilege	42	104	31	78	21	52	
AC-7	Unsuccessful Login Attempts	42	104	31	78	21	52	
AC-10	Concurrent Session Control	42	104	31	78	21	52	
AC-11	Session Lock	42	104	31	78	21	52	
AC-12	Session Termination	42	104	31	78	21	52	
AC-14	Permitted Actions without Identification or Authentication	42	104	31	78	21	52	
AC-16	Security Attributes	42	104	31	78	21	52	

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
AC-20	Use of External Information Systems	2	8	2	8	2	8	For DPW systems, PNNL assumed this control referred memoranda of agreement, memoranda of understanding, or third-party contracts. Current DoD policy (DoDI 4000.19) establishes the memoranda of agreement/ understanding process. Policy governing third-party contracts exists but is not enforced. The estimate for this task assumes personnel can identify, are tracking, are reporting, and can enforce these agreements.
AC-21	Collaboration and Information Sharing	42	104	31	78	21	52	
AT-3	Role-Based Security Training	40	80	40	80	40	80	PNNL assumed installations were staffing cybersecurity personnel in DPW to support installation infrastructure and facilities. Training expectations for these roles is clearly outlined in DoDD 1322.18 and DoD 8570.01-M. These estimates are on a per-individual basis and agnostic of information assurance or identity and access management role and level.
AU-2	Audit Events	42	104	31	78	21	52	

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
AU-3	Content of Audit Records	42	104	31	78	21	52	
AU-4	Audit Storage Capacity	42	104	31	78	21	52	
AU-5	Response to Audit Processing Failures	42	104	31	78	21	52	
AU-6	Audit Review, Analysis, and Reporting	96	192	96	192	96	192	This is a common control, but it is affected by the number of devices that need to be audited. This estimate is based on a single analyst (Information Assurance Technician) using a mature system to review familiar network traffic. When starting this practice, the actual time to review logs and audit systems will be much greater.
AU-7	Audit Reduction and Report Generation	24	48	24	48	24	48	PNNL assumed this activity would largely be automated and spot checked for correctness by an individual analyst monthly. More frequent audit requirements as dictated by local policy will result in a greater labor burden. This control would require the purchase, training, installation, configuration, and maintenance of a system to automate these reports. The cost of this system is not captured in this estimate.

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
AU-8	Time Stamps	42	104	31	78	21	52	
AU-9	Protection of Audit Information	42	104	31	78	21	52	
AU-10	Non-Repudiation	42	104	31	78	21	52	
AU-11	Audit Record Retention	5	15	5	15	5	15	PNNL did not find a current records retention policy for DPW systems. PNNL defaulted to the National Archives and Records Administration *The General Records Schedules*, dated December 2019 for Information Systems Security Records. Records should be deleted after 3 years or after 1 year if the system has been superseded. PNNL further assumed that records retention would be a function of the system procured in support of security controls AU-6 and AU-7. The labor estimate for this control includes minor maintenance of records and supporting infrastructure.
AU-12	Audit Generation	42	104	31	78	21	52	
AU-14	Session Audit	42	104	31	78	21	52	

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
CA-2	Security Assessments	80	240	80	240	80	240	PNNL assumes these assessments will cover one-third of all implemented controls annually as required by FISMA and detailed in NIST SP 800-53rev4. The assessment process will follow the format detailed in NIST SP 800-53A. Assessment techniques will include interviews, questionnaires, tabletop exercises, reviews of audit logs and vulnerability scans, and the use of penetration testing software as needed.
CA-3	Information System Connections	42	104	31	78	21	52	
CA-5	Plan of Action and Milestones	42	104	31	78	21	52	
CA-6	Security Authorization	42	104	31	78	21	52	
CA-7	Continuous Monitoring	42	104	31	78	21	52	
CA-9	Internal System Connections	2	10	2	10	2	10	Activities related to internal connections will vary with an installation's operational tempo. The hours estimate associated with this control assumes the installation's security architecture is managed by an experienced professional (Information Assurance Manager III) using

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
								mature processes to vet and authorize new connections.
CM-2	Baseline Configuration	42	104	31	78	21	52	
CM-3	Configuration Change Control	8	40	8	40	8	40	Assuming minimum changes in FRCS network.
CM-4	Security Impact Analysis	42	104	31	78	21	52	
CM-5	Access Restrictions for Change	42	104	31	78	21	52	
CM-6	Configuration Settings	42	104	31	78	21	52	
CM-7	Least Functionality	42	104	31	78	21	52	
CM-8	Information System Component Inventory	42	104	31	78	21	52	
CM-9	Configuration Management Plan	42	104	31	78	21	52	
CM-10	Software Usage Restrictions	42	104	31	78	21	52	
CP-2	Contingency Plan	42	104	31	78	21	52	
CP-3	Contingency Training	42	104	31	78	21	52	
CP-4	Contingency Plan Testing	42	104	31	78	21	52	
CP-6	Alternate Storage Site	42	104	31	78	21	52	
CP-7	Alternate Processing Site	42	104	31	78	21	52	
CP-8	Telecommunications Services	42	104	31	78	21	52	

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
CP-9	Information System Backup	42	104	31	78	21	52	
CP-10	Information System Recovery and Reconstitution	42	104	31	78	21	52	
CP-12	Safe Mode	42	104	31	78	21	52	
IA-2	Identification and Authentication (Organizational Users)	42	104	31	78	21	52	
IA-3	Device Identification and Authentication	42	104	31	78	21	52	
IA-4	Identifier Management	42	104	31	78	21	52	
IA-5	Authenticator Management	42	104	31	78	21	52	
IA-6	Authenticator Feedback	42	104	31	78	21	52	
IA-7	Cryptographic Module Authentication	42	104	31	78	21	52	
IA-8	Identification and Authentication (Non-Organizational Users)	42	104	31	78	21	52	
IR-2	Incident Response Training	42	104	31	78	21	52	
IR-3	Incident Response Testing	42	104	31	78	21	52	
IR-4	Incident Handling	42	104	31	78	21	52	
IR-5	Incident Monitoring	42	104	31	78	21	52	
IR-6	Incident Reporting	42	104	31	78	21	52	

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
IR-7	Incident Response Assistance	42	104	31	78	21	52	
IR-8	Incident Response Plan	42	104	31	78	21	52	
IR-9	Information Spillage Response	42	104	31	78	21	52	
IR-10	Integrated Information Security Analysis Team	42	104	31	78	21	52	
PE-5	Access Control for Output Devices	42	104	31	78	21	52	
PE-6	Monitoring Physical Access	42	104	31	78	21	52	
PE-9	Power Equipment and Cabling	42	104	31	78	21	52	
PE-10	Emergency Shutoff	42	104	31	78	21	52	
PE-11	Emergency Power	42	104	31	78	21	52	
PE-12	Emergency Lighting	42	104	31	78	21	52	
PE-14	Temperature and Humidity Controls	42	104	31	78	21	52	
PE-15	Water Damage Protection	42	104	31	78	21	52	
PE-16	Delivery and Removal	42	104	31	78	21	52	
PL-2	System Security Plan	42	104	31	78	21	52	
PL-4	Rules of Behavior	42	104	31	78	21	52	
PL-8	Information Security Architecture	42	104	31	78	21	52	
PS-2	Position Risk Designation	42	104	31	78	21	52	

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
PS-6	Access Agreements	42	104	31	78	21	52	
PS-7	Third-Party Personnel Security	42	104	31	78	21	52	
PS-8	Personnel Sanctions	42	104	31	78	21	52	
RA-2	Security Categorization	42	104	31	78	21	52	
RA-3	Risk Assessment	42	104	31	78	21	52	
RA-5	Vulnerability Scanning	48	96	48	96	48	96	PNNL assumes DPW cybersecurity personnel would use the Assured Compliance Assessment Solution freely available to DoD personnel and accessible on the Defense Information Systems Agency website. The estimate for this control assumes an experienced analyst (IAT II) at a small installation.
SA-2	Allocation of Resources	42	104	31	78	21	52	
SA-3	System Development Life Cycle	42	104	31	78	21	52	
SA-4	Acquisition Process	42	104	31	78	21	52	
SA-5	Information System Documentation	42	104	31	78	21	52	
SA-8	Security Engineering Principles	42	104	31	78	21	52	
SA-9	External Information System Services	42	104	31	78	21	52	

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
SA-10	Developer Configuration Management	42	104	31	78	21	52	
SA-11	Developer Security Testing and Evaluation	42	104	31	78	21	52	
SA-12	Supply Chain Protection	42	104	31	78	21	52	
SA-15	Development Process, Standards, And Tools	42	104	31	78	21	52	
SA-19	Component Authenticity	42	104	31	78	21	52	
SC-2	Application Partitioning	42	104	31	78	21	52	
SC-4	Information in Shared Resources	42	104	31	78	21	52	
SC-5	Denial of Service Protection	42	104	31	78	21	52	
SC-7	Boundary Protection	24	48	24	48	24	48	PNNL assumes the solution for this security control would be the same as the technical solution used in AC-4 "Information Flow Enforcement." This estimate covers the additional hours needed annually to protect data traversing the boundary for DPW systems. PNNL assumes this information is minimal and the boundary protection device would implicitly deny externally initiated connections.
SC-8	Transmission Confidentiality and Integrity	42	104	31	78	21	52	

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
SC-10	Network Disconnect	42	104	31	78	21	52	
SC-12	Cryptographic Key Establishment and Management	16	32	8	16	4	8	Beyond Public Key Infrastructure, PNNL assumes no cryptographic technology will be used on DPW devices or networks. This estimate covers the labor needed to acquire a new certificate from an existing, non-Army certificate authority. This estimate does not cover a loss of functionality to a large number of certificates at one time.
SC-13	Cryptographic Protection	24	72	23	62	17	44	
SC-15	Collaborative Computing Devices	42	104	31	78	21	52	
SC-17	Public Key Infrastructure Certificates	12	36	12	36	12	36	Beyond Public Key Infrastructure, PNNL assumes no cryptographic technology will be used on DPW devices or networks. This estimate covers the labor needed to acquire a new certificate from an existing, non-Army certificate authority. This estimate does not cover a loss of functionality to a large number of certificates at one time.
SC-18	Mobile Code	42	104	31	78	21	52	

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	42	104	31	78	21	52	
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	42	104	31	78	21	52	
SC-22	Architecture and Provisioning for Name/ Address Resolution Service	42	104	31	78	21	52	
SC-23	Session Authenticity	42	104	31	78	21	52	
SC-24	Fail in Known State	42	104	31	78	21	52	
SC-28	Protection of Information at Rest	42	104	31	78	21	52	
SC-38	Operations Security	42	104	31	78	21	52	
SC-39	Process Isolation	42	104	31	78	21	52	
SC-41	Port and I/O Device Access	42	104	31	78	21	52	
SI-2	Flaw Remediation	42	104	31	78	21	52	
SI-3	Malicious Code Protection	12	48	12	48	12	48	PNNL assumes most devices on DPW networks will not support malicious code protection. Traditional workstations used by DPW should be protected using standard Army practices and technologies.
SI-4	Information System Monitoring	42	104	31	78	21	52	

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
SI-5	Security Alerts, Advisories, and Directives	42	104	31	78	21	52	
SI-7	Software, Firmware, and Information Integrity	42	104	31	78	21	52	
SI-8	SPAM Protection	42	104	31	78	21	52	
SI-10	Information Input Validation	42	104	31	78	21	52	
SI-11	Error Handling	42	104	31	78	21	52	
SI-12	Information Handling and Retention	42	104	31	78	21	52	
SI-16	Memory Protection	42	104	31	78	21	52	
SI-17	Fail-Safe Procedures	42	104	31	78	21	52	
PM-2	Senior Information Security Officer	42	104	31	78	21	52	
PM-3	Information Security Resources	42	104	31	78	21	52	
PM-4	Plan of Action and Milestones Process	42	104	31	78	21	52	
PM-5	Information System Inventory	42	104	31	78	21	52	
PM-6	Information Security Measures of Performance	42	104	31	78	21	52	
PM-7	Enterprise Architecture	42	104	31	78	21	52	
PM-8	Critical Infrastructure Plan	42	104	31	78	21	52	
PM-9	Risk Management Strategy	42	104	31	78	21	52	

Number	Title	Large Installation Min	Large Installation Max	Medium Installation Min	Medium Installation Max	Small Installation Min	Small Installation Max	Justification
PM-10	Security Authorization Process	42	104	31	78	21	52	
PM-11	Mission/Business Process Definition	42	104	31	78	21	52	
PM-12	Insider Threat Program	42	104	31	78	21	52	
PM-13	Information Security Workforce	42	104	31	78	21	52	
PM-14	Testing, Training, and Monitoring	42	104	31	78	21	52	
PM-15	Contacts with Security Groups and Associations	42	104	31	78	21	52	
PM-16	Threat Awareness Program	42	104	31	78	21	52	
	Totals:	5,711	14,141	4,303	10,813	3,023	7,485	

Table D.7 is the determination of the total labor hours and estimated FTEs needed to implement the assessed security controls.

Table D.7. Estimated FTEs Needed to Secure DPW Assets

	Range	Mid-Point	Nearest FTE
Small	3,023–7,485	5,254	2–3
Medium	4,303–10,813	7,558	3–4
Large	5,711–14,141	9,926	5

The suggested roles and responsibilities from the Committee on National Security Systems (CNSS 2015) and the U.S. Department of Defense Enterprise Software Initiative required to secure a stand-alone FRCS network include:

- **Project Manager** - Individual responsible for the day-to-day leadership and oversight of the project. The Project Manager works with the project team to oversee the development of the cybersecurity controls for FRCS and coordinates the efforts of each team member. Key activities executed by the Project Manager include planning, status reporting, issue management, scope management, budget management, and quality assurance.
- **Information Assurance Manager** - Individual responsible for the information assurance of a program, organization, system, or enclave. Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise and implements systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including national security systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.
- **Information System Security Officer** - Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program.
- **Information System Security Engineer** - Individual responsible for applying scientific, engineering, and information assurance principles to deliver trustworthy systems that satisfy stakeholder requirements within their established risk tolerance.
- **System Administrator** - Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established information assurance policy and procedures.

The approximate level of effort required to implement cybersecurity controls on stand-alone FRCS is aligned with the FTE roles at a typical Army installation. The implementation effort is based on the size of each installation and does not include the number of FRCS present on an installation.

Table D.8 shows the roles needed to implement security controls for a stand-alone FRCS network on small, medium, and large installations. Not all roles will be needed at every

installation. Specific criteria to choose between two or three FTEs for a small installation or three to four FTEs for a medium installation are not identified in this report.

Table D.8. FTE Roles Alignment to Army Installations

Roles		Army Installation FTEs by Size				
		Small (2-3 FTEs)		Medium (3-4 FTEs)		Large (5 FTEs)
A	Project Manager	A	A	A	A	A
B	IA manager					B
C	ISSO	C	C	C	C	C
D	Security Engineer	D			D	D
E	System Administrator		D	D	E	E

D.1 References

CNNS 2015. *Committee on National Security Systems (CNSS) Glossary*, Committee on National Security Systems (CNSS) Instruction, Number 4009, April 6, 2015.

Appendix E – Asset Valuation of Army FRCS

Pacific Northwest National Laboratory used the inventory data from 31 buildings to estimate the total asset valuation facility-related control systems (FRCS) for an estimated 150,000 Army-owned buildings. The Army provided the 150,000-building estimate to Pacific Northwest National Laboratory. The inventory data set is not an ideal representation of Army-owned FRCS given the sample size is only 0.021% of the estimated population size.

The inventory data set contained 129 devices, of which 89 were unique devices. The cost to replace each device was determined using market research. Table E.1 is a list of the inventory data and their associated replacement costs.

Table E.1. Known FRCS Inventory by Building on Army installations; Specific Models Were Omitted in This Document

Manufacturer	Cost to Replace
Automated Logic	$1,300.00
Dell Monitor	$123.00
Vertx	$1,330.00
Vertx	$792.99
Dell	$95.30
SMC	$561.27
Allen-Bradley	$3,990.00
Allen-Bradley	$253.00
Siemens	$1,254.33
Siemens	$1,530.00
Siemens	$1,233.08
Daikan	$425.00
Tridium Niagara	$4,045.00
NetGear	$19.99
Dell	$3,009.00
Fargo	$1,945.95
Leviton	$1,008.33
LightLEEDER	$1,120.00
Advantor	$1,822.00
Advantor	$276.53
Monaco	$25.00
D-Link	$439.74
E300 02D	$189.00
sierra-sw3	$3,495.00
E300 05C	$2,310.00
sierra-sw4	$2,424.00
LOCAL_S03	$156.00
LOCAL_S04	$1,349.99
sierra-sw1	$2,496.74
sierra-sw2	$2,496.74

Manufacturer	Cost to Replace
Allen-Bradley	$3,590.00
BMS Panelview	$3,599.00
Signamax	$475.39
Sierra-Hist	$2,999.00
Sierra-PASS	$1,250.00
Sierra-OWS-1	$895.41
R02_00	$2,007.90
R03_00	$2,007.90
R04_00	$2,007.90
R05_00	$2,007.90
R06_00	$2,007.90
R07_00	$2,007.90
IS_R01_00	$1,429.00
IS_R02_00	$1,429.00
IS_R03_00	$1,429.00
IS_R04_00	$1,429.00
ACER	$1,699.99
LoyTech	$1,008.00
PowerEdge	$1,429.99
HP	$1,899.99
Cisco	$16,584.99
Cisco	$4,294.00
Cisco	$4,857.35
Cisco	$5,929.99
NEXlink	$84.96
Honeywell/Vindicator	$149.00
Honeywell/Vindicator	$149.00
Cisco	$834.00
Cisco	$881.33
Allen-Bradley	$3,338.00
Allen-Bradley	$3,129.00
Trend	$280.00
Fire Lite	$81.99
HP	$88.99
Honeywell	$148.45
AutoPulse	$626.61
Signamax	$348.75
icpdac	$616.42
SEL	$823.88
SEL	$990.00
SEL	$950.00
General Electric	$750.00
Honeywell	$2,846.18

Manufacturer	Cost to Replace
Sur-gard	$400.00
invensys	$5,000.00
Acheating-PC	$21.95
Prodesk	$820.70
Rauland-bord Corp	$690.66
Rauland-bord Corp	$690.66
Siemens	$460.16
Fire Protection Signaling Service	$344.95
Hubbell Premise Wiring	$126.57
BROCADE	$17,572.99
Ortronics	$169.00
Honeywell	$295.36
Loytec	$462.48
Dell	$1,009.00
Alerton	$2,593.60
BASE ELECTRONICS VM VIGILANT	$1,380.00
Novar	$3,425.00
Honeywell	$178.99
Lenovo	$6,752.31
Niagara	$1,265.00
Cisco	$4,680.50
TP-Link	$79.99
Niagara Talon	$1,349.91
Delta	$231.00
Blackbox	$847.80
IMCnetworks	$205.99
Siemens	$2,072.00
BlackBox	$572.99
VYKON by Tridium Niagara	$1,295.00
Siemens	$7,422.00
Tridium Inc.	$499.00
Allen-Bradley	$1,672.00
wiedmuller	$108.00
Arista	$12,800.88
Honeywell	$760.00
Allen-Bradley	$1,397.00
N-tron	$357.00
Corning	$131.67
BrocadeSwitch	$4,146.99
Honeywell	$6,900.00
Delta	$1,980.00
SEL	$3,940.00
SEL	$2,480.00

Manufacturer	Cost to Replace
SEL	$1,680.00
SEL	$990.00
SEL	$3,100.00
Dell	$232.20
SEL	$450.00
SEL	$960.00

The devices in Table E.1 were searched in vulnerability and exposure databases to determine if known vulnerabilities existed for inventory data. Nineteen unique vulnerabilities were found for the 129 devices. The search criteria were limited to the specific make and model of the device. Other attributes such as operating system, software libraries, major applications, device firmware, and protocols were not researched.

Table E.2 associates the inventory data with their corresponding building and installation. Building totals were used to determine the range of the replacement costs. Table E.3 shows the minimum, maximum, median, and average values the data set.

Table E.2. Inventory and replacement Cost of Known FRCS Used on Army Installations

	Building Total	Location Total
Installation 1		$20,867
Bldg 1	$9,494	
Bldg 2	$6,082	
Bldg 3	$5,290	
Installation 2		$83,163
Bldg 1	$4,243	
Bldg 2	$10,673	
Bldg 3	$5,819	
Bldg 4	$6,074	
Bldg 5	$1,008	
Bldg 6	$7,564	
Bldg 7	$489	
Bldg 8	$47,289	
Installation 3		$263,686
Bldg 1	$75,004	
Bldg 2	$6,917	
Bldg 3	$1,123	
Bldg 4	$4,130	
Bldg 5	$5,506	
Bldg 6	$400	
Bldg 7	$9,883	
Bldg 8	$1,330	
Bldg 9	$18,673	
Bldg 10	$757	
Bldg 11	$9,965	

	Building Total	Location Total
Bldg 12	$8,745	
Bldg 13	$1,330	
Bldg 14	$33,645	
Bldg 15	$12,914	
Bldg 16	$15,340	
Bldg 17	$4,414	
Bldg 18	$36,530	
Bldg 19	$10,210	
Bldg 20	$6,862	
Total	$367,717	

Table E.3. The Minimum, Maximum, Median, and Average Building Values for the Sample Data Set

	Minimum	Maximum	Median	Average
Sample Data Set	$400	$75,004	$6,917	$12,588

Table E.4 shows the estimated asset valuation for the total number of FRCS in Army-owned buildings.

Table E.4. Total FRCS Asset Valuation from All Data

	Minimum	Maximum	Median	Average
Estimated Army Inventory	$60,000,000	$11,250,735,000	$1,037,697,000	$1,888,229,000

The minimum estimated value of the FRCS in all 150,000 Army-owned facilities is $60M.

The maximum estimated value of the FRCS in all 150,000 Army-owned facilities is $11,250M.

Table E.5 shows the same minimum, maximum, media, and average estimated value of all Army-owned FRCS removing outliers.

Table E.5. Total FRCS Asset Valuation, Outliers Removed

	Minimum	Maximum	Median	Average
Estimated Army Inventory	$60,000,000	$4,881,049,500	$911,242,500	$1,156,573,278

Using the median value for the data set, the estimated value of the FRCS in all 150,000 Army-owned facilities is $912M.

Using the average value for data set, the estimated value of the FRCS in all 150,000 Army-owned facilities is $1,709M.

If we remove any data that is more than 2 standard deviations from the mean, then our median and average values become, $1,028M and $1,888M respectively.

The best estimated value range for all Army-owned FRCS using currently available data is:

- A minimum of $60M
- A maximum of $4,881M
- A likely value of $1,888M

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov