AU/ACSC/2019

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

SAFE FROM STUXNET: LEVERAGING AIR FORCE CYBER EXPERTISE TO SECURE INDUSTRIAL CONTROL SYSTEMS AND CRITICAL INFRASTRUCTURE

by

Jenni S. Dorsey-Spitz, Civilian, DAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Raj Agrawal

Maxwell Air Force Base, Alabama

October 2019

Disclaimer

The views expressed in this academic research report are those of the author and do not reflect the official policy or position of the United States government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

Page

FIGURES

Page

TABLES

Page

PREFACE

This research paper is an attempt to merge my experiences at the squadron level within the Civil Engineer career field with my time at the Air Force Personnel Center to help identify possible manpower solutions that would aid in adverting cybersecurity vulnerabilities in respect to Industrial Control Systems and critical infrastructure.

I extend my sincerest gratitude to my husband, for not only his patience and support while I typed away but also to be my sounding board throughout the entire process. I would also like to thank Ms. Lara Schoenenberger for her recommendation to pursue this topic in the first place, her continuous mentorship and friendship.

Finally, I extend my appreciation to my research advisor Dr. Raj Agrawal and my classmates who provided extremely valuable feedback who helped shape this research paper into the final end product. Thank you!

ABSTRACT

Over the years, technology has been integrated into a wide array of systems that the United States Air Force (USAF) relies on for sustainment, such as generation of electricity, distribution systems for drinking water, and in-home/consumer systems (e.g., air conditioning), temperature regulating equipment necessary to cool data centers, and server rooms to support technology capabilities. These systems depend on Industrial Control Systems (ICS) to provide real-time control and monitoring capabilities. ICS are vital in operating critical infrastructure to support assets, provide capabilities, and execute the mission. The Civil Engineer (CE) career field is responsible for establishing, operating, maintaining, and protecting installations and ICS. However, CE currently does not have the expertise to implement cybersecurity to protect ICS from attacks and vulnerabilities and relies on support from other units and organizations, which either do not have sufficient manning to support or can result in delays to restore capabilities. The vulnerabilities and mission impacts on critical facilities and functions raise the question: what are the best uses of Information Technology Management (2210) civilian job series to implement and maintain cybersecurity at Air Force installations to prepare for and conduct multi-domain command and control (MDC2)?

The problem/solution framework was used to analyze the requirements of mitigating cybersecurity vulnerabilities in ICS and potential manning solutions to determine whether embedding 2210 personnel into CE units to provide local, organic capabilities is the best option to support MDC2. The research identified four possible alternatives to meet cybersecurity requirements. However, when evaluated against the set criteria, a hybrid solution between assigning positions and permanently establishing 2210 is recommended as the best-proposed alternative to mitigate both short and long-term risk.

INTRODUCTION

Industrial Control Systems (ICS) are increasingly susceptible to cybersecurity attacks. In 2016, cyberattacks on ICS increased over 110%.[1] Over the past two decades, industry has integrated technology into a wide array of systems that society uses on a daily basis to improve functionality and efficiencies. If this trend persists, developers will continue to optimize technology to improve the way the general population uses systems. United States Air Force (USAF) installations rely on many of these systems for sustainment, such as generation of electricity, distribution systems for drinking water, and in-home/consumer systems (e.g., air conditioning), computer room air conditioning (CRAC) units necessary to cool data centers, and server rooms to support technology capabilities, depend on ICS.

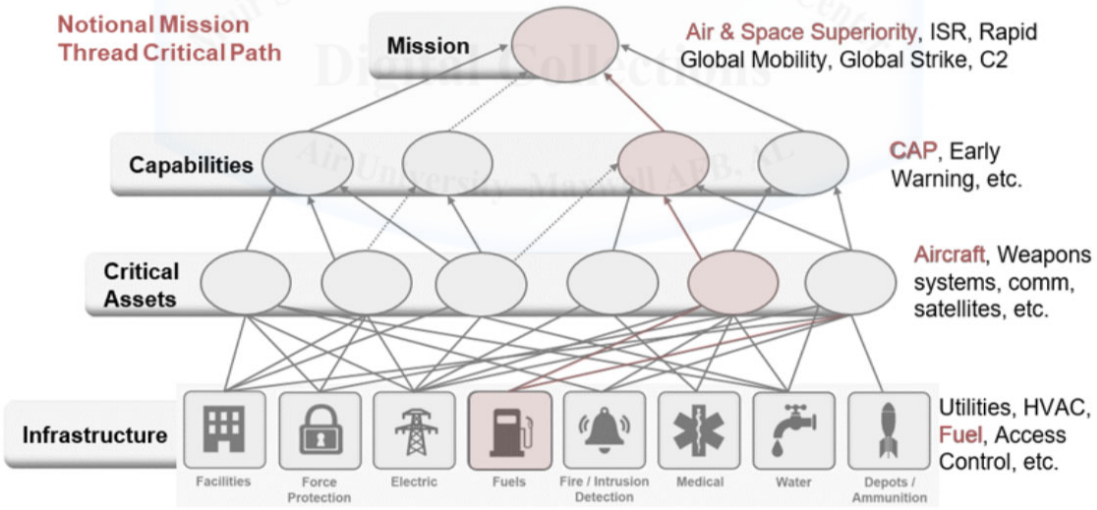

Figure 1. USAF mission dependency on infrastructure[2]

ICS provide supervisory control, data acquisition, and monitoring functions in order to achieve the desired output to enhance industrial processes. Additionally, ICS deliver real-time control and monitoring capabilities of all of these systems to ensure a system operates safely, especially if it detects an abnormality. ICS are vital in operating critical infrastructure to support assets, provide capabilities, and execute the USAF mission. For example, a cyberattack on ICS

not only disrupts fuel services, but may ultimately hinder mission capabilities and impact the mission to obtain Air and Space Superiority (Figure 1).

The Civil Engineer (CE) career field is responsible for establishing, operating, maintaining, and protecting installations that enable all USAF missions.[3] USAF leaders leverage Information Technology Management Series (2210) series to perform critical IT functions to cyber and cybersecurity. However, CE currently does not have the 2210 expertise to implement cybersecurity to protect ICS from attacks and vulnerabilities, which could cause critical infrastructure that enables mission operations to fail. The vulnerability and mission impact raises the question: what is the best use of 2210s to implement and maintain cybersecurity at USAF installations to prepare for and conduct Multi-Domain Command and Control (MDC2)?

In a MDC2 environment, USAF leaders can expect state and non-state actors to target their installations via traditional and non-traditional means. Therefore, USAF must embed expertise to protect and quickly restore capability of critical assets and restore normal operations necessary to project power from in order to conduct MDC2.[4] Manpower personnel argue that CE has Computer Clerk and Assistant (0335) personnel to perform IT-related work; however, this series does not include the technical competencies the 2210 series requires to identify system vulnerabilities.[5] The Communications and Information (C&I) career field holds the 2210 series to provide expertise and cybersecurity functions for installation networks. However, C&I does not have sufficient manning to support the daily operations for the ICS that CE operates and maintains, resulting in increased vulnerabilities and risk and delays in restoring capabilities.

Thus, the USAF must embed 2210 personnel into CE units to execute cybersecurity of ICS and support MDC2.

This research report will utilize a problem/solution framework to address the stated research question to identify the best use of 2210 personnel to implement and maintain cybersecurity with ICS to prepare for and conduct MDC2. First, the research paper outlines the current vulnerabilities associated with ICS. Second, the following section introduces the reader to the Office of Personnel Management (OPM) and the established requirements for occupational series, qualifications, and duty responsibilities; and regulatory and policy requirements for cybersecurity. The OPM guidance and cybersecurity requirements will generate specific criteria for positions needed to mitigate ICS vulnerabilities. And lastly, after the development of specific criteria, this research report will formulate alternatives and recommendations to the stated question that best meets the criteria.

This research begins with a background section, which addresses the current state of manpower within the Air Force and associated vulnerabilities. Next, the problem/solution will provide the framework through a discussion of research methodology, cybersecurity requirements, and establish the set criteria to evaluate proposed alternatives against. Then, in the analysis section, each proposed alternative will be evaluated against the set criteria. Finally, in the conclusion and recommendations sections, suggestions are made based on the results of the evaluation and analysis of the proposed alternatives to resolve manpower shortfalls.

BACKGROUND

Overview of Industrial Control Systems (ICS)

The USAF depends on critical infrastructure to support and execute its mission. These services include, but are not limited to, electric, water, and communication utilities and systems. ICS provide supervisory control, data acquisition, and monitoring functions in order to achieve the desired output to enhance industrial processes. ICS can either be fully automated or assist human operations and are vital to the operation of critical infrastructure.[6] Without ICS, the USAF's ability to effectively and efficiently cool server rooms supporting communications equipment, provide electricity to mission-critical facilities, or distribute water to the base population would be disrupted temporarily until CE implements responsive methods such as manual controls.

The emergence of system controls and industrial automation started during the industrial age and continued to evolve throughout the 1800s.[7] Despite industrial automation, ICS were predominately linear, simple "on-off" controls until the 1950s when engineers linked the control systems to data processing machines (computers) and greatly improved the reliability and functionality.[8] Today's modern controls, information technology (IT) has replaced many of physical components and controls of these systems. The IT evolution and implementation of "smart" technology has dramatically cut costs by improving preventative maintenance programs, providing remotely controlled systems to save on manpower, and other real-time system monitoring services.[9] These once isolated systems are now more interconnected to provide monitoring and control from a centralized location. While technology greatly improves efficiencies, the systems are now more open and vulnerable to cyberattacks.

Cyber Risks and Requirements

In 2017, President Donald Trump issued Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This EO outlines three focus areas: Cybersecurity of Federal Networks, Cybersecurity of Critical Infrastructure, and Cybersecurity for the Nation in order to defend and provide additional capabilities to increasing threats against the United States.[10] While EO 13800 acknowledges the looming risks and criticality of defending the critical infrastructure against cyber threats, it does not put forth any clear guidance on policy and risk management. It does, however, task government agencies on establishing policy and identifying "…how federal capabilities and authorities can best support specially designated critical infrastructure entities."[11] As the USAF meets this EO through various policies and guidance documents identified below, they do not specify the manpower resources to support current cybersecurity needs for ICS.

In addition to EO 13800, the *2018 National Defense Strategy* discusses that today's security environment is becoming increasingly more challenging and complex. The implementation of newer technology is changing the method in which the United States fight wars. Likewise, non-state actors are using such sophisticated capabilities against the United States and its allies, including cyber-hackers that are causing mass disruption through cyber activity against personal, commercial, or government infrastructure.[12] This risk not only impacts military operations but might damage critical public services that support military installations, such as drinking water and electrical systems. As a result, the *National Defense Strategy* outlines key priorities, to include investing in "…cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations."[13] Investments not only include technology capabilities but also cultivating workforce talent in order to have a lethal,

agile and highly skilled force to integrate new capabilities.[14] Also mentioned is creativity and change to business practices in order to ensure the talent of the American warfighter is ready to achieve mission objectives. In the end, it is a collection of new technological capabilities both in the software and hardware arenas, as well as experienced cyber warfighters are needed to secure this domain. Therefore, to support MDC2 operations, the USAF must invest in both its infrastructure and personnel to operate it.

The Unified Facilities Criteria (UFC) 4-010-06, *Cybersecurity of Facility-Related Control Systems,* is an additional source that provides requirements for incorporating cybersecurity into the design of facility-related control systems, which are used to monitor and control equipment ranging from building control systems (i.e., utility control and fire and life safety controls) to manufacturing control systems.[15] The UFC defines specific parameters for the design of control systems, incorporating cybersecurity into the design, and requirements for documenting cybersecurity aspects. Furthermore, it addresses implementing a risk management framework resulting in "…(i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system."[16] Despite the UFC identifying the type of specific roles, such as the system owner who is responsible for the operation and maintenance of an information system, it does not outline where organizations should place these positions. This is consistent across the variety of sources that outline processes, design standards, the risk management framework, and other important factors of industrial control systems and critical infrastructure as they pertain to cybersecurity (Appendix A).

Air Force Instruction (AFI) 17-101, *Risk Management Framework (RMF) For Air Force Information Technology (IT),* provides implementation instructions for the RMF methodology

for IT systems to align with governing federal and DOD guidance. While the USAF cannot eliminate every cyberattack, the RMF provides a framework to assess system vulnerabilities and propose a corrective action plan to mitigate risk. To meet increasing cybersecurity requirements, the USAF must have a robust risk assessment and management process.[17] As a result, AFI 17-101 outlines specific roles and responsibilities to achieve cybersecurity of IT systems (Table 1).

With the widespread integration of IT into CE owned and operated ICS and mission dependency, USAF issued an Air Force Guidance Memorandum (AFGM) 2019-32-02, *Civil Engineer Control Systems Cybersecurity,* to establish unique operational requirements to mitigate cybersecurity risk. AFGM highlights the need to follow the RMF and further refines the roles and responsibilities (Table 1). One of the CE specific roles is for the Base Civil Engineer to appoint an ISO for the installation.[18] Although additional details on where the PM, ISSM, and ISSO are located within the installation are not explicitly identified, they are most likely within the CE organization as they directly support and advise the ISO. However, in order to serve in the roles specified, the individual(s) must possess the knowledge, skills, and abilities to implement the cybersecurity requirements and may require a certification, which current desktop support technicians embedded within CE units are not required to have.

Table 1. Roles and Responsibilities for Cybersecurity

Role	Primary Cyber Responsibility	Additional CE Cyber Requirements
Authorizing Official (AO)	Official responsible for implementing RMF for systems in their area of responsibility, accepting various levels of risk, and advocates for cybersecurity resource requirements. Review security authorization packages. Must be O-7 or SES at a minimum and completes training and	Responsible for managing the risk and may tailor controls to balance security and availability.

	certification IAW Air Force Manual (AFMAN) 17-1303.	
Security Control Assessor (SCA)	Security assessor to ensure continuous monitoring. Prepares documentation on issues and provides recommendations as required. Must be at least an O-4 or GS-12 and authority within the area of responsibility for the assessment determination. Complete training and cybersecurity certification IAW AFMAN 17-1303.	Responsible for making assessment determinations and authorization recommendations to the AO.
Information System Owner (ISO)	Official responsible for the overall procurement, development, integration, modification, and operation and maintenance of AF IT.	Ensure execution of the ISO responsibilities are satisfied for CE-owned, operated, and maintained CS.
Program Manager (PM)	The ISO is assigned the PM duties when no PM is assigned. Identify, implement, and ensure full integration of cybersecurity into all acquisition life cycle phases.	None specified
Information Systems Security Engineer (ISSE)	ISSE is an individual, group, or organization responsible for conducting information system security engineering activities. Captures and refines information security requirements and ensures the requirements are effectively integrated into IT products and information systems.	None specified
Information Systems Security Manager (ISSM)	Primary cybersecurity technical advisor to the AO, PM, and ISO. For base enclaves, the ISSM manages the installation cybersecurity program. Complete and maintain required cybersecurity certification IAW AFMAN 17-1303	Ensures the ISSM responsibilities are satisfied for CE-owned, operated, and maintained CS. Supports the ISO.

Information Systems Security Officer (ISSO)	Responsible for ensuring the appropriate operational security posture is maintained for assigned IT. Includes activities related to maintaining situational awareness and initiating actions to improve or restore cybersecurity posture. Complete and maintain required cybersecurity certification IAW AFMAN 17-1303	Ensures the ISSO responsibilities are satisfied for CE-owned, operated, and maintained CS.

_____
Adapted from AFGM 2019-32-02, *Civil Engineer Control Systems Cybersecurity*, 5 September 2019, 6 and AFI 17-101, *Risk Management Framework (RMF) For Air Force Information Technology (IT)*, 2 February 2017.

Current Situation and Vulnerabilities

IT systems that lack security controls are vulnerable and have significant risk if compromised. The more interconnected a system is, the more devastating an attack can be on the system. ICS rely on a combination of communication networks in order to be interconnected to computing systems and servers to provide control and monitoring. Initially, ICS were isolated systems; however, to improve efficiencies, these systems are now interconnected to other controls, which communicate over a shared network. Additionally, these systems often have multiple remote access and wireless networks that offer entry points into the IT system, not only for the particular equipment but into the Ethernet and IP network. Despite the advantages IT emergence into ICS provide, the interconnected system increases cybersecurity risks and vulnerabilities. Moreover, as many ICS impact critical infrastructure supporting daily operations, the greater the need is to secure and protect these systems. Failure for the USAF to do so may lead to other impacts.

For example, hackers might access the environmental controls network through unprotected points for heating, ventilation, air conditioning (HVAC) systems, which results in the disruption of heating or cooling and could lead to equipment failure. HVAC and related

CRAC systems are specially designed to ensure precise control of temperature and humidity for server and data center rooms for optimal performance.[19] HVAC and CRAC systems outages could impact IT processes of sensitive and classified data (non-classified internet protocol router network (NIPRNet) and secret internet protocol router network (SIPRNet)) and disrupt functions such as MDC2. Furthermore, if a hacker can penetrate and gain access to the HVAC system, the interconnected system allows access to other IT systems throughout the shared network, creating significant vulnerabilities within the system that range from system intrusion to kinetic effects.

In addition to current potential vulnerabilities, another area of concern is the inability to monitor the ICS security controls effectively in support of the RMF. Continuous monitoring of current security protections is necessary for mitigating and quickly responding to any cyberattacks. While current guidance identifies some roles and responsibilities, the AFGM states that further roles and responsibilities are still needed to determine how best to coordinate for incident response and automated continuous monitoring of ICS.[20] The vulnerabilities ICS present, in addition to the lack of certified individuals and unclear guidance of incident monitoring and response, strongly justifies the need to provide personnel with the skillsets necessary to support IT and cybersecurity requirements for ICS.

Case Studies and Results of Improper Cybersecurity

In addition to individual targets, the risk of system-wide infiltration and attacks can also occur, such as Stuxnet in 2010. In June 2010, multiple industrial sites in Iran were attacked by a computer worm adept at not only collecting data on the infrastructure but capable of taking over the systems and causing physical damage.[21] Security experts believe Stuxnet was uploaded to the network by someone inserting an USB, which then quickly spread throughout the network.[22] The targeted facilities included Iran's uranium-enrichment plant, which from there the malware

continued to spread and proliferate throughout the local network system. Although Iran never reported physical damage of the uranium-enrichment plant centrifuges, Stuxnet is one of the first publicly-acknowledged cyberattacks to supervisory control and data acquisition (SCADA) systems.[23] Besides the direct threat to the assets SCADA systems manage, they can also be a vulnerable hole into the rest of the network. SCADA and other ICS were not designed with security in mind as they communicate with a variety of equipment and sensors.[24] The number of equipment and connections to support the operational technology of the ICS present a possibility for several vulnerable access points for which a state or non-state actor can target for a cyberattack (see Figure 2).[25] Once into the system, the attacker can then reach other IT assets, compounding the magnitude of the attack as demonstrated with Stuxnet.

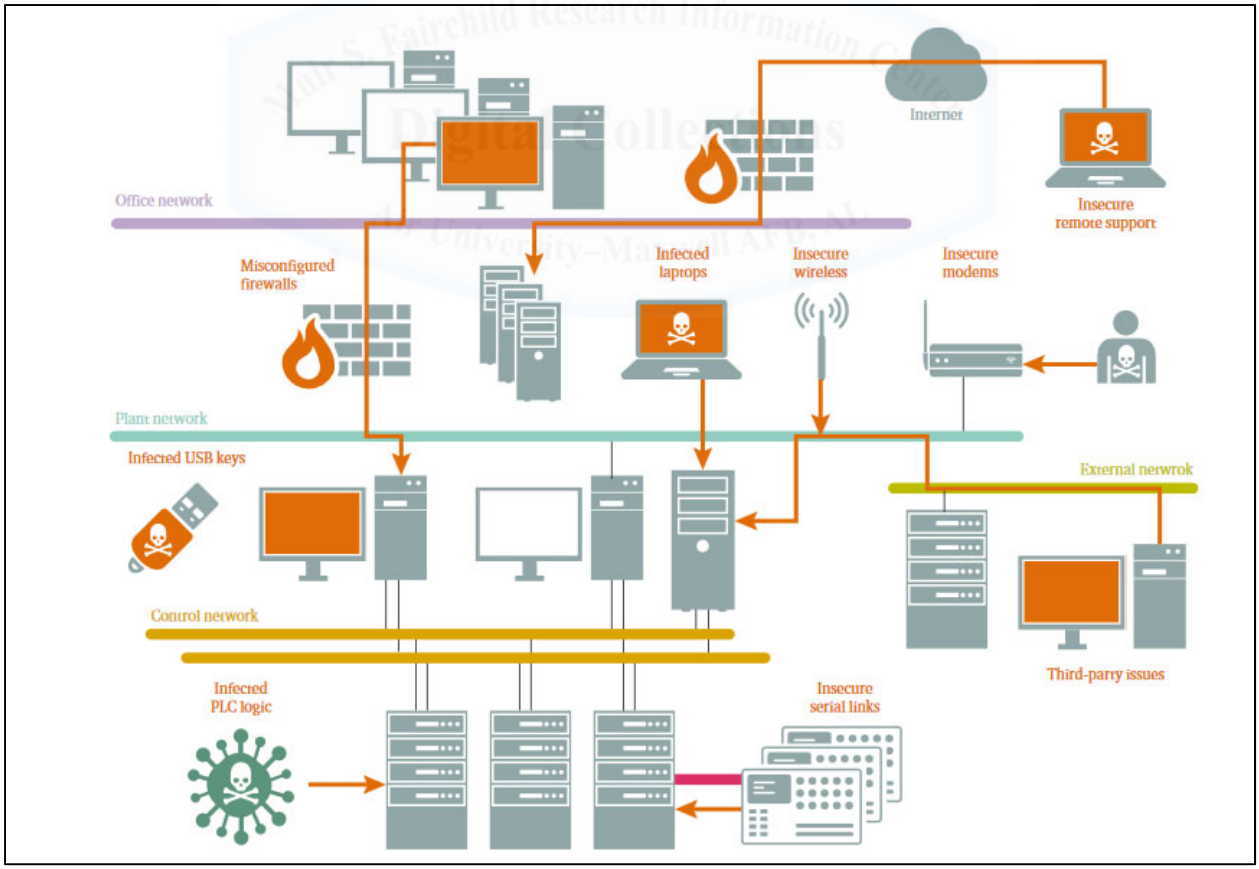

Figure 2. Potential ICS vulnerabilities[26]

Since Stuxnet, attacks to ICS have steadily risen.[27] For example, a cyberattack caused physical damage to a steel mill in Germany in 2015.[28] Hackers took operational control over the blast furnace's ICS causing it to overheat, which operators could not override. Perhaps more troubling is that it was the second unobstructed attack on the ICS at the facility. Therefore, ICS not only require trained and skilled operators, but also cybersecurity specialists to implement to defend and monitor the system from such attacks and vulnerabilities. Similar attacks should be concerning to the DOD.

In a 2018 Federal Cybersecurity Risk Determination Report and Action Plan, the Office of Management and Budget, in coordination with the Department of Homeland Security (DHS), recognized the impacts of limited resources on federal agencies' ability to mitigate cybersecurity risks.[29] Additionally, the report found that a significant number of agencies are unable to dedicate the necessary personnel and resources to defend their systems.[30] In a 2017 interview, Lucian Niemeyer, Assistant Secretary of Defense for Energy, Installations and Environment, stated he believes energy grids supporting military installations are too vulnerable to cyberattacks.[31] Military installations must take action to assess, mitigate, and protect ICS supporting critical infrastructure.

In light of DOD concerns over defending and combating against cyberattacks, other studies have focused on the gaps within the current framework and propose new solutions. In one research paper, *United States Cybersecurity Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment?,* William K. Tirrell, LCDR, USN argues that despite the emphasis on cyberattacks, the response has fallen short and is vulnerable to attacks.[32] He uses critical infrastructure and the industrial control systems as examples of devastating vulnerable areas and proposes changes in order to improve interagency collaboration through

policy revisions and transforming the cybersecurity organization. While he argues the proposals will aid in advancing a robust national cybersecurity effort and better align strategy and policy, it does not get into the details of how to implement on an operational level, as the ICS are not centralized and CE often operates and maintains the systems locally. The USAF finds itself in a similar position with identifying what needs to be done to protect its ICS network, but as the cyber domain evolves the DOD still needs to develop specific roles and responsibilities at the operational level.

In effort of mitigating cybersecurity risks, other USAF specialties have investigated the need to appropriately and effectively support manning requirements to accomplish cyber operations. In [Air Force Office of Special Investigations (*AFOSI)] Cyber Threat Pursuit: The Air Force's 'Outside the Box' Response to Cyber Exploitation,* by Daron M. Hartvigasen, the author takes the problem/solution framework to address the need to invest further and provide additional resources, including manpower, and update policy impacting the AFOSI to support cyber threat pursuit capabilities. Mr. Hartvigasen highlights that despite the increased production of cyber operations and mission (e.g., Air Force Cyber (AFCYBER), 24th and 25th Air Force) in response to increasing attacks to IT and computer systems, AFOSI did not gain any additional funding or manpower.[33] While AFCYBER and the other agencies provide support to cyber operations, they are limited when it comes to threats outside Air Force networks, especially those during peacetime.[34] Furthermore, a recent congressional research report confirmed that AFYCYBER and USCYBERCOM are both incomplete when it comes to engaging cyber threats, particularly those that are conducted by unknown actors.[35] AFOSI is the bridge between the defensive capabilities these entities traditionally provide and the offensive maneuvers of the intelligence community (i.e., *warriors*). Therefore, the author argues, the Air Force must invest

and provide additional manpower to AFOSI in order to provide "…in-house capability to operate against cyber threats when attribution is ambiguous, and when military operations are not an option."[36] In addition to providing cyber positions to AFOSI, he also mentions USAF policy warrants revision to integrate AFOSI into the USAF's core cyber functions in order to enable the right tools to be effective in defending and responding to threats across the cyber spectrum. Similarly, with the nature of ICS and potential access points to the IT network, the USAF must provide the proper tools and resources to protect and defend against cyberattacks.

Despite recent reports, case studies highlighting the vulnerabilities, and the comprehensive guidance on operating and protecting ICS, the USAF currently does not clearly define support or manpower requirements to effectively cover the extensive list of cybersecurity responsibilities as outlined in Table 1. Currently, 2210s are often held within the Communications and Information (C&I) career field and do not sit in other units, such as CE. Although CE operates and maintains systems (e.g., ICS) that require significant cybersecurity requirements, they do not have the 2210s to perform this work. Furthermore, C&I does not have manning to support the daily operations, resulting in vulnerabilities to cyberattacks.

While the AFOSI case study focuses more on the counterintelligence activities required to fully be able to respond and defend against cyberattacks, it highlights and serves as an example that despite the tools within the USAF portfolio, additional in-house capabilities are needed to fill the gaps between AFCYBER and related missions and unit, specific operations.

IDENTIFICATION OF CRITERIA AND REQUIREMENTS

The key criteria used to evaluate each proposed alternative include: complying with federal law on the type of position (classification) and associated duties, responsibilities and qualifications; certification requirements to perform the cybersecurity tasks as outlined by USAF policy; and possessing the operational knowledge of ICS to guarantee functionality of the system. These three areas are further defined in the subsections below.

Position Classification Requirements

The USAF needs to assign individuals to a position and provide guidance on the responsibilities related to ICS and cybersecurity. Similar to many government actions, decisions pertaining to personnel actions are regulated under federal law to provide unity and standardization. Title 5, United States Code (U.S.C.) is the law that governs the type, level of difficulty, and responsibility (classification) of positions in the Federal government.[37] The United States Office of Personnel Management (OPM) is the office that manages, provides policy directives and guidance for the government's civilian workforce to comply with 5 U.S.C. The USAF must follow OPM policy and ensure individuals are not performing duties outsides their position classification as it would be a violation of the law.

To assign cybersecurity duties to an individual, USAF leadership must be familiar with OPM guidance and policy to stay compliant. OPM's *Handbook of Occupational Groups and Families* provides information on occupational job descriptions and qualification requirements, which are designated by job series. Similar to Air Force Specialty Codes (AFSCs), Occupational Series consists of positions similar to the specialized line of work and qualifications required to perform the job. Information Technology Management (2210) is the occupational series OPM defines as individuals who "…manage, supervise, lead, administer, develop, deliver, and support

IT systems and services."[38] The USAF leverages the 2210 series to perform critical IT functions to cyber and cybersecurity. Another series that often performs IT-related work is the Computer Clerk and Assistant (0335). However, this series does not include the technical competencies to "…for which the paramount requirement is knowledge of IT principles, concepts, and methods; e.g., data storage, software applications, and networking" and proper certifications, according to OPM.[39] Moreover, paragraph 2301(b) of title 5 of the U.S.C. protects personnel from performing work outside their duties, and as such, 0335s cannot perform job duties that OPM classifies to fall within the 2210 series. For CE to meet the demanding requirements of RMF into ICS, leaders must properly assign the appropriate roles and responsibilities, which may fall under the responsibilities of a 2210 versus a 0335.

Cyber Certification

Individuals performing cybersecurity duties are required to have a baseline certification to demonstrate a common understanding of concepts, principles, and application of cybersecurity requirements. AFMAN 17-1303 outlines the commensurate certification level related to various duties and access rights for organizations to assign personnel.[40] The DOD mandates the level of certification to provide a clear indicator of the type of training and education necessary to be qualified to use, operate, administer, maintain, and defend DOD systems.[41] All USAF personnel are required to accomplish a particular level of training if they access a DOD system. For most users, the annual cybersecurity user awareness training through the Advanced Distributed Learning Service (ADLS) will be the extent of the training requirements. On the other hand, cybersecurity personnel with access to installation enclaves require to obtain and maintain an Information Assurance Technical (IAT) level I cybersecurity baseline certification at a minimum.[42] Other certification and position requirements, such as security clearances, also apply

depending on the installation. To effectively operate and defend ICS against cybersecurity incidents, CE requires certified personnel to demonstrate the foundational knowledge of securing the system.

ICS Knowledge, Skills, and Abilities

ICS are unique in the aspect that they are not centralized and vary in the type and lifecycle phase that occurs at each installation. Currently, there is no program management office to provide standardization of cybersecurity measures; therefore, with the help from Air Force Civil Engineer Center (AFCEC), installations are required to define and verify requirements into the design of the system.[43] The UFC 4-010-06 provides guidance on acquisition or replacement of such ICS, but to ensure cybersecurity requirements are fully met, the ISO is there to oversee all processes and procedures.

To balance both functionality and security, the individual in the ISO role needs to have a unique mixture of IT and ICS knowledge (see Figure 3). Beyond the daily operating procedures, the individual needs to have robust IT knowledge regarding the operating systems sufficient to troubleshoot, test and maintain those systems to optimize the functionality and ensure the reliability of servers. ICS include a wide array of systems, to include cathodic protection, natural gas distribution, fire suppression, and airfield lighting control systems, the position must be able to consider both the operational and cybersecurity aspects to balance security controls without hindering performance and reliability.[44] If the individual takes a conservative approach and hardens the system

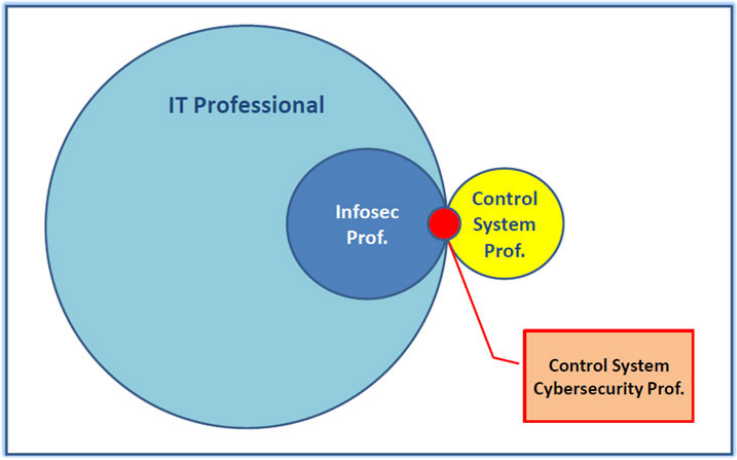

Figure 3. Knowledge requirements to maintain functionality and cybersecurity

too much, the ICS cannot communicate with the rest of the system and functionality is loss. However, ICS require a degree of security to minimize the number of pathways for intruders to enter and impact critical infrastructure.

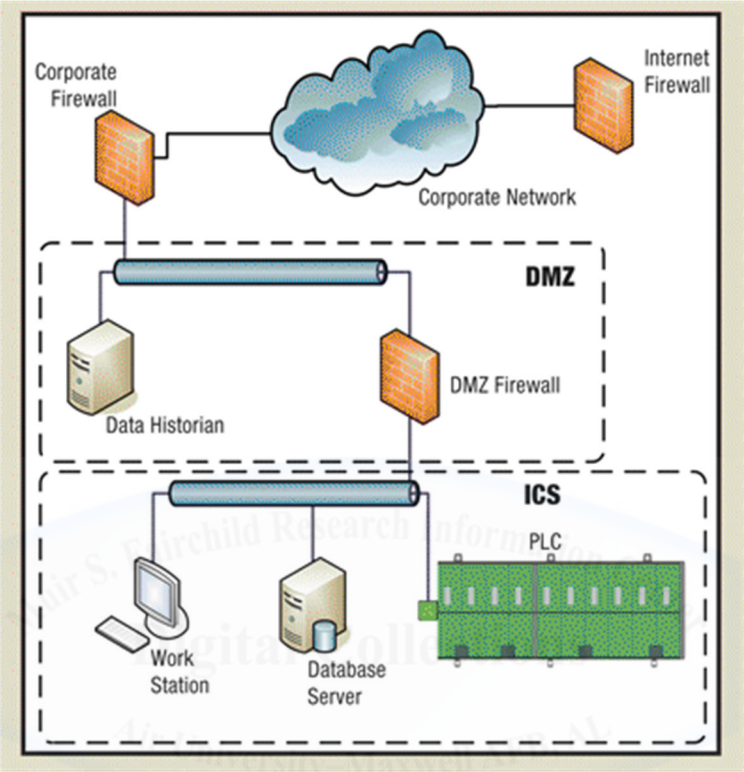

Figure 4. Example ICS network

Additionally, the individual must be proficient with a full range of ICS database management concepts and approaches used to meet current and future organizational business requirements, while balancing cybersecurity requirements to meet RMF methodologies specific to that location. To do so, the individual must understand the entire ICS network (see Figure 4) to determine where to establish firewalls to defend the system and where to allow open communication between the programmable logic controller (PLC) that manages the sensors and actuators of equipment and the work station for the operator to provide input. The person must have corporate knowledge of the CE enterprise and a comprehensive understanding of both

cybersecurity and ICS in order to meet both requirements without compromising the support CE provides to its mission partners.

Funding Required

The U.S. President must allocate funding in the budget for the DOD to sustain the President's commitment to protect America's security and provide military readiness to deter and defeat future threats to the Nation's security.[45] The USAF's Fiscal Year (FY) 2020 budget request was approximately $165.6 billion dollars, which includes a 6% increase from FY 2019.[46] Although the USAF did receive an increase, it targeted the majority of the additional funding to recruit, train, and develop Airmen on leading in MDO and fill critical manpower shortfalls, such as pilots.[47] To request additional funding to support civilian personnel requirements, the USAF would need to prioritize it in its Program Objective Memorandum (POM). The POM covers a 5-year time period and is typically completed 2-years or more out from executing the requirement.[48] While there is not a restriction from requesting funding to support additional manpower requirements or contractor support, the amount of funding required and the duration until the USAF receives its POM request needs to be a consideration in the proposed solution as the action is contingent upon funding.

Another funding consideration is the potential for the DOD to reallocate internal resources to support other requirements. For example, despite the increase in funding for FY20, the Pentagon recently announced it will use $3.8 billion in military construction funding to pay for a border wall to support National Security objectives.[49] This potential expense could impact whether or not the USAF can allocate funding to one or more of the possible solutions mentioned below.

Timeline to Implement

As the Assistant Secretary of Defense for Energy, Installations and Environment mentioned, military installations are extremely vulnerable to cyberattacks and must take action now to assess, mitigate, and protect ICS supporting critical infrastructure.[50] Therefore, the USAF must consider how long the solution would take to implement. Each potential solution must consider both the short-term and long-term duration. The short-term implementation addresses the immediate need to mitigate current and known threats while the long-term supports the further development and sustainment of services that protect the ICS. In the short-term, the Air Force will need to look at what organic capabilities exists that it can leverage to combat cybersecurity threats while simultaneously planning, resources and executing the long-term version. The longer the delay to implement a sustainable solution, the more at-risk ICS are to cyberattacks.

ANALYSIS OF POTENTIAL SOLUTIONS

No Action Alternative - Status Quo

CE currently does not have the capabilities to fully implement the requirements of RMF in accordance with DODI 8510.01, AFI 17-101, and AFGM 2019-32-02.[51] In response, the Chief, Information Dominance and Chief Information officer (SAF/CIO A6) approved a deviation from the RMF for the CE Career Field while the Air Force Civil Engineer (A4C) leaders and A6 work together to determine the best path forward.[52] A4C crafted an interim solution, which splits the responsibility between the AFCEC Operations Maintenance Division (AFCEC/COO) and the installation's Base Civil Engineer (BCE), who also fills the role of the squadron commander. AFCEC/COO provides the technical support and conducts vulnerability assessments while the BCEs are responsible to own, operate, and maintain ICS, in addition to, mitigating risks and vulnerabilities generated from the assessment.[53] Once the cybersecurity risk assessment is complete, it is up to the installation to implement the risk mitigation actions, which falls on the BCE. As the BCE is also the squadron commander, it is unlikely the BCE is also performing all of the duties necessary – risk mitigation is likely delegated down to other personnel within the CE squadron.

Most CE squadrons have Computer Clerk and Assistant (0335) positions assigned to perform various data processing support and services functions associated with computer systems. These individuals support the ICS operators with IT-related tasks such as managing assets, programming, and desktop support, but they do not meet the demanding requirements that RMF requires as identified in Table 1. Some 0335s may obtain the DOD 8570 certification and perform the cybersecurity functions to comply with RMF, while others do not have the certified personnel and accept operational risk.

A significant benefit to USAF leadership keeping with status quo is the funding and timeline as no additional actions are required. Additionally, the IT personnel that currently assist and support the ICS operators have the ability to gain the ICS knowledgebase—if they do not have it already—to maintain functionality of the systems, on top of computer systems and data processing proficiencies. With the general mix of IT security and control systems knowledge, they may become proficient in control system cybersecurity. Moreover, they have reach-back support from AFCEC for assistance with conducting cybersecurity risk assessments and identifying mitigation measures.

Despite the advantages, this course of action includes two deficiencies with respect to the cyber certification and position classification requirements. As of July 2019, approximately 45% of the IT personnel within CE are 0335s (not including unfilled positions).[54] The 0335 standard core personnel document (SCPD) that outlines the position requirements does not include a cyber certification.[55] While the individual could obtain the cyber certification on their own, the SCPD does not require it making it difficult if not impossible to retain this capability. Moreover, as identified under the criteria, Title 5 of the USC prohibits individuals in the 0335 series to perform duties that are covered under a different classification (2210).[56] Therefore, nearly half of the workforce should not perform the cybersecurity functions in accordance with the law. Continuing with the status quo either results in installations lacking sufficient manning to perform the necessary cybersecurity functions or potentially breaking the law.

Assign 2210s to the CE Mission

An alternate action to the status quo is for the C&I to assign 2210s to protect the ICS network and support the CE mission. The action involves C&I career field moving the position(s) from the Communications Squadron to the CE Squadron, rather than CE obtaining

additional manpower. One possible method to move position(s) and personnel is for Headquarters Air Force CE (HAF/A4C) to issue a global memorandum of agreement (MOA) to support the action across all installations. The MOA would outline the agreement between C&I and CE to lend 2210s to support cybersecurity requirements within CE squadrons. The 2210s would possess the required certifications necessary to implement risk mitigation actions and comply with RMF. The size of the installation and scope of ICS will determine the number of personnel needed to reduce overall risk to the systems. The Air Force Personnel Center (AFPC) would need to develop a unique position description to outline the specific ICS requirements. While the 2210s would be in CE, they would still be covered under the C&I career field to maintain the integrity of the position in respect to cyber training requirements, certification, accountability, and oversight.

Assigning 2210s to CE meets three of the criteria: position classification requirements, cyber certification and funding. Unlike the status quo action, this proposed solution would meet the law by having individuals perform duties under the appropriate series and the 2210 series requires a cyber certification.[57] Furthermore, as this action does not include adding more positions or changing the series, additional funding is not needed. A gap in the criteria is the ICS knowledge. As the position is coming from the C&I career field, the individual may not have any experience with ICS systems as they are unique to CE. As they learn ICS and how to balance the requirements between functionality and security, the timeline to have full capability may vary depending on the individual. Additionally, as the action is supported by a MOA, new leadership or changes to C&I mission could influence them to back out of the MOA, pulling the 2210s out of CE. Implementing this course of action would meet the top criteria necessary to provide

cybersecurity support to ICS, but may require additional time to implement the MOA and allow for ICS-specific training and familiarization and may not provide a permanent solution.

Permanently Establish Cyber Support Positions within CE

Another option to garner local, organic capabilities for cybersecurity/IT expertise is for Air Force Manpower, Personnel and Services (A1) to permanently establish 2210s within CE. The action would require additional manpower authorizations to support the roles and responsibilities listed in Table 1. Once A1 added the manpower authorizations to the unit manning documents (UMD), AFPC would need to create position descriptions to highlight the requirements needed to implement RMF requirements for ICS to support critical infrastructure. Similar to the alternate action of communication squadrons assigning 2210s to CE, C&I would still have oversight of the position to maintain training and certification requirements in accordance with DOD 8570 and AFI 17-101. The size of the installation and scope of ICS will determine the number of personnel needed to improve overall risk to the systems.

In like manner of C&I assigning 2210s to CE mission, A1 permanently establishing 2210s also meets the two top criteria: position classification and cyber certification requirements. This action also allows the hiring manager to recruit new individuals into the position that may have familiarity or experience with ICS. On the other hand, the timeline to implement this solution is significantly greater than other options because of the timeframe for A1 to add the manpower authorizations and hiring managers to recruit and fill the vacancies. The timeframe directly impacts the duration of how long ICS remain vulnerable to cyberattacks. Additionally, USAF would need to prioritize funding to support the increase manpower requirement.

A mitigation consideration is for CE to swap the 0335 manpower authorizations for 2210s. While this would aid in cutting down the timeframe, additional funding is still required.

The 2210 series is covered under a special salary rate to aid in recruiting and retaining cyber-expertise. For example, at the same GS-11 grade, a 2210 gets paid $63,490 per year with an 18% supplement compared to a 0335 who gets paid $62,236 per year.[58,59] Thus, additional funding is required, even for the mitigation option, to gain 2210s within CE, but it provides a permanent solution to meet the cybersecurity requirements.

Contract Out Cybersecurity Support

An alternate option to providing organic, local capabilities without going through manpower authorization requests is for CE to outsource cybersecurity to an industry partner. To do this, AFCEC would program a requirement to obtain funding for an USAF-wide cybersecurity support contract. The contract would need to specify providing ISO at each installation who would meet DOD 8570 certification and USAF security clearance requirements. While the contractor would be able to help with some roles as mandated by AFI 17-101, the contractor cannot perform "inherently governmental functions," since an "inherently governmental function is one that has been determined to be—through statute or otherwise—a function that must be performed by Government personnel, either civilian or military, and that may not be performed by a contractor."[60] Acquisition officials have determined IT strategy and architecture is one of the products and services to require heightened management attention and to check how closely associated it is to inherently governmental functions.[61] Therefore, positions that require any involvement in designing networks or providing system administration would not be allowed by the contractor. Other roles such as the PM or ISSM could be covered by the contract. The ISSE would most likely still be an inherently governmental position.

This course of action has several advantages over the previous proposals. First, position classification requirements do not apply to contractors; therefore, the company can provide

certified individual(s) capable of accomplishing the requirements outlined in the contracting documents without worrying about Title 5 requirements. Additionally, the performance work statement can specify to provide staff with ICS knowledge to address those criteria. As this action requires CE working with contracting to award a contract, the duration to implement a solution and provide on-site support to resolve cybersecurity risks may be longer compared to other options. Moreover, CE would need to prioritize in the POM for additional funding as the contract would need to cover salary, which is greater than federal employees ($83,000-$117,000 per year), and overhead costs, potentially doubling the amount for one position compared to a federal employee.[62] Nevertheless, this course of action would allow CE to fill the non-inherently governmental positions more quickly compared to gaining additional manpower authorizations. This proposed action would need to be combined with one of the other alternative actions in order to provide a complete and comprehensive solution to the ICS cybersecurity risk.

CONCLUSION

The USAF's mission and operational capabilities rely on critical infrastructure, which is monitored, operated, and controlled by ICS. Yet, these systems are vulnerable to cyberattacks as the nature of ICS and IT integration depend on interconnectivity.[63] Therefore, the USAF must embed cybersecurity personnel into CE units to mitigate vulnerabilities and cyberattacks to ICS. CE currently does not have the expertise to implement cybersecurity to protect the system from attacks, which could result in failure of critical infrastructure that enables mission operations such as MDC2. This research considered four actions and alternatives to meet the cybersecurity requirements: a no action alternative – status quo, assigning 2210s to CE, permanently establishing cyber support positions within CE and contracting out cybersecurity support.

Table 2. Comparison of potential solutions against set criteria

Potential Solution	Position Classification Requirements	Cyber Certification	ICS Knowledge Skills & Abilities (KSAs)	Funding	Timeline
No Action Alternative – Status Quo	-	-	+	+	+
Assigning 2210s to the CE Mission	+	+	-	+	O
Permanently Establish 2210s within CE	+	+	+	-	-
Contract Out Cybersecurity Support	N/A*	+	O	-	-

+ Meets or exceeds criteria
- Does not meet criteria
O Varies depending on individual/installation
N/A Not applicable as Contractor is not a Federal Employee and is does not require to follow OPM policy*

Each proposed solution was evaluated against the set criteria (Table 2). The action to assign 2210s to the CE mission met more of the criteria compared to the other proposed alternative. However, that course of action does not provide a permanent solution to advert all risk as C&I could take back the must-needed resources. The action to permanently establish 2210s within CE met more of the higher priority criteria and establishes a long-term solution, but would require additional time and funding to implement, creating short-term vulnerabilities to the system. Therefore, a hybrid solution between the two is needed to mitigate both short and long-term vulnerabilities.

RECOMMENDATIONS

Innovative technologies and capabilities are weaved throughout the USAF's critical infrastructure and ICS. The connectivity provides for real-time monitoring, automation, and remote control to greatly enhance productivity and efficiencies. However, "[o]ur adversaries have analysed our systems, capabilities, and tactics attempting to minimize our advantage in every domain…" and as such, justifies the immediate need to invest in areas to support MDC2.[64] One area is for the USAF to embed expertise to protect and quickly restore capability of critical assets necessary to support MDC2.[65] The research identified four possible alternatives to meet cybersecurity requirements. However, a hybrid solution between assigning positions and permanently establishing 2210 is recommended in order to mitigate both short and long-term risk.

Similar to the recommendations AFOSI proposed to support their cyber capabilities, the USAF must take action to integrate cybersecurity expertise into CE's daily operations in order to provide the USAF with the right tools to be effective in defending and responding to threats across the cyber spectrum. CE, C&I, A1 need to engage at Headquarters Air Force (HAF) to 1) first develop a MOA between CE and C&I to temporarily assign 2210s to CE squadrons to provide immediate support. 2) Next, CE should then work with A1 to resource additional manpower authorizations to support permanent 2210s within all CE squadrons. Finally, AF/A4C needs to update the AFGM2019-32-02 to clearly define the roles and responsibilities at the installation level in order to implement initial operating capability and prevent cyberattacks against critical infrastructure, reduce vulnerability and minimize manage and recovery time from cyberattacks. In order to provide full operational capability, additional manpower with the above-mentioned certifications need to be assigned to the critical team that protects the CE ICS

network. A Stuxnet-like attack aimed at the ICS of the USAF would not only threaten the military, but also the critical civil infrastructure and institutions that house and support those whom the military protects.

NOTES

[1] Dave McMillen, "Attacks Targeting Industrial Control Systems (ICS) Up 110 Percent" *SecurityIntelligence*, 27 December 2016, https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/.
[2] Air Force Guidance Manual (AFGM) 2019-32-02, *Civil Engineer Control Systems Cybersecurity*, 5 September 2019, 3.
[3] Ibid.
[4] U.S. Army Training and Doctrine Command, "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040," Version 1.0, December 2017, 29.
[5] U.S. Office of Personnel Management (OPM), *Handbook of Occupational Groups and Families,* (Washington, D.C.: OPM, December 2018), 123.
[6] Keith Stouffer et al, "Guide to Industrial Control Systems (ICS) Security" National Institute of Standards and Technology: U.S. Department of Commerce, NIST Special Publication (May 2014): 800-822-1.
[7] Erine Hayden, Michael Assante, and Tim Conway, *An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity*, SANS Analyst white paper. North Bethesda, MD: SANS Institute, August 2014, 4.
[8] Ibid., 12.
[9] Ibid.
[10] Executive Order (EO) 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*,* 2017.
[11] Ibid.
[12] Joint Chiefs of Staff, *Summary of the 2018 National Defense Strategy of the United States of America,* Washington, D.C., 3.
[13] Ibid., 6.
[14] Ibid., 7.
[15] Department of Defense, *Unified Facilities Criteria (UFC) 4-010-06, Cybersecurity of Facility-Related Control Systems,* (Washington D.C.: National Institute of Building Sciences, 18 January 2017), 1.
[16] Ibid., 29.
[17] AFI 17-101, *Risk Management Framework (RMF) For Air Force Information Technology (IT),* 2 February 2017.
[18] AFGM 2019-32-02, *Civil Engineer Control Systems Cybersecurity*, 5 September 2019, 6.
[19] Department of Defense, *Unified Facilities Criteria (UFC) 4-133-01, Air Traffic Control and Air Operations Facilities,* (Washington D.C.: National Institute of Building Sciences, 25 June 2019), 44.
[20] AFGM 2019-32-02, *Civil Engineer Control Systems Cybersecurity*, 5 September 2019, 11.
[21] David Kushner, "The Real Story of Stuxnet: How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program," *IEEE Spectrum,* 26 Feb 201, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.
[22] BBC, "Timeline: How Stuxnet attacked a nuclear plant," *iWonder,* 2019, https://www.bbc.com/timelines/zc6fbk7.
[23] Ibid.

[24] Domenico Raguseo, "Lessons Learned From Stuxnet," *SecurityIntelligence,* 10 March 2017, https://securityintelligence.com/lesson-learned-from-stuxnet/.
[25] Ibid.
[26] Caroline Baylon, Roger Brunt, and David Livingstone, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks,* (London, UK: Chatham House Report, September 2015), 11, https://www.chathamhouse.org/sites/default/files/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf.
[27] Dave McMillen, "Attacks Targeting Industrial Control Systems (ICS) Up 110 Percent" *SecurityIntelligence*, 27 December 2016, https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/.
[28] Kim Zetter, "A cyberattack has caused confirmed physical damage for the second time ever." *Wired*, 08 Jan 2015, https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.
[29] U.S. Office of Management and Budget (OMB), *Federal Cybersecurity Risk Determination Report and Action Plan,* Whasington, D.C.: WhiteHouse, May 2018, 2.
[30] Ibid., 16.
[31] Aarom Mehta, "Pentagon weighs new requirements to secure military's vulnerable power grid," *DefenseNews,* 29 Nov 2017, https://www.defensenews.com/pentagon/2017/11/29/pentagon-weighs-new-requirements-to-secure-militarys-vulnerable-power-grid/.
[32] Tirrell, LCDR, William K. "United States Cybersecurity Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment?" Fort Leavenworth, KS: U.S. Army Command and General Staff College, February 2012, 5.
[33] Hartvigsen, Daron M. "AFOSI Cyber Threat Pursuit: The Air Force's 'Outside the Box' Response to Cyber Exploitation." Maxwell AFB, AL: Air Command and Staff College, February 2017, 1.
[34] Ibid., 2.
[35] Ibid., 24.
[36] Ibid., 4.
[37] OPM, *The Classifier's Handbook,* (Washington, D.C.: OPM, August 1991), 4.
[38] OPM, *Handbook of Occupational Groups and Families,* (Washington, D.C.: December 2018), 123.
[39] Ibid.
[40] AFMAN17-1301_AFGM2019-01, *Cybersecurity Workforce Improvement Program*, 09 August 2019.
[41] Ibid., 1.
[42] Ibid., 19.
[43] AFGM 2019-32-02, *Civil Engineer Control Systems Cybersecurity*, 5 September 2019, 8.
[44] Ibid., 3.
[45] "DoD Budget Request*,"* Under Secretary of Defense (Comptroller), accessed 4 October 2019, https://comptroller.defense.gov/Budget-Materials/.
[46] "Air Force President's Budget FY20," USAF Financial Management & Comptroller, accessed 4 October 2019, https://www.saffm.hq.af.mil/FM-Resources/Budget/.
[47] Ibid.
[48] "PBE Process: Program Objective Memorandum (POM)," AcqNotes, http://acqnotes.com/acqnote/acquisitions/program-objective-memorandum-pom.

[49] Mosheh Gains and Dareh Gregorian, "Pentagon is moving $3.6 billion in military funding to build Trump's wall," *NBCNews,* 3 September 2019, https://www.nbcnews.com/politics/national-security/pentagon-moving-3-6-billion-military-funding-build-trump-s-n1049406.
[50] Aarom Mehta, "Pentagon weighs new requirements to secure military's vulnerable power grid," *DefenseNews,* 29 Nov 2017, https://www.defensenews.com/pentagon/2017/11/29/pentagon-weighs-new-requirements-to-secure-militarys-vulnerable-power-grid/.
[51] AFCEC, memorandum, subject: Interim Process for Obtaining an ATO for Air Force Civil Engineer Control Systems During Transition to RMF, June 2017.
[52] Ibid.
[53] AFGM 2019-32-02, *Civil Engineer Control Systems Cybersecurity*, 5 September 2019.
[54] AFPC Database, C&I Career Field Extract, July 2019.
[55] MyPers, "0335 Standard Core Personnel Document," under "SCPD Library," https://mypers.af.mil.
[56] OPM, *The Classifier's Handbook,* (Washington, D.C.: OPM, August 1991), 4.
[57] MyPers, "2210 Standard Core Personnel Document," under "SCPD Library," https://mypers.af.mil.
[58] OPM, "Special Rate Table" (Number 999B), 2019, https://apps.opm.gov/SpecialRates/2019/Table999B01012019.aspx.
[59] OPM, "Salary Table 2019" (RUS), 2019, https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2019/RUS.pdf.
[60] DOD, *Handbook of Contract Function Checklists for Services Acquisition*, (Washington D.C.: Government Printing Office, May 2018), 4.
[61] Ibid.
[62] "What Is the Average Cyber Security Salary by State", *ZipRecruiter,* https://www.ziprecruiter.com/Salaries/What-Is-the-Average-Cyber-Security-Salary-by-State.
[63]Curtis E. LeMay Center for Doctrine Development and Education, *Air Force Doctrine, Annex 3-12, Cyberspace Operations*, 30 November 2011, 9-10.
[64]Major General (retired) Tim Zadalis, US Air Force, "Multi-Domain Command and Control: Maintaining Our Asymmetric Advantage," *The Journal of the Joint Air Power Competence Center (JAPCC),* Journal 26 (Spring/Summer 2018): 10-11.
[65] U.S. Army Training and Doctrine Command, "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040," Version 1.0, December 2017, 29.

APPENDIX A

Glossary of References and Supporting Information

Congressional Law:

- FY17 NDAA S. 1650: Evaluation of Cyber Vulnerabilities of Department of Defense Critical Infrastructure

National Institute of Standards and Technology (NIST):

- NIST SP 800-37r1: Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010
- NIST SP 800-39: Managing Information Security Risk, March 2011
- NIST SP 800-53r5: Security and Privacy Controls for Information Systems and Organizations, draft as of August 2017
- NIST SP 800-82r2: Guide to Industrial Control Systems (ICS) Security, May 2015
- NIST SP 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007
- NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems, August 2011
- NIST SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011
- NIST SP 800-171r1: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, December 2016

DOD:

- DEPSECDEF Memo: Enhancing Cybersecurity Risk Management for Control Systems Supporting DOD Owned Defense Critical Infrastructure, 19 Jul 2018

- DOD CIO Memo: Control Systems Cybersecurity, 19 Dec 2018
- ASD EI&E Memo: Managing Cyber Risks to Facility-Related Control Systems, 31 Mar 2016
- DOD's Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DOD) Industrial Control Systems (ICS) (Version 1), January 2016
- DODI 5000.02: Operation of the Defense Acquisition System
- DOD 8570.01-M: Information Assurance Workforce Improvement Program, 10 November 2015
- DODD 3020.40: Mission Assurance (MA), 29 November 2016
- DODD 8140.01: Cyberspace Workforce Management, 31 July 2017
- DODI 8500.01: Cybersecurity, 14 March 2014
- DODI 8510.01: Risk Management Framework (RMF) for DOD Information Technology (IT), 28 July 2017
- DODI 8530.01: Cybersecurity Activities Support to DOD Information Network Operations, 25 July 2017
- UFC 4-010-06: Cybersecurity of Facility-Related Control Systems, 18 Jan 2017
- Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204.7012: Safeguarding Covered Defense Information and Cyber Incident Reporting, October 2016

Air Force:

- AFI 10-1701: Command and Control (C2) for Cyberspace Operations, 20 January 2018
- AFI 17-101: Risk Management Framework (RMF) for Air Force Information Technology (IT), 02 February 2017

- AFI 17-110: Information Technology Portfolio Management and Capital Planning and Investment Control
- AFI 17-130: Air Force Cybersecurity Program Management, 13 August 2015
- AFI 17-203: Cyber Incident Handling
- AFI 63-101/20-101: Integrated Lifecycle Management
- AFMAN 17-1303: Cybersecurity Workforce Improvement Program, 20 March 2015
- AFGM2019-32-02: Civil Engineer Control Systems Cybersecurity, 05 September 2019
- AF Memo: MILCON Programming Guidance for the Cybersecurity of Facility-Related Control Systems, 11 Jan 19
- DHS's Cyber Security Procurement Language for Control Systems, September 2009

BIBLIOGRAPHY

Adler, Lieutenant Jordan M. *Cybersecurity Rick Management Afloat.* Monterey, CA: Naval Postgraduate School, 2015.

Curtis, Pamela, Nader Mehravari, James Stevens. *Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0.* Technical Report CMU/SEI-2015-TR-003. Pittsburgh, PA: Carnegie Mellon University, April 2015.

Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions. Report to Congressional Committees. Washington, DC: United States Government Accountability Office (GAO), June 2018.

Department of Defense, Unified Facilities Criteria (UFC) 4-010-06, *Cybersecurity of Facility-Related Control Systems,* Change 1, 18 January 2017.

Executive Order (EO) 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*,* 2017.

Farwell, James P. and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival,* 53:1 (2011): 23-40.

Hartvigsen, Daron M., *AFOSI Cyber Threat Pursuit: The Air Force's 'Outside the Box' Response to Cyber Exploitation,* Maxwell AFB, AL: Air Command and Staff College, February 2017.

Joint Chiefs of Staff, *Summary of the 2018 National Defense Strategy of the United States of America,* Washington, D.C.

McMillen, Dave, "Attacks Targeting Industrial Control Systems (ICS) Up 110 Percent" *SecurityIntelligence*, 27 December 2016, https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/.

Office of Personnel Management (OPM), *Handbook of Occupational Groups and Families,* (December 2018).

Tirrell, LCDR, USN William K., *United States Cybersecurity Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment?* Fort Leavenworth, KS: U.S. Army Command and General Staff College, February 2012.

U.S. Army Training and Doctrine Command, "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040," Version 1.0, December 2017.