STUDENT SCHOLARSHIP RELEASE FORM

Please convert your product to PDF, complete this form, and insert it as the cover sheet of your product.

LAST NAME: Hood

FIRST NAME: Jeremiah

COLLEGE (check one):

- ◯ College of Information and Cyberspace
- ◯ College of International Security Affairs
- ◯ Eisenhower School
- ◉ Joint Forces Staff College
- ◯ National War College

Graduation Month & Year (e.g., June 2021): June 2024

Choose one statement below concerning access to your document:

[X] **Option A: Access Restricted to NDU Users** – The product will be archived and discoverable in the Library's digital archives. All current NDU faculty, staff, and students will have access to the product but it will not be open and available to the general public. Access is controlled by NDU IP ranges which restricts access to authorized users on campus, connecting through VPN, or via Blackboard. External dissemination is unauthorized without permission from the appropriate college and DoD security reviews.

[ ] **Option B: Access by Request Only** – The product will be archived and discoverable in the Library's digital archives. However, only select members of the Library staff will have access to the student product. All NDU and external users must contact the Library and formally request access. The Library will vet each request with the academic dean at the appropriate college. Written permission must be obtained before access will be granted. External dissemination is unauthorized without permission from the appropriate college and DoD security reviews.

[ ] **Option C: Request Exemption** – NDU Instruction 5015.02 (Student Scholarship Preservation and Access) includes an addendum to address the possibility that students might produce research products that may be considered sensitive and possibly provoke retribution if released. In these rare cases, students may submit a written request for an exception to releasing their product through their faculty or research director, Dean, and then to the Deputy Provost. Students choosing this option must write a justification and insert it as a separate page after this form before submitting the paper. Justifications must describe perceived harm if the product was released. If the request is approved, the paper will not be released or archived. If the request is disapproved, students must choose Option A or B and resubmit.

x

Student Signature

Digitally signed by HOOD.JEREMIAH.CHRISTOPHER.1237527468
Date: 2024.02.14 09:21:05 -05'00'

Date (mm/dd/yyyy): 02/14/2024

REPORT DOCUMENTATION PAGE

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
		START DATE	END DATE
20240214	Individual Strategic Research Paper	20230710	20240214

4. TITLE AND SUBTITLE
Talent Strategy: Evolving the Department of Defense Cyber Workforce Strategy through Self-Efficacy

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**

6. AUTHOR(S)

Lieutenant Colonel Jeremiah C. Hood, United States Army Reserve

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Joint Forces Staff College Joint Advanced Warfighting School 7800 Hampton Blvd Norfolk, VA 23511-1702	

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Department of Defense (DoD) faces a vital imperative to expand and strengthen its cyber workforce amid rising threats from a contested and congested environment. The Fourth Industrial Revolution, Third Strategic Offset and increasingly capable, determined adversaries provide precedence for strategy. The DoD faces persistent shortfalls in the capacity and capability of its cyber talent pipeline. Fundamentally transforming its talent management approach requires a renewed focus on empowering cyber personnel by cultivating self-efficacy. This study examines practices that develop self-efficacy across the talent pipeline. Key strategy includes professionalizing the cyber workforce.

15. SUBJECT TERMS

Building the DoD Cyber Workforce Self-Efficacy through Professionalization, Prosocial Motivation, Organizational Citizenship Behavior and Private Public Partnerships, moderated through Talent Development and Talent Engagement

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	C. THIS PAGE		
Unclassified	Unclassified	Unclassified	Unclassified Unlimited	65

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER *(Include area code)*
Jeremiah C. Hood, Lieutenant Colonel, United States Army Reserve	(865)-770-2831

PREVIOUS EDITION IS OBSOLETE.

STANDARD FORM 298 (REV. 5/2020)
Prescribed by ANSI Std. Z39.18

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

Talent Strategy: Evolving the Department of Defense Cyber Workforce Strategy through Self-Efficacy

By:

Jeremiah C. Hood

Lieutenant Colonel, United States Army Reserve

Page Intentionally Left Blank

Talent Strategy: Evolving the Department of Defense Cyber Workforce Strategy through Self-Efficacy

by Jeremiah C. Hood

Lieutenant Colonel, United States Army Reserve

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes (or appropriate statement per the Academic Integrity Policy).

Student Signature: Digitally signed by HOOD.JEREMIAH.CHRISTOPHER.1237527468 Date: 2024.02.14 09:22:21 -05'00'

14 February 2024

Thesis Advisor Signature: HOLLANDSWORTH.EDGAR.M.1033669913 Digitally signed by HOLLANDSWORTH.EDGAR.M.1033669913 Date: 2024.02.16 14:18:03 -05'00'

Edgar M. Hollandsworth, PhD
Assistant Professor

Signature: FOWLER.ERIC.STEPHEN.1065030663 Digitally signed by FOWLER.ERIC.STEPHEN.1065030663 Date: 2024.03.01 12:40:24 -05'00'

Eric S. Fowler, Colonel, U.S. Army
Director, Joint Advanced Warfighting

Page Intentionally Left Blank

Abstract

The Department of Defense (DoD) faces a vital imperative to expand and strengthen its cyber workforce amid rising threats from a contested and congested cyber domain. The Fourth Industrial Revolution, Third Strategic Offset and increasingly capable, determined adversaries provide precedence for this strategy. The DoD faces persistent shortfalls in the capacity and capability of its cyber talent pipeline. Fundamentally transforming its talent management approach requires a renewed focus on empowering cyber personnel by cultivating self-efficacy. Research shows that self-efficacy predicts motivation, perseverance and performance. This study examines practices that develop self-efficacy across the talent pipeline. Key strategies include professionalizing the cyber workforce, establishing a cyber ambassadorship program, fostering prosocial motivation and organizational citizenship, capitalizing on "hidden workers" and scaling private-public partnerships (PPPs). Evolving the *DoD Cyber Workforce Strategy* to center on human capital development requires prioritizing talent engagement and development initiatives to enhance self-efficacy, yielding increased prosocial motivation and organizational citizenship behavior (OCB). A people-focused strategy will empower the workforce and maximize purposeful work.

Through a qualitative analysis of the theory, precepts and strategy, this study aims to interject new ideas, perspectives and arguments to shape and evolve the *DoD Cyber Workforce Strategy*. By establishing that self-efficacy is a valuable instrument for increasing the capacity and capability of the cyber talent pipeline, this research implies that scaling cybersecurity PPPs can be mutually beneficial to DoD and the cybersecurity enterprise in the perceived "War for Cyber Talent."

Page Intentionally Left Blank

Dedication

To my wife, best friend and life partner, thank you for your encouragement and undying support. Without you, my self-efficacy to pursue excellence in life would significantly pale in comparison to the aspirations I have set for myself. Thank you for your commitment and sacrifices to support me, our family and the citizens of this great nation.

To my daughter, thank you for being my beacon of hope to fulfill the responsibilities that military leadership positions require of me. You have a bright future, and I am confident that you will take advantage of every chance to establish and achieve your own ambitious goals. Thank you for inspiring your mother and me with optimism that far exceeds our own. In everything that you do, do it with a servant mentality, and always attempt to do the things that you think that you cannot do.

To my extended family and friends, thank you for your enduring support as I have journeyed through military service. Your love, support and friendship are always in my heart. My service to this country would be far less rewarding if you were not in my thoughts.

Page Intentionally Left Blank

Acknowledgments

I would like to acknowledge my advisor, Dr. Edgar M. Hollandsworth for the coaching and teaching that you provided to me during the writing process. I greatly appreciate the time that you invested in making this research a fruitful product and for challenging me to think creatively and critically about the subject.

I would also like to acknowledge my fellow seminar classmates and faculty. Thank you for devoting the time and effort required to make this academic venture a rewarding experience. The academic challenges and problems that we faced were exigent, but with unparalleled instruction, leadership and teamwork, the endeavor was rewarding. I extend my sincerest wishes for success and fulfillment to all as you advance in your professional endeavors.

Page Intentionally Left Blank

Table of Contents

Page Intentionally Left Blank

Figures and Tables

Page Intentionally Left Blank

Chapter 1: Introduction

The Department of Defense (DoD) is competing for cyber talent while embracing the advent of the Fourth Industrial Revolution, characterized by the convergence of the Internet of Things (IoT), artificial intelligence (AI), advanced automation, quantum science and biotechnology. This technical innovation possesses the potential to revolutionize the global landscape and warfare. The impact of this phenomenon will extend to all aspects the world's geopolitical environment. The size, scope and intricacy of the transformation will surpass any previous encounters in human history. The revolution's double-edged effects could hinder the DoD's Third Strategic Offset technological priorities from outperforming the nation's top adversaries.[1] Hence, strategic competition is the scene-setter for the current challenge: the DoD and cybersecurity enterprise face a serious cybersecurity talent pipeline gap. This talent gap is a top DoD concern in the 21st century. In illustration, CyberSeek reports that the current supply of cybersecurity professionals in the United States (U.S.) is only sufficient to meet 69% of the existing demand for cybersecurity positions.[2] Further, the demand for cybersecurity professionals is accelerating due to ever-evolving threats. As a result, our nation's response must be comprehensive and integrated. Human capital, as opposed to financial resources, will be the deciding factor. Hence, the nation's cybersecurity enterprise must establish partnerships that prioritize people and give them agency.[3] Increasing workforce self-efficacy is paramount to this strategy.

The utilization of secure technology and data plays a crucial role in ensuring national security. Rising vulnerabilities have the potential to disrupt economies, foster distrust toward institutions and undermine national security. In contrast, the constricted

cybersecurity talent pipeline for the DoD has resulted in an increased workload for cyber teams, unfilled job requisitions and a notable prevalence of job burnout. According to the DoD's internal assessment, the situation has the potential to negatively impact its operational readiness, imposing adverse implications for national security.[4] Adding cause for concern, the Office of the Director, Operational Test & Evaluation reported in 2022 that the DoD is currently facing significant cyber talent and mission deficits in automation, cybersecurity, data management, AI and digital engineering.[5]

Facing a national shortfall of cybersecurity talent, demand signals are emerging to research strategies to address the nation's critical need for a highly capable cybersecurity workforce. Current scholarly discourse highlights cyber talent pipeline capacity and capability deficiencies, the growing competition for cybersecurity talent, concerns over great power competition and the DoD's attrition challenge. The predominant theme throughout the literature characterizes the environment as a "people war." Human capital is viewed as the key resource of a sustained cybersecurity talent strategy, and having the right people with the needed skills is the goal. Further, building and growing a cybersecurity talent pipeline is contingent upon removing barriers and establishing a competitive advantage. So, how can the DoD most effectively use its means to favorably influence the strength and direction of its cyber workforce strategy? The DoD can further improve its talent strategy, aiming to lead, not win, the nation's buildup of cyber talent, through a focus on building self-efficacy toward a cybersecurity career. Since people are the center of gravity, and the object of the competition, the approach must enable talent as its focal point, and address the adaptive challenges of self-efficacy. Mediating initiatives may include: 1) promoting career opportunities through ambassadorship, 2)

providing stability and a family-centric quality of life and 3) providing autonomy, mastery and purpose.[6]

As one of the nation's major employers, the DoD is a laggard in the cyber talent competition, which threatens national security. The DoD no longer maintains a competitive advantage in acquiring top cybersecurity talent and is no longer the innovator for technology, a status that it maintained during the Cold War period. Low self-efficacy toward a cyber career and military service threatens the department's ability to compete for cyber talent by not meeting recruitment targets and not maintaining and growing its Cyber Mission Force (CMF). These personnel challenges produce gaps, such as incapability to fill senior leadership positions and incapacity to meet emerging needs within Cyberspace Operations (CO). Low DoD personnel self-efficacy toward cyber careers reflects the following competitive assumptions: 1) higher-paid private sector jobs are more desirable, 2) DoD CMF mission requirements preclude personal development, 3) the DoD CMF lacks clear professional pathways, 4) the reward system for maintaining demanding credentialing and privileging status is inadequate and 5) the military structure is inflexible toward family-centric quality of life. These barriers within DoD's cyber talent management system (TMS) provide insight into opportunities for improvement. The DoD Cyber Workforce Strategy Implementation Plan 2023-2027 estimates that the DoD currently faces a 25 percent vacancy rate in its CMF.[7]

In terms of strategic risk, the U.S. Government Accountability Office (GAO) reports that the U.S.' ability to provide cybersecurity over the nation's critical infrastructure is a high risk. The report highlights the foremost need to establish a talent comprehensive cybersecurity strategy. Further, the GAO reported that solving cyber

management issues is one of the four critical actions to mitigate the risk.[8]

In context, a recent Defense Business Board (DBB) assessment noted the DoD is in a "war for talent" as a result of a perfect storm of market stressors: 1) the workforce is aging, 2) workforce participation is dropping, 3) there is global talent competition and 4) there is a rising need for "knowledge workers."[9] In addition, the report highlights the following DoD unique stressors: 1) the pay gap concerning private industry, 2) its waning appeal to younger workers, 3) an aging workforce and 4) great power competition. While these changes have been difficult for the private sector, they are just the beginning for the DoD.[10] The DBB states that growing the cyber talent pipeline is the best strategy for winning the talent war and that the approach must be aimed at maintaining a continuous supply of qualified job candidates to meet current and future staffing needs. The pool of candidates must include individuals from outside the organization as well as existing employees, and the pipeline must incorporate personnel currently in education or training and hidden workers. The DBB asserts that the DoD talent acquisition approach must adopt private industry methods to grow its talent pipeline. In addition, the DBB emphasizes that the DoD must cultivate talent networks to increase the self-efficacy of its cyber workforce and build critical skillsets.[11] Consequently, the DBB warns that if the DoD does not develop a more modern, proactive strategy, then the DoD will fall further behind the People's Republic of China (PRC) in terms of cyber modernization and operational readiness.[12]

In framing the problem, a consistent scholarly perspective is that there is a "war for cyber talent," suggesting that the dyadic relationship between government and industry has progressed negatively from competition to conflict. There is rising fear over

impending transformations, and a compounding perception that the DoD is in a position of disadvantage.[13] However, research does not indicate any deliberate and destructive acts between government and industry in competing for cyber talent. Although fear is usually a greater catalyst for change than hope, it can provide a bond for cooperation and collaboration, and the stance of this research is that the cybersecurity enterprise is at a crucial moment mandating that this fear and hope be yoked together.[14] In expanding this problem frame, a pragmatic analysis deduces that there is chaos and anarchy in the hyper-competitiveness for cyber talent, which presents an opportunity for a leading approach versus a winning approach.[15] In sum, this research seeks to introduce the idea that improving the self-efficacy toward a career in cybersecurity can be a common theme for partnership, binding the DoD and industry in growing a mutually supportive talent pipeline, vice competing with each other over scarce human capital.

In examining national strategic guidance, the *National Security Strategy 2022* defines the interest of securing cyberspace as a vital national interest to protect the nation's national functions and critical infrastructure.[16] Our world is on the verge of significant change, characterized by geopolitical upheavals, causing a reconfiguration of the worldwide economic order that has thrived since the Cold War. This movement is pervasive and poses structural issues, such as rivalry across economic models, struggle for technological leadership and control over physical and digital communication and technology. In response, the President of the United States (POTUS) directs the nation to increase its cybersecurity capacity and capability to reshape the technological landscape.[17] Further, the POTUS aims to gain and maintain a strategic advantage in cybersecurity and proclaims that our nation's strength and resilience is dependent upon a

capable and inclusive cybersecurity workforce. In concert, the POTUS declared that the nation's cyber enterprise (government, industry and academia) must reconceptualize how it acquires, maintains and develops its cyber workforce. The POTUS provides the following amplifying guidance for enterprise leadership: 1) prioritize equality, diversity, inclusion and ease of access; 2) enhance the efficacy and efficiency of recruiting, retention and talent development practices; 3) provide pragmatic professional pathways; 4) support opportunities for talent transfers and 5) prioritize the acquisition of underrepresented and untapped talent.[18] Further, the POTUS emphasizes scaling private-public partnerships (PPPs) to build a more resilient national cybersecurity posture.[19] Hence, this research is relevant because it seeks to interject new ideas, perspectives and arguments to shape and evolve a talent strategy for the national security imperative of building, developing and growing a national cyber workforce. As the cyberspace domain has evolved as a consequential environment for strategic competition,[20] the DoD must develop resilience and enhance endurance in its cyberspace capabilities.[21]

To inspire innovation, the POTUS, through the *National Cybersecurity Strategy 2023*, challenges the cybersecurity enterprise to strengthen and diversify America's cyber workforce. The POTUS challenges the enterprise to remove the gatekeepers, myths and other impairments for the profession, and develop the ways to make a career in cybersecurity accessible and attainable to every American who desires to pursue and attain it. In support, the administration will realign incentives to favor long-term investments in security, resilience, and promising new technologies, and will collaborate with Congress to provide the necessary resources and tools to guarantee the strategy's survivability.[22] A talent deficit in the U.S. threatens the nation's ability to counter the

PRC's and Russia's growing asymmetric information operations threat, which both produce more cyber workforce capacity. The federal government has the most direct and indirect impact on cyber talent development in addressing the issue.[23]

Additionally, the *2023 National Cyber Workforce and Education Strategy* highlights the need to make a cybersecurity career more attainable and attractive, and challenges the cybersecurity enterprise to coalesce to reach the cyber workforce needs of our nation.[24] Further, the *2022 National Defense Strategy* asserts that the DoD must change its cyber talent management strategic culture and approach to establish a competitive advantage.[25] In response, the *DoD 2023 Cyber Strategy* emphasizes that people are the nation's most valuable cyber asset and that reforming DoD's cyber workforce TMS is a top priority. With the strategy, the DoD prioritizes: 1) establishing targeted cybersecurity skillset incentive programs, 2) founding rotational employment programs with the private sector, 3) revamping tour length and commitment personnel policies, 4) clearly defining career progression models and 5) utilizing the Reserve Components more strategically to share and develop talent with the private sector.[26] The Secretary of Defense (SECDEF) directs that to effectively attract and retain a world-class workforce, it is imperative to transform the DoD's institutional culture and implement comprehensive reforms in its business practices.[27] Moreover, the *Fiscal Year 2023 National Defense Authorization Act* (NDAA) directs a review of the cyber personnel policies, strategy, education and training of the DoD's CMF to mitigate security risks to the nation. This study will address these strategic requirements by providing recommendations for increasing personnel self-efficacy toward a DoD cyber career and identifying barriers to be removed. To posit the thesis, enhancing personnel self-efficacy

will advance the talent development and talent engagement initiatives within the *DoD Cyber Workforce Strategy*.

This research will employ a four-part analysis structure: first, gain an understanding of the problem from a theoretical and practical standpoint; second, conduct a critical examination of the current cyber strategy for addressing the problem; third, review a similar high-demand TMS within the DoD to identify components that meet the critical needs of a highly technical/professional workforce; and fourth, provide recommendations for filling gaps in the *DoD Cyber Workforce Strategy 2023-2027* and *DoD Cyber Workforce Strategy Implementation Plan 2023-2027*. The overall aim of the research is to show that self-efficacy is a positive mediating factor in increasing the capacity and capability of the DoD's cyber talent pipeline and is crucial to acquiring underrepresented and untapped talent. Increasing self-efficacy is the basis for DoD and industry collaboration and cooperation toward innovation and creating a mutually supportive cybersecurity talent pipeline. The collective capacity of the cybersecurity enterprise is greater than the problem at hand.

Background

The Defense Business Board (DBB) reported that private-public collaborations (PPCs), a term that has evolved in current discourse to private public partnerships (PPPs), can provide the DoD competitive advantages and offer efficiency and cost savings in a budget-constrained environment,[28] and are critical as the nation shifts from a "whole of government" toward the "whole of society" strategic competition approach.[29] Moreover, the DBB proclaimed that PPCs can leverage private and other agency resources, but that the DoD either misses, weakly pursues or does not exploit PPCs, and that the DoD must

implement this skill set to help match private sector speed and agility.[30] In this vein, the *National Infrastructure Protection Plan (NIPP) 2013* emphasizes greater emphasis on cyber integration between all levels of government, private and nonprofit sectors.[31]

Concerning cyber talent management, the National Research Council (NRC) conducted a project, supported by the U.S. Department of Homeland Security, on building the capacity (pipeline) and capability (knowledge, skills and abilities) of the nation's cybersecurity workforce. The NRC concluded that the number of qualified workers willing to fill positions depends on the visibility and desirability of cybersecurity occupations, the availability of training and education, and the overall labor market stressors.[32] Further, the NRC's report encouraged professionalization mechanisms to establish a long-term pipeline of cybersecurity talent.[33]

More recently, the National Academy of Public Administration (NAPA) highlighted the need for a government-wide strategy for developing the national cybersecurity workforce. In addition, the NAPA suggested the incorporation of four components: 1) encouraging more people to choose a career in the cybersecurity field through outreach and education, 2) enabling education and training to build needed competencies and alternative career pathways, 3) overcoming talent acquisition obstacles and 4) assessing performance and promoting innovation in workforce development practice.[34]

Further, the Senate, as part of the *2022 NDAA* directed the GAO to review the DoD's cyber talent management challenges. The GAO's report highlighted that ensuring the cybersecurity of the nation is a high risk, persisting since 1997.[35] The GAO asserts that the DoD faces rising levels of competition for cyber talent from private industry,

attributing the strain to social and economic issues, including low unemployment rates, competitive labor markets and limited entry-level workforce eligibility.[36] In addition, the GAO concludes that an alignment of incentive pay to critical skill sets was required.[37]

Further, a recent military academic initiative noted that to effectively address DoD's cyber workforce needs, it is imperative to employ partnerships with industry and academia. This approach, articulated as a whole-of-society defense, aims to streamline efforts and enhance the nation's ability to meet cybersecurity challenges. The researchers argue that the establishment of such partnerships will be operationally and strategically beneficial for all. This synergy will result in the development of a flexible cyber workforce, which will be strengthened by the interconnected network of cyber agencies and organizations in the U.S. The authors conclude that to effectively achieve talent management objectives, it is imperative for the implementation plan to address the needs of the workforce in its human capital pillars.[38]

In terms of the DoD CMF feedback, three DoD-supported retention-oriented surveys provide bottom-up insights to help mitigate the problem. A *2019 Army Cyber Command (ARCYBER) Retention Study* produced the following top three insights for why personnel were dissatisfied with military/government service: 1) inability to focus on their mission without constant administrative burdens/distractions, 2) lack of time to exercise their skills and complete skills training and 3) greater pay and incentives in the private sector.[39] In addition, a *2021 U.S. Cyber Command (USCYBERCOM) Retention in Cyber Command Survey* concluded with the following perspicacity: 1) personnel were dissatisfied with pay and benefits, 2) family members were dissatisfied with the military lifestyle, 3) personnel felt less in control of their careers, 4) 50% of respondents would

leave the service early to take a civilian industry position if it was available to them, 5) provided schooling and training opportunities were highly valued and 6) latitude/control over assignment/location of choice and job of choice would be a significant motivator for retention.[4041] Furthermore, the Blue Star Families' *Military Family Lifestyle Survey:2022* concluded that: 1) military families worry most about money issues and 2) the ramifications of military duty on family life persist.[42]

Concerning increasing the capacity of the cyber talent pipeline, research indicates that there is a large, overlooked "hidden worker" talent pool able and willing to work under the right circumstances. The DoD traditionally acquires talent from categories like veterans, immigrants, people with disadvantaged backgrounds, young people not in education/employment/training (NEETs), people without traditional qualifications, degrees, or work history and the long-term unemployed. Further engaging this non-traditional talent pool, the DoD can target compatible demographics, establish a foundation and utilize champions to connect with them.[43]

Moving forward, the U.S. government must further scale PPPs in emerging technologies and domains, alongside the maintenance and augmentation of investments in domestic research and innovation.[44] In support, the POTUS provides the following 2025 cybersecurity investment priorities: 1) increasing the capacity and capability of the nation's cyber workforce; 2) strengthening PPPs through the sharing of knowledge, data and information; 3) building additional capacity for specialized cyber analysts to partner with private industry and 4) invest in, and prioritize initiatives, to develop fundamental, technical cyber competencies and required capabilities.[45]

Methodology

This research will utilize a multi-component qualitative methodology to critically analyze and provide recommendations for improvements to the *DoD Cyber Workforce Strategy & Implementation Plan 2023-2027*. The qualitative analysis includes: 1) a review of literature on the theory of self-efficacy and motivation, 2) a review of the role of the human capital pillars of talent management on increasing self-efficacy, 3) a critical analysis of the current *DoD Cyber Workforce Strategy and Implementation Plan 2023-2027* and 4) a recursive analysis of professionalization within the Defense Health Agency's (DHA's) TMS. Through an informal content analysis of the *DoD Cyber Workforce Strategy and Implementation Plan 2023-2027,* inferences will be made on the extent the strategy aims to improve and/or build self-efficacy in the CMF. Hence, the overall analysis structure of the research will be to first, understand the problem in theory and experience; second, critically analyze the current cyber strategy for fixing the problem; third, to conduct a review of a sister high-demand TMS within the DoD, to identify components that meet the critical needs of a highly technical workforce and fourth, to make recommendations to fill gaps in the *DoD Cyber Workforce Strategy 2023-2027* and *DoD Cyber Workforce Strategy Implementation Plan 2023-2027*. The gap analysis will involve two parallel lines of investigation: 1) determine the level and scope of incorporating self-efficacy theory/practice into the current strategy and 2) highlight what additional goals and initiatives should be included. Further, the qualitative review of the theory of self-efficacy and motivation will recommend ways to increasing the capacity and capability of the DoD's cyber talent pipeline. Finally, the study will recommend ways to apply self-efficacy and motivation theories and precepts to improve

the *DoD Cyber Workforce Strategy and Implementation Plan 2023-2027*, setting conditions for the DoD to become an incubator for cyber talent. The research has three aims. Research Aim 1 is to establish that self-efficacy is a key personnel variable that must be cultivated throughout the continuum of talent management. Research Aim 2 is to identify gaps in the *DoD Cyber Workforce Strategy and Implementation Plan 2023-2027* concerning addressing the self-efficacy needs of the current and future DoD cyber workforce and any structural weaknesses in its strategic approach. Research Aim 3 is to deduce ways to improve and/or innovate the existing cyber workforce strategy.

Together, these four components enable a holistic evaluation of how well the current DoD cyber workforce strategy addresses self-efficacy as a mediator for increasing the capacity and capability of its cyber talent pipeline. The methodology will produce actionable recommendations for the DoD to better manage its cyber talent pipeline in support of the DoD's strategic focus on empowering its cyber workforce and scaling PPPs.

Chapter 2: Enhancing Self-Efficacy as a Promising Addition to DoD's Cyber Talent Management Strategy

Despite the burgeoning demand for cybersecurity professionals, the lack of motivated applicants is an additional focus area for mitigating the DoD's cyber talent pipeline dilemma. Two primary aspects affecting cybersecurity as a career option are the candidate's awareness of the field and confidence in their abilities to follow it as a career path. Self-efficacy, a concept introduced by renowned psychologist Albert Bandura, refers to people's perceived beliefs in their abilities to control their choices and events influencing their lives.[46] Concerning career choices, Bandura acknowledged the role of interest and perceived abilities to pursue a specific career path as candidates disregard the options they think are beyond their capabilities. In support, Marilyn Gist proposes that two important factors can be influenced to improve personnel self-efficacy: 1) personal factors (e.g., skill level, anxiety, desire and available effort) and 2) situational factors (e.g., competing demands and distractions),[47] and that the availability and degree of skill acquisition and one's understanding of their relative contribution to the organization's mission/goals are the most important conditions.[48] Other prominent theorists emphasize the significance of self-efficacy in empowering individuals to persevere in the face of adversity, especially in the pursuit of a chosen career.[49] Further, researchers have noted that a lack of awareness crops up when candidates are ignorant or uninformed of their abilities and how they could relate their interests to cybersecurity job opportunities.[50] Thus, cybersecurity self-efficacy becomes an essential aspect in motivating candidates to pursue it as a career. Daniel Pink posits that the key to achieving optimal employee job satisfaction lies in fulfilling people's needs to have control over their own lives, engage in

continuous learning and innovation, and strive to be a part of something greater than themselves.[51] In his work, Pink draws upon a substantial body of scientific research spanning four decades that focuses on human motivation. He sheds light on the disparity that exists between employee motivation and business human resource practices, and how it affects attracting and retaining employees. The author concludes that there are three fundamental components of genuine motivation, namely autonomy, mastery and purpose.[52]

Self-efficacy theory presents four critical sources of self-efficacy, namely, mastery experience, social persuasion, vicarious experience and intrinsic motivation.[53] Mastery experience, an essential construct in the formation of self-efficacy, refers to how individuals perform. It also includes their prior experiences of success or failure. Further, vicarious experience is an observational method that refers to observing others' actions. Seeing other people completing tasks enhances self-efficacy by strengthening the belief about one's own competencies. It also provides a reference for social comparison between others' performance and individual expectations in a field. In addition, social persuasion means encouragement, support and feedback from friends, parents, teachers, etc. Moreover, intrinsic motivation refers to emotional arousal toward a specific career. Further, research indicates that cybersecurity candidates have a propensity towards traits such as openness, investigative interests and logical decision-making styles.[54]

Literature asserts that experiential learning supports all sources of self-efficacy.[55] Experiential learning helps candidates apply theories to real-world situations, which significantly boosts their confidence and self-efficacy.[56] Thus, completing hands-on assignments improves a candidate's mastery experience as their self-efficacy gets a boost

when they finish the tasks successfully. For example, completing a task in a cybersecurity experiential lab will significantly build a candidate's confidence and self-efficacy. Seeing others doing the same task will nurture vicarious experience, building their motivation to perform similar tasks. Further, seeing their peers effectively doing cybersecurity lab will develop their self-assurance in similar tasks. There is a solid consensus in the literature that the self-efficacy of cybersecurity career candidates can be improved using: 1) experimental labs, 2) gaming and 3) playable case studies (PCSs).

Ten studies revealed that game-based strategies are effective in motivating students to pursue a career in cybersecurity.[57] A practical game-based approach can efficiently engage students, honing their skills in identifying and countering cyberattacks. Secondly, games allow students to perform as both attackers and protectors, which helps them to anticipate various ways attackers can use and appropriate measures to defend themselves. Various scholars cited in this review acknowledged the challenges children face and how they inspire them to enhance their ability to pursue cybersecurity.

Further, the literature mentions the significance of these games in enhancing skills and improving self-efficacy. Players must analyze the situation, adapt to the environment, employ critical thinking and judge their decisions based on the relative value of choices. Providing supporting evidence, Bandura suggests that self-efficacy comes from self-modeling and social comparisons, i.e., evaluating own capabilities and observing how others, like them, are accomplishing similar tasks. Undeniably, game-based learning provides ample opportunities for players to observe others and make comparisons. Therefore, playing games provides solutions to students and helps them observe the effectiveness of their choices.[58]

PCSs are a type of educational simulation that allows learners to “play” through authentic scenarios and solve realistic problems as a member of a professional team. The PCS architecture offers learning activities and allows them to observe and analyze those activities. This is in sync with self-efficacy principles, especially the vicarious experience or the social comparison.[59] In support, another study stated that cybersecurity PCSs were found to increase learners’ understanding of key aspects of cybersecurity and improve their confidence in applying cybersecurity-related skills. Around fifty percent of the respondents reported that case studies improved their curiosity toward cybersecurity.[60] Another research study demonstrated that cybersecurity PCSs enhanced cybersecurity self-efficacy among teenage girls. Almost all participants reported that the case studies made them feel more assertive about their capability to perform well in cybersecurity education and training.[61]

In sum, addressing the cyber talent pipeline dilemma requires addressing candidate self-efficacy deficiencies. Factors influencing personnel self-efficacy include personal and situational factors. Experiential learning can boost confidence and self-efficacy. Game-based strategies can engage students and enhance their skills. PCSs provide educational simulations that allow learners to experience authentic scenarios and solve problems. These tools increase learners' understanding of key aspects of cybersecurity and improve their confidence in applying cybersecurity-related skills.

Role of Talent Management on Self-Efficacy

Today's global and fast-paced strategic environment and ever-changing labor force conditions require a rigorous and well-planned approach to managing talent.[62] Government and industry leaders recognize that talent helps drive the performance of an organization. It is, therefore, no surprise that talent management has become a crucial strategic priority.[63] The DoD urgently needs to expand and strengthen its cyber workforce. Beyond recruitment, retaining top talent requires career development strategies that empower employees and instill confidence in their ability to have a meaningful impact through their work. This literature review explores current research on the human capital pillars of talent management that have the greatest effect on increasing self-efficacy.

In an organizational context, an employee with high self-efficacy is more likely to pursue challenges, see obstacles as surmountable and be intrinsically motivated to achieve organizational goals. As such, self-efficacy has been positively associated with job performance and satisfaction and negatively associated with turnover intentions. These conditions make developing self-efficacy an important objective for talent management strategies.

Talent engagement involves creating an environment where individuals feel valued and connected to their work, while talent development focuses on enhancing skills and capabilities. As noted in the previous section, fostering engagement through challenging tasks, ongoing learning opportunities and a supportive environment can boost self-efficacy of employees in the cyber workforce. Offering training programs, mentorship and exposure to real-world scenarios can also empower personnel, increasing

their confidence in handling cybersecurity challenges and pursuing a career in the field.

How can the DoD take advantage of self-efficacy to improve its strategy for managing cyber talent? Research indicates that prioritizing ongoing learning opportunities is imperative to surmount talent shortages.[64] Talent development enhances the competencies, skills and knowledge of individuals, which are intricately linked to talent engagement.[65] Further, when talented people learn and grow in the right ways, their career growth is positively enhanced, which inspires them to participate and contribute more in and towards organizational activities and goals.[66] Therefore, talent development boosts the organization's appeal as a source of non-monetary gain and an instrument for employee engagement. New abilities boost talents' sense of self-efficacy. Talent development initiatives not only boost trainee capacity but also foster a good attitude among employees toward the organization. The more an employee believes that his or her talent is being developed, the more engaged he or she becomes. Employees who are provided professional development opportunities tend to engage more in their work and remain loyal to the organization.[67]

Talent engagement is a leading indicator in forecasting the recruitment and acquisition of talent, and it is an essential aspect of talent management.[68] Investing in talent engagement has shown to be an effective way to leverage human capital while providing them with sufficient extrinsic and intrinsic rewards to maintain motivation.[69] As a result, organizational socialization strategies are mediated by self-efficacy, as demonstrated by the increased recruitment and retention of talent.[70]

The *DoD Cyber Workforce Strategy 2023-2027* guides efforts to build and sustain a highly skilled cyber workforce. Research suggests that talent development and

talent engagement pillars have the greatest potential to increase self-efficacy among cyber workforce personnel. Talent development and talent engagement generate employee value proposition (EVP), which results in higher talent self-efficacy and improved organizational performance.[71] The coordination of talent engagement and talent management strategies enhances organizational performance by lowering staff attrition.[72]

Building competencies significantly increases cyber personnel self-efficacy, and talent development signals to candidates and current employees that the organization values continuous growth and empowers them to meet new challenges.[73] Further, empowering cyber workforce personnel to participate in decision-making provides opportunities to apply their expertise. Involving cyber personnel in decisions positively influences their self-efficacy by signaling trust in their judgment. Empowerment fulfills autonomy needs and cultivates a sense of ownership over work.[74] Additionally, access to mentors and role models allows for vicarious learning, an important source of self-efficacy. Mentorship programs increase the self-efficacy of cyber talent by guiding experienced professionals. Exposure to successful professionals who have overcome challenges builds confidence.[75] An organizational climate that supports innovation can enhance cyber workforce personnel's beliefs in their abilities. Studies indicate that leadership, which encourages new ideas, risk-taking and learning from mistakes, promotes self-efficacy.[76] Environments where innovation is valued empower employees to think beyond norms. Last, merit-based reward systems provide cyber workforce personnel with evidence of their capabilities. Research finds that merit-based reward systems enhance cyber workforce self-efficacy by signaling organizational appreciation of their competence.[77] Formal mechanisms for recognizing contributions are validating.

Evolving the *DoD Cyber Workforce Strategy* to strengthen self-efficacy requires addressing current barriers and implementing talent management practices demonstrated to have the greatest impact. Focusing on the talent management pillars of talent development and talent engagement will likely yield substantiated results in increasing the self-efficacy of cyber talent. Beyond recruiting technical talent, retaining skilled personnel requires cultivating their self-efficacy through developmental opportunities. Talent management pillars that empower employees and build confidence will strengthen the DoD cyber workforce.

Chapter 3: Linking Self-Efficacy, Prosocial Motivation and Organizational Citizenship Behavior to Cyber Talent Management

Self-efficacy plays a significant role in shaping individuals' professional choices, their level of commitment to their chosen career path, their performance outcomes, their willingness to engage in increasingly demanding tasks and ultimately serves as a source of intrinsic motivation.[78] The distinctiveness of military and government service lies in the profound dedication to serve one's country to protect and defend others. In this respect, there is a correlation between selfless service (prosocial motivation) and the goals of military and government service. It propels individuals to voluntarily go above and beyond for coworkers and the company, which is called organizational civic behavior (OCB). Further, self-efficacy constitutes an integral component of an indispensable process of constructing meaning.[79] Scholarly discourse suggests that: 1) emerging professionals foresee obstacles within the realm of cybersecurity, and veterans need to promote and tell their stories to attract new talent; and 2) improving self-efficacy and culture can have a positive influence on the cybersecurity community.[80]

Self-efficacy, prosocial motivation and organizational citizenship behavior (OCB) are interconnected conditions. Literature suggests that self-efficacy enhances prosocial motivation and OCB,[81] and prosocial motivation impacts OCB positively.[82] Self-efficacy and prosocial motivation lead to favorable outcomes for OCB, resulting in desirable and beneficial employee actions and behaviors, such as altruism, teamwork and civic virtue.[83] Figure 1 depicts a way to visualize this relationship.

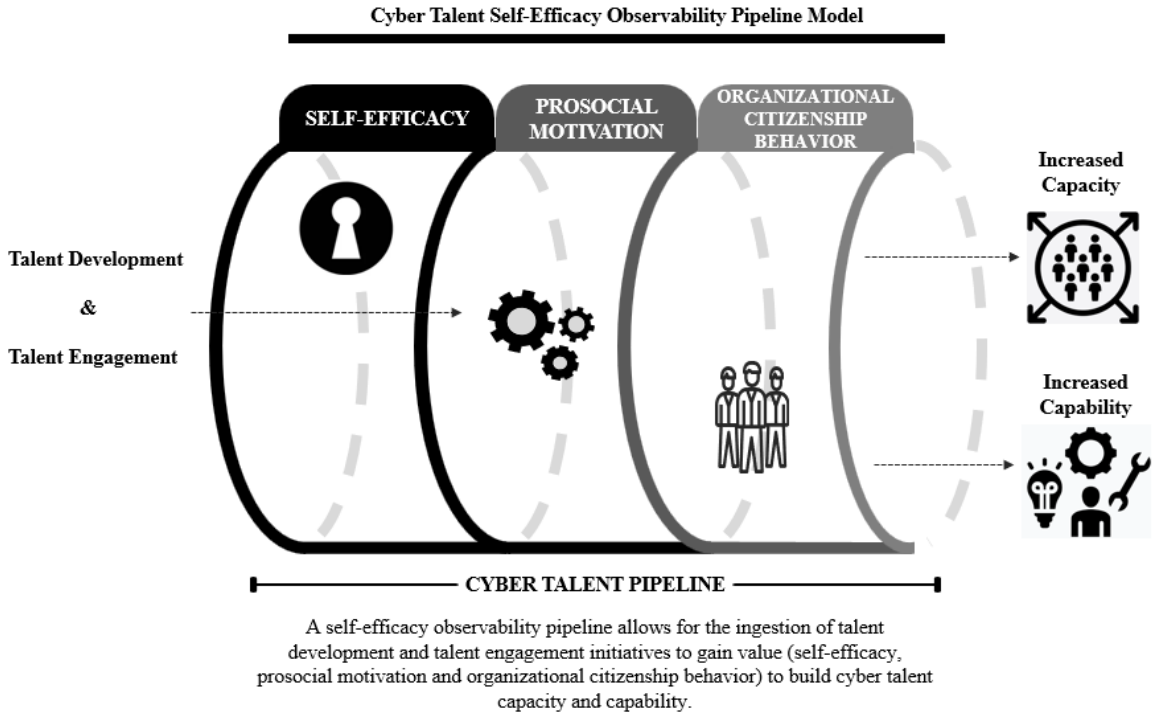

Figure 1: Cyber Talent Self-Efficacy Observability Pipeline Model (Design by author)

Prosocial motivation acts as a bridge between resources and work engagement, indicating high levels of work engagement as prosocial motivation levels rise.[84] In short, positivity is a byproduct of self-efficacy, in which a combination of high prosocial motivation and high self-efficacy tends to manifest in quality and committed employees.

Self-efficacy acts as a catalyst for prosocial motivation, which in turn manifests in increased positive organizational functioning of the institution and employee loyalty.[85] Overall, the connection between self-efficacy, prosocial motivation and OCB suggests that individuals who possess a strong belief in their capabilities and a genuine desire to benefit others are more likely to engage in behaviors that go beyond their formal job roles, contributing positively to the organizational environment. Further, increasing self-efficacy and prosocial motivation can positively impact talent acquisition and retention.

Talent acquisition is positively impacted by: 1) an increased attraction of talent, 2) a

positive organization reputation and 3) enhanced recruitment efforts. A workplace that fosters high self-efficacy and promotes a culture of prosocial motivation tends to attract talent. Further, individuals are drawn to environments where they feel they can contribute meaningfully and where their abilities are recognized and developed. Organizations known for empowering employees, nurturing their self-efficacy and encouraging prosocial behaviors tend to have a positive reputation. This reputation can attract and retain top talent, as people are inclined to join workplaces where they believe they can excel and make a difference. When an organization focuses on these factors, recruitment efforts benefit. The organization can thereby showcase its culture and values that resonate with candidates seeking environments where they can thrive and contribute beyond their roles.[86]

Increased talent retention is manifested through: 1) improved engagement and satisfaction, 2) benefits from development opportunities, 3) stronger relationships and 4) decreased turnover. Employees with higher self-efficacy are often more engaged as they feel confident in their abilities to meet challenges. Prosocial motivation manifests in individuals finding greater fulfillment in contributing to the welfare of others. This engagement and sense of gratification lead to higher job satisfaction, making employees more likely to stay with the organization. Further, organizations that invest in improving self-efficacy provide opportunities for skill development, growth and autonomy. When employees feel they are growing and enhancing their abilities, they are more likely to remain loyal to the organization. Additionally, fostering a culture of prosocial motivation encourages collaboration, empathy and support among employees. Stronger interpersonal relationships and a sense of belonging can significantly influence an individual's decision to stay within an organization. Last, higher self-efficacy and prosocial motivation can contribute to lower turnover rates. Employees who feel confident in their abilities and are connected to the organization are less likely to seek opportunities elsewhere.[87]

Prosocial motivation, a key driver of interest in military service, is influenced by self-efficacy, which plays a significant role in shaping professional choices, commitment and performance outcomes. The DoD can leverage the effects of self-efficacy through its talent development and talent engagement initiatives by fostering a culture of prosocial motivation and OCB. This combination of self-efficacy and prosocial motivation leads to increased positive organizational performance, loyalty and a positive brand. By nurturing self-efficacy and promoting prosocial motivation, the DoD can create an environment that attracts and retains top talent, leading to a more engaged workforce and reduced turnover.

Chapter 4: Evaluation of the DoD Cyber Workforce Strategy 2023-2027

The *DoD Cyber Workforce Strategy 2023-2027* establishes the framework for the DoD's efforts to cultivate a cyber workforce to carry out the department's diverse and ever-expanding cyber mission. The strategy's pillars encompass the identification of workforce needs, the recruitment of skilled individuals, the development of talent to align with mission requirements and the retention of personnel to address the cyber talent management challenges faced by the DoD. Collectively, these pillars aim to facilitate the department's capacity to see itself, understand the problem, and formulate data-driven decisions. This approach allows the DoD to proactively anticipate workforce trends through the implementation of standardized tools and processes for workforce analysis. Additionally, it involves ongoing efforts to enhance the capabilities of cyber personnel to meet emerging demands. Furthermore, the DoD advocates for the innovative utilization of human resource authorities. Lastly, it focuses on establishing strategic partnerships to support the growth, diversification and fortification of the cyber workforce. The endstate depicted in the document is a unified cyber workforce under the principles of diversity, equity, inclusion and accessibility (DEIA).[88]

The SECDEF states that the implementation of the *DoD Cyber Workforce Strategy Implementation Plan* will aid the department in promoting results-driven talent management activities to implement the goals and actions outlined in the Cyber Workforce Strategy. According to the SECDEF, the implementation plan is expected to support the DoD in its efforts to enhance personnel management activities, with a specific focus on cultivating a cyber workforce that is agile, flexible and responsive. The document states that the DoD currently experiences a twenty-five percent vacancy rate in

both military and civilian positions, but the department is currently constrained in its ability to "see itself," and is seeking to establish baseline vacancy rates in its CMF to establish recruitment and retention targets. The presented approach acknowledges the existing limitations in the cyber talent pipeline and emphasizes the need for the DoD to enhance diversity in its workforce by targeting underrepresented and untapped talent, which will contribute to increasing the acquisition of new cyber talent. The SECDEF articulates that this is a foundational plan that will evolve once personnel measures and trends are identified.[89]

In sum, the strategy and supporting implementation plan aim to synthesize data for analysis and decision-making to achieve four overarching goals: 1) to execute capability assessments to capture and define the DoD's cyber force requirements, 2) to establish a talent management program that is in line with both present and future needs, 3) to facilitate a cultural shift that optimizes personnel management activities and 4) to foster collaboration and partnership to enhance both capability development and operational effectiveness. Further, each of these objectives is associated with key performance indicators that assess the level of achievement. In addition, the DoD endeavors to establish a comprehensive categorization of all the occupational positions within its cyber workforce. This foundational step toward the professionalization of the DoD's cyber workforce will facilitate the identification and resolution of training deficiencies and the provision of policies and incentives within its services. In the context of this research, the DoD seeks to identify and target incentives that will help address its pipeline challenges and critical cyber workforce capability gaps. These initiatives will assist the DoD in its data-driven decision-making to maximize its investments, policies

and procedures for cyber talent management. The endstate of the strategy and plan is to reach 100% strength and operational readiness, supported by a self-sustaining culture and TMS.

In review, the strategy is foundational in terms of "professionalizing" the cyber workforce. It aims to fill gaps identified from Congressional reviews and studies and is aligned with current strategic guidance. Further, it incorporates an effective TMS but uses a legacy strategy of recruitment, versus talent acquisition. However, the strategy can be further evolved to incorporate self-efficacy as a tool for increasing the cyber talent pipeline, as well as establish self-efficacy as a cooperation/collaboration initiative for further scaling cybersecurity PPPs. These partnerships play a critical role in information exchange and constructing a robust cybersecurity ecosystem.[90]

The DoD does not need to research or develop a model of professionalization of a high-tech workforce with a high degree of self-efficacy. The next section presents such a model and suggests features of a talent strategy that can be considered for evolving the *DoD Cyber Workforce Strategy*.

Toward a Professionalization Strategy

The Defense Health Agency (DHA) established a strategic priority to create an enriching environment wherein performance is motivated by a sense of purpose, individual development is prioritized and competence is rewarded. As part of its *Strategic Plan 2023-2028*, DHA seeks to enhance the agency's workforce by implementing innovative talent acquisition strategies, prioritizing talent engagement and talent development investments. These efforts aim to bolster the capabilities of the workforce. DHA's talent management goal is to attract and retain a diverse and highly skilled workforce through a strategic approach that fosters a people-centric work environment.[91] The key factor to the DHA's talent strategy is the professionalization of its workforce through top-down processes.

The concept of professionalization has two main precepts. First, it entails the educational, training, credentialing and privileging activities that facilitate the transition of an individual into a professional team member. Secondly, it encompasses the social mechanisms through which a particular occupation evolves into a recognized and established profession.[92] Professionalizing a workforce involves several components aimed at elevating the skills, knowledge, behavior and overall standards within a specific field or industry. These components typically include:

1. Training and Development: Offering structured programs, workshops, seminars, or certifications to improve technical skills, industry knowledge and professional competencies to facilitate continuous learning.
2. Certifications and Qualifications: Encouraging or mandating personnel to obtain industry-recognized certificates, licenses or qualifications to

demonstrate their knowledge and advance their careers.

3. Standardized Practices and Protocols: Implementing guidelines and protocols to realize quality, consistency of performance and professionalism.
4. Ethical Standards and Codes of Conduct: Promoting integrity through the implementation and reinforcement of ethical standards.
5. Mentorship and Coaching Programs: Experienced professionals mentor newer or less experienced personnel to promote knowledge transmission, skill development and professional belonging.
6. Career Pathways and Advancement Opportunities: Providing avenues for career growth and promotion in the field, such as promotions, lateral transfers and specialized roles based on talents and knowledge.
7. Professional Associations and Networking: Promoting and incentivizing participation or membership in industry events and professional associations.
8. Performance Evaluation and Feedback: Creating fair, transparent methods for constructive criticism to set expectations and improve performance outputs.
9. Recognition and Rewards: Recognizing and rewarding performance and accomplishments with awards, bonuses and skill incentives.
10. Implementing a Continuous Improvement Culture: Promoting innovation, learning and adaptability to industry changes by encouraging employees to ask for feedback, make changes and have a growth mentality.[93]

A holistic strategy to professionalize a workforce raises standards, improves skills and maintains a profession or industry's legitimacy and effectiveness.

The field of cybersecurity has evolved since the inception of shared and

networked computers. The cyber workforce has existed for over 50 years, but it is not yet recognized as a distinct professional domain with specialized areas. Workers are increasingly identifying as cybersecurity experts based on their responsibilities, experience and expertise. Additionally, government and business sector organizations are aggressively promoting this field's professionalization. Professional societies in computer science, computer engineering, and cybersecurity have worked to build knowledge frameworks and ethical standards. Several government departments, including the DoD, the Department of Homeland Security (DHS), the National Security Agency (NSA) and the Office of Personnel Management (OPM) are now engaged in workforce development initiatives. Further, there has been an increasing proliferation of educational institutions that provide academic programs focused on cybersecurity. These accreditations are granted based on predetermined criteria established collaboratively by the federal agencies. Last, there has been a notable proliferation of certificates and certifications in diverse areas of cybersecurity expertise and specializations.[94]

The DHA's key strategy is the professionalization of its workforce through top-down processes, which include educational, training, credentialing and privileging activities. Comparatively, the professionalization of the cyber workforce in the DoD is currently a bottom-up process and is foundational in its approach and strategy. The *DoD Cyber Workforce Strategy 2023-2027* and the *DoD Cyberspace Workforce Qualification and Management Program* promote educational attainment and certification within its workforce facilitate the creation of educational curriculum, educational programs and advocate for the utilization of certification as a regulatory mechanism.[95] [96] See Table 1.

	Talent Strategy	
Components	**DoD Cyber**	**DHA**
Training & Development	Passive	Active
Certifications & Qualifications	Passive	Active
Standardized Practices & Protocols	Active	Active
Ethical Standards & Codes of Conduct	Active	Active
Mentorship & Coaching Program	Active	Active
Career Pathways	In-Progress	Active
Professional Associations & Networking	Passive	Active
Performance Evaluation & Feedback	Active	Active
Recognition & Rewards	Partial	Active
Continuous Improvement Culture	Active	Active

Table 1: Comparison Table DoD and DHA Professionalization Strategy Implementation (Table by author)

The DoD should adopt a top-down approach, as matured within the DHA's talent strategy, to fully actualize the goals of professionalization to build the capacity (pipeline) and capability (knowledge, skills and abilities) of the nation's cybersecurity workforce.[97] Additional leadership focus on the "Passive" or "Partial" components of the *DoD Cyber Workforce Strategy* could serve as a starting point for its next update.

Chapter 5: Findings & Recommendations

When talent is aligned with the resources needed to succeed, individual and organizational performance can be maximized in quality, innovation and efficiency. Why do some employees freely demonstrate innovation; ensure high-quality output; adhere to organizational principles, norms, and regulations; work effectively and efficiently within constraints; engage in constructive interactions with others and actively contribute to problem-solving?[98] The findings of this research demonstrate that increasing self-efficacy improves prosocial motivation and organizational citizenship behavior. Talent development and talent engagement initiatives provide the greatest means to boost the DoD's cyber workforce self-efficacy, which in turn will yield increased talent acquisition and retention. The factors of personal drive, personal investment and civic engagement in the workplace manifest into the formation of affective commitment.[99] The DoD can enhance its cyber talent strategy by building self-efficacy toward cybersecurity careers. This approach promotes career opportunities, stability, and autonomy, fostering collaboration and innovation within the *DoD Cyber Workforce Strategy*. Developing personnel self-efficacy is crucial for advancing the *DoD Cyber Workforce Strategy*, fostering collaboration and enhancing the collective capacity of the cybersecurity enterprise.

This research recommends that DoD should adopt a professionalization strategy to further evolve the *DoD Cyber Workforce Strategy 2023-2027* to incorporate self-efficacy as a tool for increasing the cyber talent pipeline.

To posit the recommendation, addressing the cyber talent pipeline dilemma requires addressing candidate self-efficacy deficiencies. Experiential learning, game-

based strategies and educational simulations can boost confidence and skills. The DoD can foster a culture of prosocial motivation and OCB to attract and retain top talent, leading to increased organizational performance and loyalty. A top-down approach is needed to build the DoD's cybersecurity workforce. The *DoD Cyber Workforce Strategy 2023-2027* can be further evolved to incorporate self-efficacy as a tool for increasing the cyber talent pipeline, as well as establish self-efficacy as a cooperation/collaboration initiative for further scaling cybersecurity PPPs.

In light of the research findings, it is recommended that the DoD should emphasize fostering self-efficacy among individuals in pursuit of careers in cybersecurity to evolve its talent strategy and strive to lead rather than simply win the nation's accumulation of cyber talent. The following specific recommendations/ways are provided:

1. Institute a top-down talent management approach to professionalizing the cyber workforce.

To address the gaps in implementing the educational, training, credentialing and privileging professionalization standards of practice in the *DoD Cyber Workforce Strategy 2023-2027*, it is recommended that the DoD employ a top-down cyber talent management approach that is incentives-based. Incentive management can provide the means to close the gaps of cybersecurity professionalization for the DoD. Current prioritized funding support can used for the establishment of accession bonuses for direct commission contracts, Variable Special Pay (VSP) for the acquisition of critical skill positions, Certified Special Pay (CSP) to reward the cyber workforce credentialing/privileging and additional special pay and retention bonuses for hard-to-fill

positions and continued service. Non-monetary incentives can include dedicated time, or extra leave allowances, to study for and complete certifications. These incentives can help DoD increase the self-efficacy/motivation of personnel to continue service past their initial service obligations. Alongside these incentive structures, DoD cyber personnel should be provided personalized career pathways for full professionalization and lifelong personal and professional growth.

2. Establish a Cybersecurity Ambassadorship Engagement Program.

Establishing a Cybersecurity Ambassadorship Engagement Program and developing cybersecurity experiential labs, gaming applications and PCSs can be achieved through PPPs. These efforts can bear fruit in improving the stream of qualified candidates into the field and DoD.

3. Revamp personnel service policies.

Consideration should be given to revamping DoD, service and component policies to clearly define cyber-service obligations, relax or alleviate tour length/movement requirements and promote mission area specialization. This endeavor can help mitigate dissatisfaction with the military lifestyle by allowing for the stabilization of personnel in their desired locations, which is important in improving family quality of life and supporting dual-career families.

4. Develop cybersecurity experiential labs, gaming applications and PCSs.

Personnel self-efficacy is affected by personal and situational factors. Experience builds mastery/confidence and self-efficacy. Game-based methods engage and improve skills. PCS simulations let students experience real-world circumstances and solve difficulties. These tools improve students' cybersecurity knowledge and confidence.

These tools can be developed in partnership with the cyber enterprise for mutual benefit.

By implementing these recommendations, the DoD can increase the number of personnel entering and remaining in the cyber talent pipeline in ways that would not require a disproportional investment of resources to the benefits. In support, the means are: 1) the current prioritized funding to build the capacity and capability of the cyber workforce, 2) the current strategic guidance to scale PPPs and 3) the implementation plan initiative to establish a part-time surge support capacity in the Reserve Component.

Chapter 6: Conclusion

As our world becomes increasingly interconnected through digital networks and information technology, cybersecurity has emerged as a top national security priority for the U.S. High-profile cyberattacks on critical infrastructure and government agencies demonstrate that no entity is immune from these threats. Further, these incidents underscore how cyber operations are now an integral part of modern hybrid warfare. In the *2023 National Cybersecurity Strategy*, the POTUS calls for cooperation and collaboration within the cybersecurity enterprise (government, academia and the private sector) to strengthen and diversify America's cyber workforce.[100] In response, the POTUS challenges the entire cybersecurity enterprise to remove the gatekeepers, myths and other impairments for the profession, and develop ways to make a career in cybersecurity accessible and attainable to every American who desires to pursue and attain it.[101] In support, the POTUS declares that to keep up with the rapid evolution of the cyber ecosystem, the administration will coordinate with lawmakers to secure adequate funding for cybersecurity initiatives.[102]

For the DoD, securing cyberspace is essential across all domains of warfare. Cyber capabilities are deeply integrated into U.S. military operations, combat plans and joint warfighting doctrine. From intelligence gathering to offensive operations, the cyber domain provides capabilities for and imposes risk to critical American military capabilities. Adversaries like the PRC and Russia are rapidly building up their cyber forces, posing an asymmetric threat designed to counter traditional U.S. military advantages. This pressing threat environment demands that the DoD continue building a world-class cyber workforce to defend vital national interests. Strengthening

cybersecurity and expanding cyber forces are urgent priorities for the DoD. Cyber threats continue growing more diverse, elegant and destructive with each passing year. Malicious state-sponsored hackers, criminal networks and extremist groups all utilize cyber capabilities to further their aims at America's expense. Russia's invasion of Ukraine also highlights how cyber warfare is now a key feature of modern military campaigns. To counter this complex array of threats in cyberspace and the electromagnetic spectrum, the DoD must recruit top talent, foster innovation and invest in emerging technologies. By maintaining superiority in the cyber domain, the U.S. military can deter aggression, prevail in kinetic conflict and safeguard the nation's security.

Building capacity and capability in the nation's cyber talent pipeline is a national imperative and a critical enabler for the DoD to become an "employer of choice,"[103] as well as mitigating its challenge of retaining its very best talent.[104] The DoD is hardly alone in struggling to find and retain cybersecurity talent. Estimates suggest the global cybersecurity workforce must grow by 145% to meet demand and manage risks by 2030.[105] The supply-demand gap stems from society's rapid digitization and new technological threats outpacing the professionalization of cybersecurity, and the most recent study cites that the gap between needed and available cybersecurity personnel has grown 12.6% year over year.[106] Cyber roles require highly specialized skills that constantly need updating, contributing to quick turnover. Within the DoD specifically, an understaffed cyber workforce has become a critical national security issue. Persistent personnel shortfalls have put sensitive systems and operations at risk, and there are critical skill gaps in AI/Machine Learning, Cloud Computing Security and Security Engineering/Zero Trust Implementation.[107] The cause for further concern stems from the

aging demographics of the DoD cyber workforce, with nearly two-thirds of personnel above age 45. As older cyber staff approach retirement, the DoD must recruit and develop younger talent. Yet Gen Z and young Millennials are detached and uninterested in the DoD compared to other sectors. [108] Failure to attract this cohort could leave the DoD dangerously understaffed. Fostering a culture of service is essential to overcoming the recent recruitment challenges faced by the DoD. Prosocial motivation is the main justification offered by the majority of political leaders for encouraging military/government service.[109]

The DoD has implemented various initiatives to address critical staffing gaps, from upskilling programs to recruitment bonuses to academic partnerships. However, many of these efforts adopt a reactive, piecemeal approach focused on quickly getting more people into the cyber workforce.[110] What's missing is a proactive, people-centric strategy, based on principles of workforce professionalization, with high organizational engagement and the prioritization of professional development and growth.

Strategic human capital management research indicates taking this people-focused approach is vital for building an agile, high-performing workforce suited for the digital age. Traditionally, organizations like the DoD have treated employees as interchangeable assets meant to fill roles rather than as individuals with unique passions, strengths and purposes who seek opportunities for personal growth.[111] However, today's workforce desires work-life integration where they can harmonize professional and personal identity and customized career experiences tailored to their evolving skills and interests.[112]

Centering talent strategy on empowering people pays dividends. Organizations rated highly on people-focused culture benefit from greater workforce productivity,

innovation, collaboration, knowledge sharing and reduced turnover. People-centric cultures also foster diversity and inclusion, enabling organizations to benefit from a wider range of perspectives and talents.[113] For the DoD, a humanistic approach to cyber workforce strategy will require fundamentally rethinking how it attracts, develops, organizes, and motivates personnel. Research on self-efficacy provides pathways for this transformation.

Cultivating self-efficacy for the DoD's cyber workforce should significantly enhance recruitment, retention and performance. Personnel who believe in their cyber skills and capacity to continually improve them will likely feel greater motivation for DoD service, commitment to mission and empowerment in their military and civilian roles. Highly efficacious cyber staff will pursue more learning opportunities, attempt more difficult tasks and persist through the problem-solving challenges inherent in cyber work. Increased self-efficacy should strengthen the DoD's cyber talent pipeline and enable current personnel to combat emerging threats better.

Further, promoting the development of self-efficacy and work-readiness plays a crucial role in establishing a sustainable pipeline, and must be a part of an effective talent acquisition strategy. Cultivating self-efficacy toward a cybersecurity career must be incorporated end-to-end within the TMS and is an enabler for the human capital pillars of talent acquisition, alignment, development and management. Therefore, an effectively designed talent strategy should optimize the self-efficacy of the talent pipeline to be resilient. The ability of DoD to effectively attract and retain cyber talent is of paramount importance in attaining and maintaining a competitive edge in cyberspace, and increasing the self-efficacy of its future and current cyber workforce can help create a sustained

pipeline of cyber talent. Further, increasing the self-efficacy toward a career in cybersecurity can be a cooperation and collaboration mechanism for scaling PPPs within the cyber enterprise, and the current chaotic and anarchic environment of hyper-competition for cyber talent. Doing so is in line with current national strategic guidance and funding priorities and is relevant through the prioritization of the ongoing strategic advancement of a flexible, skilled and ready DoD cyber workforce.

Expanding and diversifying recruitment pipelines will provide another lever for enhancing DoD cyber workforce self-efficacy. Currently, DoD cyber roles lack gender, racial, ethnic and neurodiversity, drawing from a narrow talent segment.[114] However, extensive research confirms that diversity and inclusion are vital for maximizing workforce performance, especially in complex, cognitively demanding fields like cybersecurity. Teams comprised of members with diverse backgrounds and thought patterns consider more information, generate more solution options and identify more nuanced risks.[115] Underrepresented groups also often have untapped talents and non-traditional educational backgrounds valuable in the field of cybersecurity.[116]

Critically embracing diversity requires going beyond recruitment to foster inclusion, where individuals feel valued, respected and able to express their authentic identities. Cyber personnel who feel comfortable bringing their whole selves to work experience greater belonging, empowerment, engagement and intent to stay. These outcomes stem from increased self-efficacy when work contexts enable people to harmonize their personal and professional identities.[117] Diversity and inclusion practices will expand the DoD's cyber talent pool while enabling recruited personnel to maximize their self-efficacy.

Finally, borrowing from the DHA talent strategy, the DoD should provide cyber personnel with customized career pathways, leading to full professionalization and facilitating lifelong professional and personal growth. Traditional rigid career ladders no longer motivate today's workforce, who instead seek opportunities to continually gain new skills and experiences aligned with their evolving passions and talents. The DoD should thus offer cyber staff flexible career paths with built-in on and off-ramps for retraining, rotational assignments, stretch roles and sabbaticals. Research shows that employees feel more agency over their development and future when organizations support customized career journeys.[118] This agency activates the personal choice source of self-efficacy.[119] Personnel also gain exposure to more diverse experiences, building wider competence. Adaptive career pathways will empower cyber staff to expand their capabilities while pursuing meaningful work continuously.[120] This fosters retention and enables the DoD to fully leverage investments in its cyber workforce.

Fundamentally, the DoD has yet to place the cyber workforce at the center of its human capital strategy. To evolve its approach, the DoD should draw upon research on self-efficacy to increase cyber personnel recruitment, retention and performance. Decades of research have shown that self-efficacy is a strong predictor of motivation, perseverance, resiliency and success across educational and technology adoption contexts.[121] By building cyber workforce self-efficacy, the DoD can empower personnel to overcome current obstacles, while removing barriers to future career growth and advancement. Talent development and talent engagement initiatives in the cyber talent pipeline, mediated by self-efficacy, will yield increased prosocial motivation and organizational citizenship behavior within the talent pool, enabling a Cyber

Ambassadorship Program and the scaling of private partnerships through the pipeline, ultimately resulting in the increased capacity and capability of the pipeline (Figure 2).

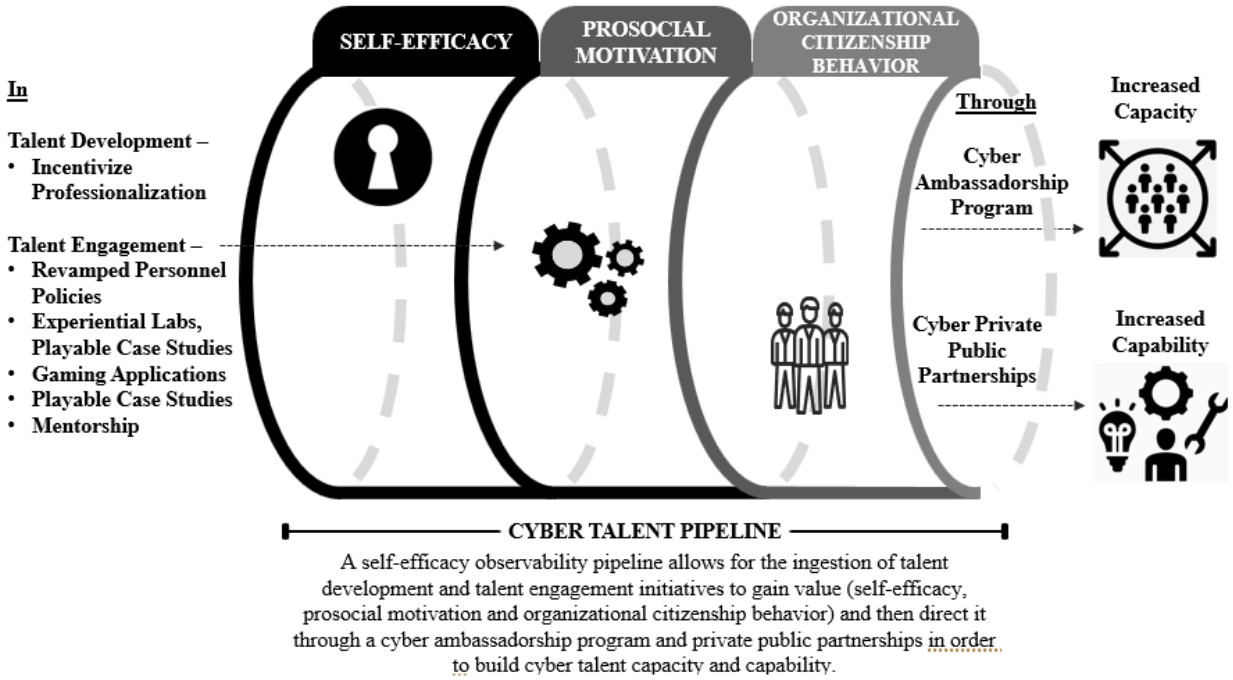

Figure 2: Expanded Cyber Talent Self-Efficacy Observability Pipeline Model (Design by author)

The current research can be continued to determine how future and current DoD employees respond to the recommended cyber talent management measures implemented. Future research can be conducted relating their level of self-efficacy to any effect on talent acquisition and retention. Future research can also be performed focusing on the relationship of development programs, self-efficacy and job performance.

Ethical Considerations

The POTUS established the National Infrastructure Advisory Council (NIAC) to ethically evaluate and improve PPP coordination to secure vital infrastructure.[122] The

private industry owns and operates 85% of our cybersecurity-critical network infrastructure, and the DoD has established PPPs to build a cybersecurity service provider network to defend this vital infrastructure. Additionally, policies and procedures have been developed for resource and information exchange within these PPPs, which operate in the same regulatory framework as the DoD.[123] The mature culture of existing partnerships allows the network to be scaled beyond perceived boundaries and within normalized activities. This strategy seeks to scale PPPs to facilitate resource interchange and improve DoD and their interactions for a common cause.

As the DoD must preserve public trust, it must establish procedures to ensure compliance with law and policy. Therefore, the recommended strategy must follow four ethical principles, and should: 1) not damage public trust, 2) maximize transparency, 3) support the core mission of protecting critical infrastructure and 4) hold agency staff accountable for implementing partnership rules and principles. Key implementation guidelines are as follows: 1) all policies, procedures and guidelines regulating partnerships with private industry should be made public to promote transparency; 2) the public should understand that the rewards outweigh the risks; 3) a formal comprehensive review process must be used to evaluate partnership decisions and 4) the DoD must identify private entities that should be excluded from partnerships.[124]

Appendix 1: Utilization of Army Data for Academic Research

DEPARTMENT OF THE ARMY
UNITED STATES ARMY WAR COLLEGE AND CARLISLE BARRACKS
CARLISLE, PA 17013-5242

CSWC-CSL 17 October 2024

MEMORANDUM FOR RECORD

FROM: United States Army War College, Center for Strategic Leadership. 122 FORBES AVENUE, CARLISLE, PA 17013-5234

SUBJECT: Utilization of Army Data for Academic Research

1. As the current steward of following data files, I approve LTC Jeremiah Hood to utilize them for academic research and use. To include publication and presentations.

   - U.S. Army Cyber Command. U.S. Army Cyber Command (ARCYBER) Retention Study (ARS). Unpublished survey brief for Lieutenant General Stephen G. Fogarty Commanding General, U.S. Army Cyber Command and Mr. Ronald W. Pontius, SES Deputy to the Commanding General, U.S. Army Cyber Command, last modified 9 December 2019. Portable Document Format file.

   - U.S. Cyber Command. Retention in Cyber Command. Unpublished survey findings, last modified 2021. Portable Document Format file.

2. POC for this memo is undersigned at chad.t.bates.mil@army.mil or (717) 245-4710.

BATES.CHAD.THOMAS.1126790364 Digitally signed by BATES.CHAD.THOMAS.1126790364 Date: 2023.10.17 12:54:13 -04'00'

CHAD T. BATES, PhD
Colonel, Cyber
Center for Strategic Leadership
U.S. Army War College

Appendix 2: Definition of Key Terms

The study examined the longitudinal relations among the individual relations of emotional, social, and work beliefs and behaviors, as well as their moderating and mediating effects on talent strategy. Social cognitive studies and the overarching social cognitive career theory (SCCT) provide valuable insight into how individual inputs, contextual affordances, and sociocognitive variables influence the development of vocational interests, career objectives, and actions.[125] For context, the terms used within this study are defined as follows:

- Organizational Citizenship Behavior: The concept of organizational citizenship behavior (OCB) encompasses all constructive and positive actions and behaviors exhibited by employees beyond the scope of their official employment responsibilities. It is anything that employees do for the benefit of the organization as a whole and in support of their coworkers.[126]
- Prosocial Motivation: Prosocial motivation refers to the human activity and meaningful commitment to serve, patriotism, and the desire to safeguard others. Prosocial motivation provides meaning in military service.[127]
- Self-efficacy: Self-efficacy refers to an individual's belief in their capacity to perform a task or achieve a goal. It encompasses an individual’s belief in their ability to regulate their own actions/decisions, exert influence over their environment, and maintain motivation while striving to achieve their objectives. Self-efficacy can be manifested in a variety of contexts and

domains, such as education, career, personal and professional relationships, and work/life situations.[128]

- Talent Development: Talent development is an integral component of talent management. Talent development enhances the knowledge, abilities, skills, and competencies of individuals within a career field, which are closely linked to their active involvement and commitment.[129]
- Talent Engagement: Talent engagement is the inclination and involvement of professionals to achieve organizational goals. Talent engagement comprises a strategy for capitalizing on human resources by providing extrinsic and intrinsic rewards to create or sustain employee motivation.[130]

Bibliography

Aguenza, Benjamin Balbuena and Ahmad Puad Mat Som. "Motivational Factors of Employee Retention and Engagement in Organizations*." International Journal of Advances in Management and Economics* 1, no. 6 (April 2018): 88-95. https://www.managementjournal.info/index.php/IJAME/article/view/233.

Ali, Mohammad, Muhammad Ullah, and Souman Guha. "Role of Talent Development on Talent Engagement and Self-Efficacy: A Structural Model." *Journal of Social Economics Research* 7, no. 2 (October 2020): 118-129. https://www.researchgate.net/publication/345083695.

Arshad, Muhammad, Ghulam Abid, Francoise Contreras, Natasha Saman Elahi, and Muhammad Ahsan Athar. "Impact of Prosocial Motivation on Organizational Citizenship Behavior and Organizational Commitment: The Mediating Role of Managerial Support," *European Journal of Investigation in Health, Psychology and Education*, no. 11 (May 2021): 436-449. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8314358/.

Bashir, Masooda, Colin Wee, Nasir Memon, and Boyi Guo. "Profiling Cybersecurity Competition Participants: Self-Efficacy, Decision-Making and Interests Predict Effectiveness of Competitions as a Recruitment Tool." *Computers & Security* 65 (March 2017): 153–165. https://doi.org/10.1016/j.cose.2016.10.007.

Bandura, Albert, Claudio Barbaranelli, Gian Vittorio Caprara, and Concetta Pastorelli. "Self-Efficacy Beliefs as Shapers of Children's Aspirations and Career Trajectories." *Child Development* 72, no. 1 (January-February 2001): 187-206. https://www.jstor.org/stable/1132479.

Bandura, Albert, Wendy Freeman, and Richard Lightsey. "Self-Efficacy: The Exercise of Control." *Journal of Cognitive Psychotherapy* 13, no. 2 (January 1, 1999): 158–166. https://doi.org/10.1891/0889-8391.13.2.158.

Bandura, Albert. "Self-efficacy: Toward a unifying theory of behavioral change." *Advances in Behavior Research and Therapy* 1, no. 4 (1978): 191-215. https://doi.org/10.1016/0146-6402(78)90002-4.

Bates, Chad, and Charlene Rose. "Leveraging Talent to Dominate in Cyber War—An Army Perspective." Edited by Adib Farhadi, Ronald P. Sanders, Anthony Masys. *The Great Power Competition* 3 (16 September 2022): 319-346. Springer, Cham. https://doi.org/10.1007/978-3-031-04586-8_16.

Bates, Chad, Charlene Rose. "Understanding—and Fixing—The Army's Challenge in Keeping Cyber Talent." *Modern War Institute at West Point*. May 17, 2022. https://mwi.westpoint.edu/understanding-and-fixing-the-armys-challenge-in-keeping-cyber-talent/.

Blue Star Families. “Military Family Lifestyle Survey: 2022 Comprehensive Report.” 2022. https://bluestarfam.org/wp content/uploads/2023/03/BSF_MFLS_Spring23_Full_Report_Digital.pdf.

Bonsignore, Elizabeth, Derek L. Hansen, Daniel T. Hickey and Kevin Kartchner. “The Playable Case Study Authoring and Simulation Platform.” *ResearchGate*, June 7, 2022. https://www.researchgate.net/publication/360936147_The_Playable_Case_Study_Authoring_and_Simulation_Platform.

Brimhall, Kim C., Erica Leeanne Lizano and Michàlle E. Mor Barak. “Do work-life inclusion policies predict inclusion climate? Exploring the mediating role of work-life conflict and enrichment.” *Human Resource Management* 56, no. 4 (April 2017): 681-701. https://doi.org/10.1002/hrm.21972.

Buckwalter, Naomi. Interview with Jen Stone: The Myth of the Cybersecurity Workforce Shortage. *Security Metrics*. Podcast 27. Accessed August 27, 2023. https://www.securitymetrics.com/learn/myth-of-the-cybersecurity-workforce-shortage.

Chairman Joint Chiefs of Staff. “Joint Concept for Competing.” Washington, D.C. 10 February 2023. https://s3.documentcloud.org/documents/23698400/20230213-joint-concept-for-competing-signed.pdf.

Chairman Joint Chiefs of Staff. “Joint Operating Environment 2035.” Washington, D.C. 14 July 2016. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf.

Chen, Tianying, Jessica Hammer, and Laura Dabbish. “Self-Efficacy-Based Game Design to Encourage Security Behavior Online.” *Proceedings of CHI Conference on Human Factors in Computing Systems Extended Abstracts*, May 2, 2019. https://doi.org/10.1145/3290607.3312935.

Cherry, Kendra. “Self Efficacy and Why Believing in Yourself Matters.” Updated on February 27, 2023. Verywellmind. https://www.verywellmind.com/what-is-self-efficacy-2795954.

Cyberseek. “Cybersecurity Supply/Demand Heat Map.” Accessed October 2, 2023. https://www.cyberseek.org/heatmap.html.

Defense Business Board. FY23 Assessment of the Department of Defense: Building a Civilian Talent Pipeline. Washington, D.C.: March 2023. https://dbb.defense.gov/Portals/35/BCTPV4.pdf.

Defense Business Board. Public-Private Collaboration in the Department of Defense. Report 12-04. Washington, D.C.: July 2012. https://dbb.defense.gov/Portals/35/Documents/Reports/2012/FY12-4_Public_Private_Collaboration_in_the_Department_of_Defense_2012-7.pdf.

Defense Health Agency. Strategic Plan 2023-2028. Falls Church, VA: Defense Health Agency, 31 July 2023. https://www.health.mil/Reference-Center/Publications/2023/07/31/DHA-Strategic-Plan.

Delaney, Molly L. and Mark A. Royal. "Breaking engagement apart: The role of intrinsic and extrinsic motivation in engagement strategies." *Industrial and Organizational Psychology* 10, no. 1 (March 2017): 127-140. https://doi.org/10.1017/iop.2017.2.

Ellett, Alberta June Shelinbarger, "Human Caring, Self-Efficacy Beliefs, and Professional Organizational Culture Correlates of Employee Retention." (2000). LSU Historical Dissertations and Theses. 7263. https://repository.lsu.edu/gradschool_disstheses/7263.

Fuller, Joseph B, Manjari Raman, Eva Sage-Gavin and Kristen Hines. "Hidden Workers: Untapped Talent." Published by Harvard Business School Project on Managing the Future of Work and Accenture, September 2021. https://www.hbs.edu/managing-the-future-of-work/Documents/research/hiddenworkers09032021.pdf.

Giboney, Justin Scott, Jason K. McDonald, Jonathan Balzotti, Derek L. Hansen, Desiree M. Winters, and Elizabeth Bonsignore. "Increasing Cybersecurity Career Interest through Playable Case Studies." *TechTrends* (February 8, 2021). https://doi.org/10.1007/s11528-021-00585-w.

Gibson, Sharon K. "Social Learning (Cognitive) Theory and Implications for Human Resource Development." *Advances in Developing Human Resources* 6, no.2 (May 2004): 193-210. https://doi.org/10.1177/1523422304263429.

Gilpin, Robert. *War and Change in World Politics*. Cambridge: Cambridge University Press, 1981. https://doi.org/10.1017/CBO9780511664267.

Gist, Marilyn E. and Terence R. Mitchell. "Self-efficacy: A theoretical analysis of its determinants and malleability." *Academy of Management Review* 17, no. 2 (1992): 183-211. https://www.jstor.org/stable/258770?seq=8.

Grant, Adam M. and David M. Mayer. "Good soldiers and good actors: Pro-social and impression management motives as interactive predictors of affiliative citizenship behaviors. *Journal of Applied Psychology* 94, no. 4 (2009): 900–912. https://doi.org/10.1037/a0013770.

Harsch, Katharina and Marion Festing. “Dynamic talent management capabilities and organizational agility: A qualitative exploration.” *Human Resource Management* 59, no. 5: 43-61. https://doi.org/10.1002/hrm.21972.

Hillner, Eric P. “The Third Offset Strategy and the Army Modernization Priorities.” *Center for Army Lesson’s Learned*. May 2019). https://usacac.army.mil/sites/default/files/publications/17855.pdf.

Hongal, Pushpa and Uttamkumar Kinange. “A Study of Talent Management and Its Impact on Performance of Organizations.” *International Journal of Engineering and Management Research* 1o, no. 1 (February 2020): 64-71. https://doi.org/10.31033/ijemr.10.1.12.

International Information System Security Certification Consortium. “Cyber Workforce Study 2019.” Accessed November 27, 2023. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2019.pdf?rev=52055d08ca644293bd7497725bb7fcb4.

International Information System Security Certification Consortium. “Cyber Workforce Study 2023.” Accessed November 27, 2023. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4.

Isa, Aerni, Hazril izwar Ibrahim, Amar Hisham Jaafar, and Nur Lyana Baharin. “Talent management practices, perceived organizational support and employee retention: Evidence from government-linked companies.” *Global Business and Management Research* 10, no. 3 (December 2018): 688-696. https://www.researchgate.net/publication/330037565_Talent_Management_Practices_Perceived_Organizational_Support_and_Employee_Retention_Evidence_From_Malaysian_Government-Linked_Companies.

Jaiswal, Neeraj Kumar and Rajib Lochan Dhar. “The influence of servant leadership, trust in leader and thriving on employee creativity.” *Leadership & Organization Development Journal* 38, no. 1 (January 2017): 2-21. In press. https://doi.org/10.1108/LODJ-02-2015-0017.

Jones, Gareth R. “Socialization tactics, self-efficacy, and newcomers' adjustments to organizations.” *Academy of Management Journal* 29, no. 2 (June 1986): 262-279. https://www.jstor.org/stable/256188.

Kania, Elisa B. “In Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovate.” *The Strategy Bridge*, August 27, 2019. https://thestrategybridge.org/the-bridge/2019/8/27/in-military-civil-fusion-china-is-learning-lessons-from-the-united-states-and-starting-to-innovate.

Ke, Weiling and Kwok Kee Wei. “Organizational culture and leadership in ERP implementation.” *Decision Support Systems* 45, no. 2 (May 2008): 208-218. https://doi.org/10.1016/j.dss.2007.02.002.

Kim, Sun Young and Sergio Fernandez. “Employee Empowerment and Turnover Intention in the U.S. Federal Bureaucracy.” *The American Review of Public Administration* 41, no.1 (January 2017), 4-22. https://doi.org/10.1177/0275074015583712.

Kravariti, Foteini and Karen Johnston. “Talent Management: A Critical Literature Review and Research Agenda for Public Sector Human Resource Management.” *Public Management Review* 22, no. 1 (July 2019): 75–95. https://doi.org/10.1080/14719037.2019.1638439.

Lent, Robert W., Steven D. Brown and Gail Hackett. “Toward a Unifying Social Cognitive Theory of Career and Academic Interest, Choice, and Performance.” Journal of Vocational Behavior 45, no. 1 (August 1994): 79-122. https://doi.org/10.1006/jvbe.1994.1027.

Lucas, William A., Sarah Y. Cooper, Tony Ward and Frank Cave. “Industry Placement, Authentic Experience and the Development of Venturing and Technology Self-Efficacy.” *Technovation* 29, no. 11 (November 2009): 738-752. https://doi.org/10.1016/j.technovation.2009.06.002.

Lunenburg, Fred C. “Self-Efficacy in the Workplace: Implications for Motivation and Performance.” International Journal of Management, Business, and Administration 14,
no. 1 (January 2011): 1-6.
http://www.nationalforum.com/Electronic%20Journal%20Volumes/Lunenburg%2C%20Fred%20C.%20SelfEfficacy%20in%20the%20Workplace%20IJMBA%20V14%20N1%202011.pdf.

Mandiant. “M-Trends 2023.” Accessed November 29, 2023. https://www.mandiant.com/m-trends.

Medicine and the Military. “Physician Salary + Compensation.” Accessed October 6, 2023. https://www.medicineandthemilitary.com/career-and-lifestyle/physician-salary-and-compensation.

Ming, Jian, Colin Wee and Masooda Bashir. “Self-Efficacy in Cybersecurity Tasks and Its Relationship with Cybersecurity Competition and Work-Related Outcomes.” 2016 USENIX Workshop on Advances in Security Education. https://www.usenix.org/sites/default/files/conference/protected-files/ase16_slides_wee.pdf.

Nakasone, Paul M. “An Interview with Paul M. Nakasone.” *Joint Force Quarterly* 92, (2019): 4-9. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf.

National Academy of Public Administration. “A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation.” Washington, D.C.: January 2022. https://s3.us-west-2.amazonaws.com/napa-2021/NAPA-Final-CISA-Cybersecurity-Workforce-Report.pdf.

National Research Council. *Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision Making*. Washington D.C.: National Academies Press, 2013. https://doi.org/10.17226/18446.

National Security Council. “Sharing Information with the Private Sector.” Accessed November 16, 2023. https://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionV.html.

Obeidat, Bader, Areej Al-Khateeb, Abdallah Abu Abdallah, and Ra’ed Masa’deh. “Reviewing the mediating role of work/life balance and motivational drivers of employee engagement on the relationship between talent management and organization performance.” *Journal of Social Sciences* 8, no. 2 (April 2019): 306-326. https://doi.org/10.25255/jss.2019.8.2.306.326.

Office of the Director, Operational Test & Evaluation. FY 2022 Annual Report. Washington DC: January 2023. https://www.dote.osd.mil/Annual-Reports/2022-Annual-Report/.

Office of the National Cyber Director. National Cyber Workforce and Education Strategy: Unleashing America’s Cyber Talent. Washington, D.C.: Office of the National Cyber Director, July 31, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.

Orlikowski, Wanda J. and Jack J. Baroudi. “The information systems profession: Myth or reality?” NYU Working Paper No. IS-88-32. https://ssrn.com/abstract=1289714.

Pandita, Deepika and Sampurna Ray. “Talent management and employee engagement–a meta-analysis of their impact on talent retention.” *Industrial and Commercial Training* 50, no. 4 (April 2018): 185-199. https://doi.org/10.1108/ICT-09-2017-0073.

Partnership for Public Service. Cyber In-Security II: Closing the Federal Cyber Talent Gap. Washington, D.C.: April 2015. https://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In Security_II__Closing_the_Federal_Talent_Gap-2015.04.13.pdf.

Peechapol, Chattavut, Jaitip Na-Songkhla, Siridej Sujiva, and Arthorn Luangsodsai. "An Exploration of Factors Influencing Self-Efficacy in Online Learning: A Systematic Review." *International Journal of Emerging Technologies in Learning* 13, no. 09 (September 29, 2018): 64-86, https://doi.org/10.3991/ijet.v13i09.8351.

Pink, Daniel H. *Drive: The Surprising Truth About What Motivates Us*. New York: Riverhead Books, 2011.

Rasa, Smaliukienė, Bekesiene Svajone, Kanapeckaitė Rosita, Navickienė Olga, Meidutė-Kavaliauskienė Ieva, and Vaičaitienė Ramutė. "Meaning in Military Service Among Reservists: Measuring the Effect of Prosocial Motivation in a Moderated-Mediation Model." *Frontiers in Psychology* 14 (February 9, 2023): https://doi.org/10.3389/fpsyg.2023.1082685.

Rock, David and Heidi Grant. "Why Diverse Teams are Smarter." *Harvard Business Review*. Last modified November 4, 2016. https://hbr.org/2016/11/why-diverse-teams-are-smarter.

Ronald Reagan Presidential Foundation. "2023 Reagan National Defense Survey." Accessed on December 4, 2023. https://www.reaganfoundation.org/reagan-institute/centers/peace-through-strength/reagan-national-defense-survey/.

Rose, Gideon. "The Fourth Founding: The United States and the Liberal Order." *Foreign Affairs* 98, no. 1 (January/February 2019): 10-21. https://www.foreignaffairs.com/articles/united-states/2018-12-11/fourth-founding.

Sanders, Ronald P. "The War for Cyber Talent: Can the US Win It?" *The Great Power Competition* 3 (September 16, 2023): 293-318. Springer, Cham. https://doi.org/10.1007/978-3-031-04586-8_15.

Santhanam, Radhika, Sharath Sasidharan and Jane Webster. "Using Self-Regulatory Learning to Enhance E-Learning-Based Information Technology Training." *Information Systems Research* 19, no. 1 (March 2008): 26-47. https://www.jstor.org/stable/23015420.

Schwab, Klaus. "The Fourth Industrial Revolution: What it Means, How to Respond." *World Economic Forum*, January 14, 2016. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

Schunk, Dale H., and Maria K. DiBenedetto. "Self-Efficacy and Human Motivation." *Advances in Motivation Science*, 153–79, 2021. https://doi.org/10.1016/bs.adms.2020.10.001.

Stewart, John, Rachel Henderson, Lynnette Michaluk, Jessica Deshler, Edgar Fuller, and Karen E. Rambo-Hernandez. "Using the Social Cognitive Theory Framework to Chart Gender Differences in the Developmental Trajectory of STEM Self-Efficacy in Science and Engineering Students." *Journal of Science Education and Technology* 29, no. 6 (August 18, 2020): 758–73. https://doi.org/10.1007/s10956-020-09853-5.

Sypniewska, Barbara, Małgorzata Baran and Monika Kłos. "Work engagement and employee satisfaction in the practice of sustainable human resource management." *International Entrepreneurship and Management Journal* 19 (March 2023): 1069-1100. https://doi.org/10.1007/s11365-023-00834-9.

Towhidi, Gelareh and Jeannie Pridmore. "Increasing Cybersecurity Interest and Self-Efficacy through Experiential Labs." *Issues in Information Systems* 23, no. 2 (January 1, 2022): 119-131. https://doi.org/10.48009/2_iis_2022_110.

Triplett, Will. "Addressing Cybersecurity Challenges in Education." *ResearchGate* (January 1, 2023). https://doi.org/10.52889/ijses.v3i1.132.

Ullah, Saif, Atif Khan Jadoon, Sana Amjad, Wasif Ali and Basharat Raza. "Linking Self-efficacy and Organizational Citizenship Behavior: A Moderated Mediation Model." *International Journal of Organizational Leadership* 10 (2021): 233-247, https://ijol.cikd.ca/article_60576_0b8e54e0c1b08085e3b514ce261c66b3.pdf.

U.S. Army Cyber Command. U.S. Army Cyber Command (ARCYBER) Retention Study (ARS). Unpublished survey brief for Lieutenant General Stephen G. Fogarty Commanding General, U.S. Army Cyber Command and Mr. Ronald W. Pontius, SES Deputy to the Commanding General, U.S. Army Cyber Command, last modified 9 December 2019. Portable Document Format file.

U.S. Cyber Command. Retention in Cyber Command. Unpublished survey findings, last modified 2021. Portable Document Format file.

U.S. Army Reserve. "Ambassador Program U.S. Army Reserve." Accessed October 6, 2023. https://www.usar.army.mil/AmbassadorProgram/.

U.S. Army Reserve. "Cyber Private Public Partnership." Accessed October 6, 2023. https://www.usar.army.mil/Featured/Private-Public-Partnership/Cyber-P3/.

U.S. Congress. House. Committee on Armed Services. National Defense Authorization Act for Fiscal Year 2023 Report of the Committee on Armed Services, House of Representatives on H.R. 7900 Together with Dissenting Views (Including Cost Estimate of the Congressional Budget Office). Washington: U.S. Government Publishing Office, 2023. https://www.congress.gov/bill/117th-congress/house-bill/7900/text.

U.S. Department of Defense. 2022 National Defense Strategy of the United States of America: Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review. Washington, D.C.: Department of Defense, 27 October 2022. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

U.S. Department of Defense. 2023 Cyber Strategy of the Department of Defense Summary. Washington, D.C.: Department of Defense, 12 September 2023. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

U.S. Department of Defense. DoD Cyber Workforce Strategy 2023-2027. Washington, D.C.: Department of Defense, 1 March 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/CWF-Strategy.pdf.

U.S. Department of Defense. DoD Cyber Workforce Strategy Implementation Plan 2023-2027. Washington, D.C.: Department of Defense, 13 July 2023. https://media.defense.gov/2023/Aug/03/2003274088/-1/-1/1/2023-2027-DOD-CYBER-WORKFORCE-STRATEGY-IMPLEMENTATION-PLAN.PDF.

U.S. Department of Defense. DoD Manual 8140.03 Cyberspace Workforce Qualification and Management Program. Washington, D.C.: Department of Defense, 15 February 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf.

U.S. Department of Homeland Security. National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience. Washington, D.C.: December 2013. https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf.

U.S. Government Accountability Office. Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements. Washington, D.C.: February 2020. https://www.gao.gov/products/gao-20-299.

U.S. Government Accountability Office. Report to Congressional Committees: High Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas. Washington, D.C. April 20, 2023. https://files.gao.gov/reports/GAO-23-106203/index.html#appendix22.

U.S. Government Accountability Office. Report to Congressional Committees: Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking. Washington, D.C.: December 2022. https://www.gao.gov/assets/gao-23-105423.pdf.

U.S. Library of Congress. Congressional Research Service. FY2023 NDAA: Cyber Personnel Policies, by Kristy N. Kamarck and Catherine A. Theohary. CRS Report R47270. Washington, DC: Office of Congressional Information and Publishing, March 6, 2023. https://crsreports.congress.gov/product/pdf/R/R47270.

U.S. President. Administration Cybersecurity Priorities for the FY 2025 Budget. Washington, D.C.: Executive Office of the President, June 27, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-18-Administration-Cybersecurity-Priorities-for-the-FY-2025-Budget-s.pdf.

U.S. President. National Security Strategy. Washington, D.C.: Government Printing Office, October 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

U.S. President. National Cybersecurity Strategy. Washington, D.C.: Government Printing Office, March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

U.S. President. National Cybersecurity Strategy Implementation Plan. Washington, D.C.: Government Printing Office, July 2023. https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

Verlinden, Neelie. "Organizational Citizenship Behavior: Benefits and 3 Best Practices." Academy to Innovate HR, accessed November 20, 2023, https://www.aihr.com/blog/organizational-citizenship-behavior/.

Winters, Desiree Marie. "Using Playable Case Studies to Influence Teen Girls' Self-Efficacy and Interest in Cybersecurity." *BYU Scholars Archive* (August 1, 2019), https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=8558&context=etd.

Workhuman. "Building the Future of Work With a Human-Centric Approach." Last modified July 6, 2022. https://www.workhuman.com/resources/reports-guides/building-the-future-of-work-with-a-human-centric-approach/.

Yaakobi, Erez and Jacob Weisberg. "Organizational Citizenship Behavior Predicts Quality, Creativity, and Efficiency Performance: The Roles of Occupational and Collective Efficacies." *Frontiers in Psychology*, no. 11 (April 2020): 1-18. https://www.frontiersin.org/articles/10.3389/fpsyg.2020.00758/full.

Yassanye, Diana M., Andrea P. Anason and Drue H. Barrett. “Mitigating Ethical Risks in Public-Private Partnerships in Public Health.” *Journal of Public Health Management and Practice* 27, no. 4 (July/August 2021): E177-E182. https://journals.lww.com/jphmp/abstract/2021/07000/mitigating_ethical_risks_in_public_private.21.aspx.

Vita

Lieutenant Colonel Jeremiah C. Hood is a career Signal Officer in the U.S. Army Reserve. He graduated from the University of Tennessee, Knoxville with a Bachelor of Science degree in Hotel and Restaurant Administration and is also a graduate of the U.S. Army Command and General Staff College. Lieutenant Colonel Hood also completed a Master of Science degree in Human Resource Development from the University of Tennessee, Knoxville.

Endnotes

[1] Eric P. Hillner, "The Third Offset Strategy and the Army Modernization Priorities," *Center for Army Lesson's Learned*, (May 2019), https://usacac.army.mil/sites/default/files/publications/17855.pdf, 3.

[2] "Cybersecurity Supply/Demand Heat Map," CyberSeek, accessed October 2, 2023, https://www.cyberseek.org/heatmap.html.

[3] Klaus Schwab, "The Fourth Industrial Revolution: What it Means, How to Respond." *World Economic Forum* (January 14, 2016), https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

[4] U.S. Department of Defense, DoD Cyber Workforce Strategy 2023-2027 (Washington, D.C.: Department of Defense, 1 March 2023), 6.

[5] Office of the Director, Operational Test & Evaluation, FY 2022 Annual Report (Washington DC: January 2023), iii.

[6] Chad Bates et al., "Understanding—and Fixing—The Army's Challenge in Keeping Cyber Talent," *Modern War Institute at West Point*, (May 17, 2022), https://mwi.westpoint.edu/understanding-and-fixing-the-armys-challenge-in-keeping-cyber-talent/.

[7] U.S. Department of Defense, DoD Cyber Workforce Strategy Implementation Plan 2023-2027, 15.

[8] U.S. Government Accountability Office, Report to Congressional Committees: High Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas (Washington, D.C. April 20, 2023), https://files.gao.gov/reports/GAO-23-106203/index.html#appendix22.

[9] Defense Business Board, FY23 Assessment of the Department of Defense: Building a Civilian Talent Pipeline (Washington, D.C.: March 2023), 3.

[10] Defense Business Board, FY23 Assessment of the Department of Defense: Building a Civilian Talent Pipeline, 12-14

[11] Defense Business Board, FY23 Assessment of the Department of Defense: Building a Civilian Talent Pipeline, 3-8.

[12] Defense Business Board, FY23 Assessment of the Department of Defense: Building a Civilian Talent Pipeline, 14.

[13] Robert Gilpin, *War and Change in World Politics*, (Cambridge: Cambridge University Press, 1981), 197.

[14] Gideon Rose, "The Fourth Founding: The United States and the Liberal Order," *Foreign Affairs* 98, no. 1 (January/February 2019): 15, https://www.foreignaffairs.com/articles/united-states/2018-12-11/fourth-founding.

[15] Chad Bates et al., "Understanding—and Fixing—The Army's Challenge in Keeping Cyber Talent."

[16] U.S. President, National Security Strategy (Washington, D.C.: Government Printing Office, October 2022), 34.

[17] U.S. President, National Security Strategy, 23.

[18] U.S. President, National Security Strategy, 46.

[19] U.S. President, National Cybersecurity Strategy Implementation Plan (Washington, D.C.: Government Printing Office, July 2023), 14.

[20] Chairman Joint Chiefs of Staff, Joint Operating Environment 2035 (Washington, D.C.: Department of Defense, 14 July 2016), 15-20.

[21] Chairman Joint Chiefs of Staff, Joint Concept for Competing (Washington, D.C.: Department of Defense, 10 February 2023), iv.

[22] U.S. President, National Cybersecurity Strategy (Washington, D.C.: Government Printing Office, March 2023), 1.

[23] Ronald P. Sanders, "The War for Cyber Talent: Can the US Win It?" The Great Power Competition 3 (September 16, 2023): 293-294, https://doi.org/10.1007/978-3-031-04586-8_15.

[24] Office of the National Cyber Director, National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent (Washington, D.C.: Office of the National Cyber Director, July 31, 2023), 1.

[25] U.S. Department of Defense, 2022 National Defense Strategy of the United States of America: Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review (Washington, D.C.: Department of Defense, 27 October 2022), 20.

[26] U.S. Department of Defense, 2023 Cyber Strategy of the Department of Defense Summary (Washington, D.C.: Department of Defense, 12 September 2023), 13.

[27] U.S. Department of Defense, 2022 National Defense Strategy of the United States of America: Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review, 20.

[28] Defense Business Board, Public-Private Collaboration in the Department of Defense (Washington, D.C.: July 2012), 1

[29] Defense Business Board, Public-Private Collaboration in the Department of Defense, 11.

[30] Defense Business Board, Public-Private Collaboration in the Department of Defense, 28.

[31] U.S. Department of Homeland Security, National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience (Washington, D.C.: December 2013), 1-2.

[32] National Research Council, Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision Making (Washington D.C.: National Academies Press, 2013), 23.

[33] National Research Council, Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision Making, 26-27.

[34] National Academy of Public Administration, A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation (Washington, D.C.: January 2022), 1-2.

[35] U.S. Government Accountability Office, Report to Congressional Committees: Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking (Washington, D.C.: December 2022), 10.

[36] U.S. Government Accountability Office, Report to Congressional Committees: Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking, 2.

[37] U.S. Government Accountability Office, Report to Congressional Committees: Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking, 31-33.

[38] Chad Bates, et al., "Leveraging Talent to Dominate in Cyber War—An Army Perspective," *The Great Power Competition* 3 (16 September 2022): 319-321, https://doi.org/10.1007/978-3-031-04586-8_16.

[39] U.S. Army Cyber Command, U.S. Army Cyber Command (ARCYBER) Retention Study (ARS), Unpublished survey brief for Lieutenant General Stephen G. Fogarty Commanding General, U.S. Army Cyber Command and Mr. Ronald W. Pontius, SES Deputy to the Commanding General, U.S. Army Cyber Command, last modified 9 December 2019.

[40] U.S. Cyber Command, Retention in Cyber Command, Unpublished survey findings, last modified 2021.

[41] The United States Army War College, Center for Strategic Leadership, provided written approval to utilize the U.S. Army Cyber Command (ARCYBER) Retention Study (ARS) and U.S. Cyber

Command. Retention in Cyber Command Survey for academic research and use. A copy is provided in Appendix 1.

[42] Blue Star Families, "Military Family Lifestyle Survey: 2022 Comprehensive Report," 10, https://bluestarfam.org/wp-content/uploads/2023/03/BSF_MFLS_Spring23_Full_Report_Digital.pdf.

[43] Joseph B Fuller, et al. "Hidden Workers: Untapped Talent," Published by Harvard Business School Project on Managing the Future of Work and Accenture, September 2021, https://www.hbs.edu/managing-the-future-of-work/Documents/research/hiddenworkers09032021.pdf.

[44] Elisa B. Kania, "In Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovate," *The Strategy Bridge* (August 27, 2019), https://thestrategybridge.org/the-bridge/2019/8/27/in-military-civil-fusion-china-is-learning-lessons-from-the-united-states-and-starting-to-innovate.

[45] U.S. President, Administration Cybersecurity Priorities for the FY 2025 Budget (Washington, D.C.: Executive Office of the President, June 27, 2023), 2-4.

[46] Albert Bandura, et al., "Self-Efficacy: The Exercise of Control," *Journal of Cognitive Psychotherapy* 13, no. 2 (January 1, 1999): 158, https://doi.org/10.1891/0889-8391.13.2.158.

[47] Marilyn E. Gist et al., "Self-efficacy: A theoretical analysis of its determinants and malleability," *Academy of Management Review* 17, no. 2 (1992): 190. https://www.jstor.org/stable/258770?seq=8.

[48] Marilyn E. Gist et al., "Self-efficacy: A theoretical analysis of its determinants and malleability," *Academy of Management Review* 17, no. 2 (1992): 203. https://www.jstor.org/stable/258770?seq=8.

[49] Albert Bandura, et el., "Self-Efficacy Beliefs as Shapers of Children's Aspirations and Career Trajectories," *Child Development* 72, no. 1 (January-February 2001): 187, https://www.jstor.org/stable/1132479.

[50] Gelareh Towhidi et al., "Increasing Cybersecurity Interest and Self-Efficacy through Experiential Labs," *Issues in Information Systems* 23, no. 2 (January 1, 2022): 121, https://doi.org/10.48009/2_iis_2022_110.

[51] Daniel H. Pink, *Drive: The Surprising Truth About What Motivates Us* (New York: Riverhead Books, 2011), 12.

[52] Daniel H. Pink, *Drive: The Surprising Truth About What Motivates Us* (New York: Riverhead Books, 2011), 78-85.

[53] Dale H. Schunk et al., "Self-Efficacy and Human Motivation," *Advances in Motivation Science*, 2021, 153–79, https://doi.org/10.1016/bs.adms.2020.10.001.

[54] Masooda Bashir, et al., "Profiling Cybersecurity Competition Participants: Self-Efficacy, Decision-Making and Interests Predict Effectiveness of Competitions as a Recruitment Tool," *Computers & Security* 65 (March 2017): 157, https://doi.org/10.1016/j.cose.2016.10.007.

[55] John Stewart et al., "Using the Social Cognitive Theory Framework to Chart Gender Differences in the Developmental Trajectory of STEM Self-Efficacy in Science and Engineering Students," *Journal of Science Education and Technology* 29, no. 6 (August 18, 2020): 762, https://doi.org/10.1007/s10956-020-09853-5.

[56] Chattavut Peechapol et al., "An Exploration of Factors Influencing Self-Efficacy in Online Learning: A Systematic Review," *International Journal of Emerging Technologies in Learning* 13, no. 09 (September 29, 2018): 64, https://doi.org/10.3991/ijet.v13i09.8351.

[57] Will Triplett, "Addressing Cybersecurity Challenges in Education," *ResearchGate*, January 1, 2023, https://doi.org/10.52889/ijses.v3i1.132.

[58] Tianying Chen et al., "Self-Efficacy-Based Game Design to Encourage Security Behavior Online," *Proceedings of CHI Conference on Human Factors in Computing Systems Extended Abstracts*, May 2, 2019, https://doi.org/10.1145/3290607.3312935.

[59] Elizabeth Bonsignore et al., "The Playable Case Study Authoring and Simulation Platform," *ResearchGate*, June 7, 2022, https://www.researchgate.net/publication/360936147_The_Playable_Case_Study_Authoring_and_Simulation_Platform.

[60] Justin Scott Giboney et al., "Increasing Cybersecurity Career Interest through Playable Case Studies," *TechTrends*, February 8, 2021, https://doi.org/10.1007/s11528-021-00585-w.

[61] Desiree Marie Winters, "Using Playable Case Studies to Influence Teen Girls' Self-Efficacy and Interest in Cybersecurity," *BYU Scholars Archive* (January 1, 2019): 2, https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=8558&context=etd.

[62] Pushpa Hongal et al., "A Study of Talent Management and Its Impact on Performance of Organizations," *International Journal of Engineering and Management Research* 10, no. 1 (February 2020): 68-70, https://doi.org/10.31033/ijemr.10.1.12.

[63] Foteini Kravariti et al., "Talent management: A Critical Literature Review and Research Agenda for Public Sector Human Resource Management." *Public Management Review* 22, no. 1 (July 2019): 75–95, https://doi.org/10.1080/14719037.2019.1638439.

[64] Bader Obeidat et al., "Reviewing the mediating role of work/life balance and motivational drivers of employee engagement on the relationship between talent management and organization Performance," *Journal of Social Sciences* 8, no. 2 (April 2019): 310, https://doi.org/10.25255/jss.2019.8.2.306.326.

[65] Aerni Isa et al.,"Talent management practices, perceived organizational support and employee retention: Evidence from government-linked companies," Global Business and Management Research 10, no. 3 (December 2018): 692, https://www.researchgate.net/publication/330037565_Talent_Management_Practices_Perceived_Organizational_Support_and_Employee_Retention_Evidence_From_Malaysian_Government-Linked_Companies.

[66] Benjamin Balbuena Aguenza et al., "Motivational Factors of Employee Retention and Engagement in Organizations," *International Journal of Advances in Management and Economics* 1, no. 6 (April 2018): 91, https://www.managementjournal.info/index.php/IJAME/article/view/233.

[67] Mohammad Ali et al., "Role of Talent Development on Talent Engagement and Self-Efficacy: A Structural Model," *Journal of Social Economics Research* 7, no. 2 (October 2020): 120, https://www.researchgate.net/publication/345083695.

[68] Mohammad Ali et al., "Role of Talent Development on Talent Engagement and Self-Efficacy: A Structural Model," *Journal of Social Economics Research* 7, no. 2 (October 2020): 119, https://www.researchgate.net/publication/345083695.

[69] Molly L. Delaney et al., "Breaking engagement apart: The role of intrinsic and extrinsic motivation in engagement strategies," *Industrial and Organizational Psychology* 10, no. 1 (March 2017): 131-132, https://doi.org/10.1017/iop.2017.2.

[70] Gareth R. Jones, "Socialization tactics, self-efficacy, and newcomers' adjustments to Organizations," *Academy of Management Journal* 29, no. 2 (June 1986): 274-276, https://www.jstor.org/stable/256188.

[71] Mohammad Ali et al., "Role of Talent Development on Talent Engagement and Self-Efficacy: A Structural Model," *Journal of Social Economics Research* 7, no. 2 (October 2020): 120-121, https://www.researchgate.net/publication/345083695.

[72] Deepika Pandita et al., "Talent management and employee engagement–a meta-analysis of their impact on talent retention," Industrial and Commercial Training 50, no. 4 (April 2018): 188, https://doi.org/10.1108/ICT-09-2017-0073.

[73] Jian Ming et al., "Self-Efficacy in Cybersecurity Tasks and Its Relationship with Cybersecurity Competition and Work-Related Outcomes," 2016 USENIX Workshop on Advances in Security Education. https://www.usenix.org/sites/default/files/conference/protected-files/ase16_slides_wee.pdf.

[74] Radhika Santhanam et al., "Using Self-Regulatory Learning to Enhance E-Learning-Based Information Technology Training," *Information Systems Research* 19, no. 1 (March 2008): 34-39, https://www.jstor.org/stable/23015420.

[75] Sharon K. Gibson, "Social Learning (Cognitive) Theory and Implications for Human Resource Development." Advances in Developing Human Resources 6, no.2 (May 2004): 195-197, https://doi.org/10.1177/1523422304263429.

[76] Neeraj Kumar Jaiswal et al., "The influence of servant leadership, trust in leader and thriving on employee creativity," *Leadership & Organization Development* Journal 38, no. 1 (January 2017): 5, https://doi.org/10.1108/LODJ-02-2015-0017.

[77] Weiling Ke et al., "Organizational culture and leadership in ERP

Implementation," *Decision Support Systems* 45, no. 2 (May 2008): 211. https://doi.org/10.1016/j.dss.2007.02.002.

[78] William A. Lucas et al., "Industry Placement, Authentic Experience and the Development of Venturing and Technology Self-Efficacy," *Technovation* 29, no. 11 (November 2009): 740-744, https://doi.org/10.1016/j.technovation.2009.06.002.

[79] Smaliukienė Rasa et al., "Meaning in Military Service Among Reservists: Measuring the Effect of Prosocial Motivation in a Moderated-Mediation Model," *Frontiers in Psychology* 14 (February 9, 2023), https://doi.org/10.3389/fpsyg.2023.1082685.

[80] Naomi Buckwalter, Interview with Jen Stone: The Myth of the Cybersecurity Workforce Shortage, *Security Metrics*, Podcast 27, Accessed August 27, 2023. https://www.securitymetrics.com/learn/myth-of-the-cybersecurity-workforce-shortage.

[81] Saif Ullah et al., "Linking Self-efficacy and Organizational Citizenship Behavior: A Moderated Mediation Model," *International Journal of Organizational Leadership* 10 (2021): 233-234, https://ijol.cikd.ca/article_60576_0b8e54e0c1b08085e3b514ce261c66b3.pdf.

[82] Adam M. Grant et al., "Good soldiers and good actors: Pro-social and impression management motives as interactive predictors of affiliative citizenship behaviors," *Journal of Applied Psychology* 94, no. 4 (2009): 901. https://doi.org/10.1037/a0013770.

[83] Neelie Verlinden, "Organizational Citizenship Behavior: Benefits and 3 Best Practices," Academy to Innovate HR, Accessed November 20, 2023, https://www.aihr.com/blog/organizational-citizenship-behavior/.

[84] Saif Ullah et al., "Linking Self-efficacy and Organizational Citizenship Behavior: A Moderated Mediation Model," *International Journal of Organizational Leadership* 10 (2021): 236, https://ijol.cikd.ca/article_60576_0b8e54e0c1b08085e3b514ce261c66b3.pdf.

[85] Saif Ullah et al., "Linking Self-efficacy and Organizational Citizenship Behavior: A Moderated Mediation Model," *International Journal of Organizational Leadership* 10 (2021): 244, https://ijol.cikd.ca/article_60576_0b8e54e0c1b08085e3b514ce261c66b3.pdf.

[86] Barbara Sypniewska et al., "Work engagement and employee satisfaction in the practice of sustainable human resource management," *International Entrepreneurship and Management Journal* 19 (March 2023): 1083-1086, https://doi.org/10.1007/s11365-023-00834-9.

[87] Alberta June Shelinbarger Ellett, "Human Caring, Self-Efficacy Beliefs, and Professional Organizational Culture Correlates of Employee Retention," (2000), LSU Historical Dissertations and Theses, 7263, https://repository.lsu.edu/gradschool_disstheses/7263, 26-27.

[88] U.S. Department of Defense, DoD Cyber Workforce Strategy 2023-2027, 11.

[89] U.S. Department of Defense. DoD Cyber Workforce Strategy Implementation Plan 2023-2027 (Washington, D.C.: Department of Defense, 13 July 2023), 3-20.

[90] Mandiant, "M-Trends 2023," accessed November 29, 2023, https://www.mandiant.com/m-trends.

[91] Defense Health Agency, Strategic Plan 2023-2028 (Falls Church, VA: Defense Health Agency, 31 July 2023), 10.

[92] National Research Council, Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision Making (Washington D.C.: National Academies Press, 2013), 15.

[93] Wanda J. Orlikowski et al., "The information systems profession: Myth or reality?," NYU Working Paper No. IS-88-32, https://ssrn.com/abstract=1289714, 4-14.

[94] National Research Council, Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision Making (Washington D.C.: National Academies Press, 2013), 15.

[95] National Research Council, Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision Making (Washington D.C.: National Academies Press, 2013), 16.

[96] U.S. Department of Defense. DoD Manual 8140.03 Cyberspace Workforce Qualification and Management Program (Washington, D.C.: Department of Defense, 15 February 2023).

[97] National Research Council, Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision Making (Washington D.C.: National Academies Press, 2013), 1-2.

[98] Erez Yaakobi et al., "Organizational Citizenship Behavior Predicts Quality, Creativity, and Efficiency Performance: The Roles of Occupational and Collective Efficacies," *Frontiers in Psychology*, no. 11 (April 2020): 2, https://www.frontiersin.org/articles/10.3389/fpsyg.2020.00758/full.

[99] Muhammad Arshad et al., "Impact of Prosocial Motivation on Organizational Citizenship Behavior and Organizational Commitment: The Mediating Role of Managerial Support," *European Journal of Investigation in Health, Psychology and Education*, no. 11 (May 2021): 440, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8314358/.

[100] U.S. President, National Cybersecurity Strategy, 4.

[101] U.S. President, National Cybersecurity Strategy, 27.

[102] U.S. President, National Cybersecurity Strategy, 35.

[103] U.S. Department of Defense, DoD Cyber Workforce Strategy 2023-2027, 10.

[104] Paul M. Nakasone, "An Interview with Paul M. Nakasone," *Joint Force Quarterly* 92 (2019): 6, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf.

[105] International Information System Security Certification Consortium, "Cyber Workforce Study 2019," accessed November 27, 2023, https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2019.pdf?rev=52055d08ca644293bd7497725bb7fcb4.

[106] International Information System Security Certification Consortium, "Cyber Workforce Study 2019," accessed November 27, 2023, https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2019.pdf?rev=52055d08ca644293bd7497725bb7fcb4.

[107] International Information System Security Certification Consortium, "Cyber Workforce Study 2019," accessed November 27, 2023, https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2019.pdf?rev=52055d08ca644293bd7497725bb7fcb4.

[108] Partnership for Public Service, Cyber In-Security II: Closing the Federal Cyber Talent Gap. Washington, D.C.: April 2015, https://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In-Security_II__Closing_the_Federal_Talent_Gap-2015.04.13.pdf.

[109] Ronald Reagan Presidential Foundation, "2023 Reagan National Defense Survey," accessed on December 4, 2023, https://www.reaganfoundation.org/reagan-institute/centers/peace-through-strength/reagan-national-defense-survey/.

[110] U.S. Government Accountability Office. Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements. Washington, D.C.: February 2020, https://www.gao.gov/products/gao-20-299.

[111] Sun Young Kim et al., "Employee Empowerment and Turnover Intention in the U.S. Federal Bureaucracy," *The American Review of Public Administration* 41, no.1 (January 2017), 18-20, https://doi.org/10.1177/0275074015583712.

[112] Katharina Harsch et al., "Dynamic talent management capabilities and organizational agility: A qualitative exploration," *Human Resource Management* 59, no. 5:, 43-61. https://doi.org/10.1002/hrm.21972

[113] Workhuman, "Building the Future of Work With a Human-Centric Approach," Last modified July 6, 2022. https://www.workhuman.com/resources/reports-guides/building-the-future-of-work-with-a-human-centric-approach/.

[114] Partnership for Public Service, Cyber In-Security II: Closing the Federal Cyber Talent Gap. Washington, D.C.: April 2015, https://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In-Security_II__Closing_the_Federal_Talent_Gap-2015.04.13.pdf.

[115] David Rock et al., "Why Diverse Teams are Smarter," *Harvard Business Review*. Last modified November 4, 2016, https://hbr.org/2016/11/why-diverse-teams-are-smarter.

[116] Partnership for Public Service, Cyber In-Security II: Closing the Federal Cyber Talent Gap. Washington, D.C.: April 2015, https://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In-Security_II__Closing_the_Federal_Talent_Gap-2015.04.13.pdf.

[117] Kim C. Brimhall et al., "Do work-life inclusion policies predict inclusion climate? Exploring the mediating role of work-life conflict and enrichment," Human Resource Management 56, no. 4 (April 2017): 692-685,

https://doi.org/10.1002/hrm.21972.

[118] Katharina Harsch et al., "Dynamic talent management capabilities and organizational agility: A qualitative exploration," *Human Resource Management* 59, no. 5:, 54-58, https://doi.org/10.1002/hrm.21972

[119] Albert Bandura, "Self-efficacy: Toward a unifying theory of behavioral change," *Advances in Behavior Research and Therapy* 1, no. 4 (1978): 196, https://doi.org/10.1016/0146-6402(78)90002-4.

[120] Katharina Harsch et al., "Dynamic talent management capabilities and organizational agility: A qualitative exploration," *Human Resource Management* 59, no. 5: 58-60, https://doi.org/10.1002/hrm.21972

[121] Fred C. Lunenburg, "Self-Efficacy in the Workplace: Implications for Motivation and Performance," *International Journal of Management, Business, and Administration* 14, no. 1 (January 2011): 3, http://www.nationalforum.com/Electronic%20Journal%20Volumes/Lunenburg%2C%20Fred%20C.%20SelfEfficacy%20in%20the%20Workplace%20IJMBA%20V14%20N1%202011.pdf.

[122] National Security Council, "Sharing Information with the Private Sector," Accessed November 16, 2023, https://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionV.html.

[123] National Security Council, "Sharing Information with the Private Sector," Accessed November 16, 2023, https://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionV.html.

[124] Diana M. Yassanye et al., "Mitigating Ethical Risks in Public-Private Partnerships in Public Health." *Journal of Public Health Management and Practice* 27, no. 4 (July/August 2021): E177-E178, https://journals.lww.com/jphmp/abstract/2021/07000/mitigating_ethical_risks_in_public_private.21.aspx.

[125] Robert W. Lent et al., ""Toward a Unifying Social Cognitive Theory of Career and Academic Interest, Choice, and Performance," *Journal of Vocational Behavior* 45, no. 1 (August 1994): 79-80, https://doi.org/10.1006/jvbe.1994.1027.

[126] Neelie Verlinden, "Organizational Citizenship Behavior: Benefits and 3 Best Practices," Academy to Innovate HR, Accessed November 20, 2023, https://www.aihr.com/blog/organizational-citizenship-behavior/.

[127] Smaliukienė Rasa et al., "Meaning in Military Service Among Reservists: Measuring the Effect of Prosocial Motivation in a Moderated-Mediation Model," Frontiers in Psychology 14 (February 9, 2023), https://doi.org/10.3389/fpsyg.2023.1082685.

[128] Kendra Cherry, "Self Efficacy and Why Believing in Yourself Matters," Updated on February 27, 2023, https://www.verywellmind.com/what-is-self-efficacy-2795954.

[129] Mohammad Ali et al., "Role of Talent Development on Talent Engagement and Self-Efficacy: A Structural Model," Journal of Social Economics Research 7, no. 2 (October 2020): 118, https://www.researchgate.net/publication/345083695.

[130] Mohammad Ali et al., "Role of Talent Development on Talent Engagement and Self-Efficacy: A Structural Model," Journal of Social Economics Research 7, no. 2 (October 2020): 119, https://www.researchgate.net/publication/345083695.