GROWING A STRONGER FEDERAL CYBER WORKFORCE

CSC White Paper #3

UNITED STATES OF AMERICA
CYBERSPACE
SOLARIUM
COMMISSION

CO-CHAIRMEN

Senator Angus King (I-Maine)

Representative Mike Gallagher (R-Wisconsin)

SEPTEMBER 2020

EXECUTIVE SUMMARY

The Cyberspace Solarium Commission (CSC) was established by the FY2019 National Defense Authorization Act (NDAA) and tasked to identify a strategic approach to protect the United States against attacks of significant consequence in cyberspace. The Commission has recommended numerous changes to policy and legislation that impact virtually every element of the cybersecurity ecosystem. While the Commission's recommendations address a broad range of issues, the need for a skilled cyber workforce is a recurring theme that runs throughout many of those recommendations. As the Commission's co-chairs, Senator Angus King and Representative Mike Gallagher, have observed, "without talented cyber professionals working the keyboard, all the cutting-edge technology in the world cannot protect the United States in cyberspace. If we do not take action now to ensure that our talented and experienced workforce continues to grow, we are leaving our country vulnerable to future cyber attacks."[1]

Currently more than one in three public-sector cyber jobs sits open.[2] Filling these roles has been a persistent and intractable problem over the past decade, in large part due to a lack of coordination and leadership. A 2009 assessment of the federal cybersecurity workforce called for "a government-wide strategic blueprint to acquire, train and retain the cybersecurity talent the federal government needs,"[3] yet we continue to face the same problem today. ***In the context of this pervasive challenge, the fundamental purpose of this paper is to outline the elements required for a coherent strategy that enables substantive and coordinated investment in cyber workforce development and calls for a sustained investment in that strategy.*** Without such investment, the cyber workforce will not grow quickly enough to meet critical national security requirements, in which case decision makers—whether in department and agency leadership or in Congress—can plan to continue debating the distribution of insufficient resources and nibbling at the edges of this problem for another decade.

This paper lays out five elements to guide development of a federal cyber workforce strategy:

- ***Organize:*** Federal departments and agencies must have flexible tools for organizing and managing their workforce that can adapt to each organization's individual mission while also providing coherence across the entirety of the federal government. To appropriately organize the federal cyber workforce, the CSC recommends **properly identifying and utilizing cyber-specific occupational classifications** to allow more tailored workforce policies, **building a federal cyber service** to provide clear and agile hiring authorities and other personnel management tools, and **establishing coordination structures** to provide clear leadership for federal workforce development efforts.

- ***Recruit:*** Federal leaders must focus on the programs that make public service an attractive prospect to talented individuals. In many ways, the federal government's greatest tool for recruitment is the mission and unique learning opportunities inherent in federal work. To capitalize on these advantages, the government should invest in existing programs such as **CyberCorps: Scholarship for Service** and **the Centers of Academic Excellence**, while also working to mitigate recruitment barriers that stem from the **personnel security clearance process**.

- ***Develop:*** The federal government, like all cyber employers, cannot expect every new employee to have hands-on experience, a four-year degree, and a list of industry certifications. Rather, the federal government will be stronger if it draws from a broad array of educational backgrounds and creates opportunities for employees to gain knowledge and experience as they work. This effort will call for many innovative approaches, among which the Commission particularly recommends **apprenticeship programs** and **upskilling opportunities** to support cyber employee development.

- ***Retain:*** Federal leaders should take a nuanced view of retention, recognizing that enabling talent to move flexibly between the public and private sectors enables a stronger cyber workforce overall. However, federal employers can take steps to encourage their employees to increase the time they spend in public service. Improving **pay flexibility** is a major consideration, but continuing the development of **career pathways** and providing interesting career development opportunities like **rotational and exchange programs** also can be critical. Of particular note, federal employers can increase retention of underrepresented groups through the **removal of inequities** and barriers to advancement in the workplace.

- ***Stimulate growth:*** The federal government cannot simply recruit a larger share of the existing national talent pool. Rather, leaders must take steps to grow the talent pool itself in order to increase the numbers of those available for federal jobs. To promote growth of the talent pool nationwide, the federal government must first **coordinate government efforts** working toward this goal. Executive branch and congressional leaders should also invest in measures to **promote diversity** across the national workforce and **incentivize research** to provide a greater empirical understanding of cyber workforce dynamics. Finally, federal leaders must work to **increase the military cyber workforce**, which has a significant impact on the national cyber workforce because it serves as both a source and an employer of cyber talent.

This five-part structure is intended to lay the groundwork for an effective federal cyber workforce development strategy, leveraging existing efforts whenever possible, while explicitly noting that strengthening the federal cyber workforce also relies on expanding the pool of talent from which it recruits. We want to highlight and emphasize the critical importance of growing the talent pool nationwide, while noting that the recommendations outlined in this paper focus primarily on the federal workforce. This focus is vital, because one of the most effective methods for the federal government to support national workforce development efforts is to lead by example, demonstrating best practices in organizing, recruiting, developing, and retaining its own cyber workforce.

With a cohesive strategy, effective leadership, and sustained investment, the federal government can be a leader in cyber workforce development while also driving toward a stronger cyber workforce nationwide.

Angus King

Senator Angus King (I-Maine)
Co-Chairman
Cyberspace Solarium Commission

Representative Mike Gallagher (R-Wisconsin)
Co-Chairman
Cyberspace Solarium Commission

A. INTRODUCTION

At present, the public sector needs to fill more than 31,000 cybersecurity jobs. Given that the sector currently employs 52,000 cybersecurity professionals, this shortfall means that about one in three public-sector cybersecurity jobs sits unfilled.[4] To address this gap in 2009, experts called for the White House Cybersecurity Coordinator to develop a federal cyber workforce strategy.[5] Eleven years later, the United States federal government does not have a cyber workforce strategy—or even the position of cybersecurity coordinator.[6] This is not to imply that nothing has been done. Many federal laws and policies have attempted to address this gap, including the Cybersecurity Enhancement Act of 2014,[7] the Federal Cybersecurity Workforce Assessment Act of 2015,[8] and the 2019 Executive Order on America's Cybersecurity Workforce.[9] Some of these efforts, such as the codification of the National Initiative for Cybersecurity Education (NICE), are making meaningful changes;[10] however, others did not produce timely change or yielded only piecemeal results, and no effort has been able to make improvements faster than the workforce gap itself was growing.

In addition to large-scale legislation and policy, many individual initiatives to build the federal cybersecurity workforce are under way across the federal government, including long-running programs like CyberCorps: Scholarship for Service and emerging personnel systems like the Department of Defense's Cyber Excepted Service and the Cybersecurity and Infrastructure Security Agency's Cyber Talent Management System; but without clear leadership and a unifying strategy, these disparate efforts are unlikely to advance coherence as a whole.

Most of the workforce development recommendations discussed in this paper—and in the Commission's report more generally—are not new. Like the 2009 report calling for a workforce strategy, many of these recommendations have been circulating for years but remain unimplemented or underutilized because of underresourcing and bureaucratic hurdles in the executive branch and Congress. Because cyber workforce development efforts cross into so many different fields—science, education, commerce, security, intelligence—numerous different congressional committees claim jurisdiction over the issue, which prevents legislation from gaining widespread traction. Meanwhile, many federal departments and agencies have begun to set up their own array of independent programs, dividing resources and ensuring that efforts are disjointed.

As the Cyberspace Solarium Commission has noted throughout its work,[11] protecting the United States in cyberspace requires a whole-of-nation response. This is equally true of enhancing the cyber workforce. With half a million cybersecurity jobs to fill nationwide,[12] stakeholders across the country must consider ways to increase the quantity and diversity of cyber talent in the United States, while also building opportunities for development that strengthen the existing workforce and talent pool. Accordingly, both the CSC recommendations and the government's actions must reach beyond the federal cyber workforce. To improve cybersecurity nationwide, the federal government cannot just focus on recruiting a larger share of available talent, effectively cutting itself a bigger slice of the overall national workforce pie. Rather, the federal government needs to focus on how it can help grow the pie for the whole nation, and thus grow its own slice in the process. The CSC report published in March 2020 provides recommendations on how to improve the national workforce development posture,[13] and many of them are discussed in this paper. However, one of the most effective ways that the federal government can support growth of the national workforce is by serving as a proof of concept of effective cyber workforce planning and policies. Therefore, this paper concentrates predominantly on policies that will help the federal government to serve as an exemplar.

This paper first describes the current state of federal cyber workforce development and then provides the groundwork and basic structure for a federal cyber workforce strategy while identifying specific cyber workforce policies and programs that are required to address the workforce gap. To that end, this paper outlines a framework to **organize**, **recruit**, **develop**, and **retain** the federal civilian cyber workforce. Finally, the paper highlights that an effective federal policy cannot stop at strengthening only its own workforce, because a thriving federal workforce requires a healthy workforce development ecosystem in the private sector, the military, and throughout the whole of the national cyber workforce. To support this larger ecosystem, a federal strategy should align with, and support, broad goals for shaping the national workforce. Accordingly, this section identifies additional steps that can be taken to **stimulate growth** of the cyber workforce nationwide.

B. THE STATE OF FEDERAL CYBER WORKFORCE DEVELOPMENT

What is the federal cyber workforce? While the federal cyber workforce is difficult to define precisely, the multitude of unfilled jobs is a clear problem no matter what definition is used. The NICE Cybersecurity Workforce Framework offers a taxonomy and lexicon for understanding cybersecurity work, outlining 52 work roles and the knowledge, skills, abilities and tasks that characterize them. The Framework helps us better understand the competencies that could reasonably be included in conversations on the federal cyber workforce, and efforts are under way to determine federal cybersecurity workforce needs, using this taxonomy.[14] However, the requirements of cyber workforce development can encompass a much wider range of positions. While those in a first category of positions focus explicitly on security-specific tasks, employees in a second category "need some level of digital and cyber fluency." All workers—a third category—need a basic awareness of cybersecurity.[15] CSC recommendations do touch on the opportunity to strengthen the cyber knowledge and skills of those in the second of these categories: for example, by recommending the incorporation of cybersecurity concepts in career technical education in other fields and industries. This paper, however, focuses primarily on the first category—positions concerned explicitly with security-specific tasks—while recognizing that protecting the United States in cyberspace has implications for digital literacy required in a wide range of jobs, including the disciplines of the law, management, engineering, and basic administration.

Who is responsible for federal cyber workforce development today? Within the federal government, many organizations and systems are responsible for cyber workforce development. But as this paper will go on to discuss, the large number of organizations involved has not translated into overall effectiveness at filling cyber positions. Although many different actors are working to address cyber workforce development, the central problem remains: the federal government is encountering a need for new positions in cyber that is growing far faster than it can recruit, develop, and retain employees to fill them.

NICE—which sits within the National Institute of Standards and Technology (NIST)—not only serves as the home for the NICE Cybersecurity Workforce Framework but is also a focal point for developing a national community of practice around cybersecurity workforce development topics. As the Framework is increasingly used as a standard throughout government, its work shapes much of the federal cyber workforce conversation, with a scope that extends beyond government alone. But there are a number of other key players in the field. For example, the Office of Personnel Management (OPM) sets the policies for the federal workforce, including establishing guidance on hiring authorities, categorization of the cyber workforce, and other essential central functions.

In addition to NICE and OPM, the Department of Homeland Security (DHS) has an office dedicated to workforce development and runs the National Initiative for Cybersecurity Careers and Studies. It also serves as the organizational anchor for CYBER.ORG, a K-12 educational initiative funded by the Cybersecurity Training and Education Assistance Program

(CETAP). In parallel to this, the Department of Defense (DoD) and DHS are both developing agency-specific personnel management systems, and the DoD has also developed a bespoke version of the NICE Framework specific to its own jobs.

Cutting across all these elements are several cross-departmental initiatives: the National Science Foundation (NSF), OPM, and the Cybersecurity and Infrastructure Security Agency (CISA) within DHS jointly run the CyberCorps: Scholarship for Service program; the National Security Agency (NSA) and DHS jointly run the Centers of Academic Excellence program; and NSA and NSF partner on the GenCyber educational program. In short, the system for federal (and national) cyber workforce development is complicated, uneven in its focus, and lacking foundational principles and access to common resources—thereby encouraging the current practice of reinventing competing cyber workforce development strategies in various stovepipes. By investing in its own workforce strategy, the federal government can become an exemplar for effective steps toward a stronger cyber workforce. In order to expand the national talent pool from which they hire, federal leaders can also supplement their investment in the workforce with additional measures to stimulate growth across the whole of the national cybersecurity ecosystem.

C. INVESTING IN A WORKFORCE STRATEGY

Cyber workforce development is a complicated topic, and some degree of complexity in the systems that support it is unavoidable. However, in this decentralized, intricate, and occasionally overlapping system of responsibilities, there is currently no one actor who can take a leadership role to provide cohesive, agile action. A National Cyber Director, a position that the Commission has recommended be established within the Executive Office of the President,[16] should spearhead the effort to develop a cyber workforce strategy, leading a steering committee of other department and agency representatives. This leader, equipped with a clear strategy, would limit duplication of effort, ensure strategically beneficial distribution of resources, reduce interagency competition for the same talent pools, and serve as a central voice to advocate for effective, integrated workforce development. Moreover, implementation of a clear strategy would enable the system as a whole to be more agile and responsive to the changing requirements of protecting U.S. assets in cyberspace. To put government decision makers on a path toward this goal, this paper presents a basic structure of five elements: to **organize, recruit, develop, and retain** the federal civilian cyber workforce, and **stimulate growth** across the cyber workforce ecosystem nationwide, including in the military. Note that this structure is not the same as a strategy. Rather, it is a means for thinking about what must underpin a comprehensive federal strategy.

Working through this structure, this paper will discuss problems that affect the current system of cyber workforce development, highlighting Commission recommendations that are relevant to addressing them. These recommendations do not fully address any element of this structure. No one recommendation will fix how the U.S. government recruits or retains its cyber workforce. Rather, the recommendations demonstrate the types of solutions that the Commission has identified that support an element generally. The elements discussed are not mutually exclusive. In fact, the opposite is true: they are mutually reinforcing and overlapping. Strong retention aids in recruitment, and development tools—like scholarships for education—are often an extremely valuable part of recruiting new talent.

Most critically, none of these recommendations or elements can solve or meaningfully improve the present condition of the cyber workforce independently of other efforts. As leaders implement plans to increase the pool of talent available, they must also consider the other side of the supply-and-demand equation for cybersecurity employees. By addressing the vulnerability of the larger cyber ecosystem, cyber leaders can decrease demand for employees, thereby reducing the gap between available employees and unfilled cyber jobs.[17] More widespread implementation of shared services across government would also reduce the overall demand for additional talent. Yet even with significant improvements in these areas, the cyber workforce must grow dramatically to meet current requirements, let alone future expectations. In order to build a federal cyber workforce strategy to meet this need, Congress and the executive branch must commit to investing the time, attention, and resources needed to make sustainable, coordinated improvements in strengthening the workforce.

1. ORGANIZE

A strong federal cyber workforce must sit on top of a well-organized structure. Departments and agencies must have flexible tools that can adapt to each organization's individual mission while also providing coherence across the whole of the federal government.

Properly Identify and Utilize Cyber-Specific Occupational Classifications

One of the first steps in creating and implementing a federal cyber workforce strategy is determining a way to identify and impact the federal cyber workforce as a whole and different work roles within it. Doing so requires understanding the size, distribution, and composition of today's cyber workforce. Currently, departments and agencies are using two systems of codes in combination—occupational series designations from OPM plus a 3-digit code based on the NICE Workforce Framework—to provide and evaluate this information. As this section makes clear, the current coding effort functions adequately in identifying work roles but does not consistently translate into the establishment and use of appropriate hiring authorities and compensation tools. The Commission recommends an increased effort by OPM to enable departments and agencies to identify cyber work roles and utilize hiring authorities and compensation tools to attract and retain cyber talent. If external assessments continue to show uneven performance by departments and agencies, leaders in the executive branch and Congress must consider shifting to a cyber-specific occupational series. In the long term, this effort will also contribute to the proper identification of candidate positions for inclusion in a Federal Cyber Service (see below).

The Federal Cybersecurity Workforce Assessment Act of 2015 (FCWAA) established a framework to designate and distinguish cyber-specific positions in the federal government. Departments and agencies were required to identify positions that perform cybersecurity work and assign them codes that aligned with the 52 different work roles outlined in the NICE Framework.[18] These three-digit codes were "intended to enhance agencies' ability to identify critical IT, cybersecurity, and cyber-related workforce needs, recruit and hire employees with needed skills, and provide appropriate training and development opportunities to cybersecurity employees."[19]

The three-digit codes operate alongside the existing classification system of OPM occupational series codes, and the two are designed to serve different purposes. Whereas the NICE Framework was designed for talent development and offers a greater focus on competencies than jobs, OPM's system was designed as a classification tool for the purposes of managing personnel. The OPM occupational series codes serve to define occupations and provide occupation-specific standards throughout government, not just in cyber.[20] Currently, cybersecurity roles fall mainly under the Information Technology (IT) Management occupational series, which is numbered 2210. However, not all cyber positions fall within it, and not all positions in 2210 are focused on cyber issues. The highly interdisciplinary nature of much cyber work makes this situation even more complex, because not all cyber positions in 2210 are focused on IT management.[21] This impacts recruitment particularly because job titles align with OPM occupational series, and many job candidates well-suited to this interdisciplinary work may hesitate to apply to a job labeled "IT Specialist (Security)."

These two systems together are intended to identify, count, and rationalize differing standards of defining the common skills and career development needs of the federal cyber workforce. However, there have been persistent barriers to accurately coding cyber positions. In two separate reports, the Government Accountability Office (GAO) studied the implementation of the requirements of the FCWAA, and both identified significant flaws with the implementation of the coding structure. While the first GAO report, published in 2018, identified bureaucratic and procedural issues as the main barriers to implementation,[22] the second, published in 2019, suggested a larger pattern of inaccurate coding by those using the system. GAO found that "22 of the 24 agencies assigned a 'non-IT' work role code to 15,779 (about 19 percent) of their IT positions within the 2210 occupational series."[23] OPM has continued to provide guidance on how these positions are to be coded,[24] but information has not yet been presented as to whether this effort has led to a reliable accounting of cyber positions.

The current system for classifying cybersecurity roles raises two questions. First, is the coding structure working to help leaders in government assess the size, distribution, and needs of their cyber workforce? Judging from the 2018 and 2019 GAO reports, the answer to this question is that the data currently being generated is not sufficiently reliable or useful. Efforts to date have been inadequate, whether because of ineffective processes, confusion around non-IT roles housed in an IT occupational series, or the fact that the NICE Framework and OPM's existing system are designed to serve two different purposes. To quote from DHS's response to the 2019 GAO report, "The current OPM classification and related qualification standards were not designed for describing 21st century cybersecurity work nor developed to align with the specificity of the NICE Workforce Framework."[25]

A second question on the functionality of the present system speaks to the utility of the NICE Framework codes beyond the informational requirements of simply assessing the workforce. Can the codes be used to tailor workforce policies to specific positions within the cyber workforce? For example, if federal hiring managers were struggling to attract systems security analysts (work role 461 in the NICE Framework–based Federal Cybersecurity Coding Structure), but had no problem recruiting technical support specialists (work role 411),[26] could pay flexibilities or special hiring authorities be made available for and be effectively used by agencies to fill the positions with the greatest need? The answer to this question is complex and varied.

In addition to specific hiring authorities authorized separately for use in DoD and DHS,[27] flexibilities are currently available for positions based on occupational series for which department or agency leadership determines—and can document—that there is an urgent need.[28] The categorizing of positions according to the NICE Framework is a helpful tool for these leaders in identifying what positions or competencies are most urgently needed. For example, these designations could be used by agency heads to design professional development or workforce action plans tailored to specific needs highlighted in the coding process, and they can be used to apply certain personnel actions, like retention incentives, based on NICE Framework category.[29] However, other policies, and particularly direct hiring authority, are applied as a function of occupational series; as a result, cyber roles outside the 2210 series (and a very few other technical occupational series)[30] may not have access to the same flexibilities, regardless of inclusion in the NICE Framework. Nevertheless, for positions where flexibilities such as direct hire authorities are already available, the descriptions of cybersecurity work in the NICE Framework may be used to help agency leaders determine the positions for which they want to use those authorities. In short, the three-digit coding structure is (or very soon will be) helpful on an informational and planning level, but some of the most powerful cyber-specific workforce policies are still determined on the basis of occupational series, not Framework-based codes. Because of the underlying structure of the coding system and its reliance on existing OPM occupational series, the availability of hiring authorities and compensation tools for cyber jobs is inconsistent—and where they do exist, they are often underutilized.

The simultaneous use of both the OPM occupational series classifications and the NICE Framework is complex because these two systems are intended for different uses—personnel management and workforce development, respectively—but that does not necessarily mean that the fundamental architecture of the system cannot work. Moreover, the NICE Framework itself is a well-crafted tool, and the individuals charged with coordinating the Framework-based coding process are working diligently to use the system they have to create thoughtful solutions. With sufficient outreach and education—as OPM is currently undertaking with efforts like a webinar series—many of these challenges could be addressed in ways that increase the use of existing hiring authorities and pay flexibilities. In addition, departments and agencies are legally obligated to code their cybersecurity positions, and to do so accurately. The complexity of the system does not excuse non-compliance or underutilization. However, there is a risk that slowly reinforcing a cumbersome system rather than building a new one may drive users to abandon the system altogether. To illustrate, in responding to the 2019 GAO report, DHS stressed its use of alternative authorities to create a bespoke system for its own department, noting that "until the current OPM classification and related qualification standards are updated, [the position description] issues highlighted by GAO will continue to occur[.]"[31]

Despite these challenges, the CSC recommends continuing and even expanding outreach to educate departments and agencies about the proper use of the dual system of OPM occupational series and NICE Framework–based codes. As part of this effort, OPM should push departments and agencies to increase their use of hiring authorities and pay flexibilities for cyber work roles, including those outside the 2210 series. However, if external evaluations continue to indicate limited effectiveness in this approach, leaders in the executive branch and Congress must be prepared to pivot to a new system based on an occupational group containing multiple occupational series aligned to the NICE Framework. This approach, recommended by the CSC, is intended to give ongoing efforts a better chance to take root, while acknowledging that the current system for classifying and coding the federal cyber workforce has distinct disadvantages that additional educational and policy efforts may not remove. However, wide-scale redevelopment of the whole system also comes with costs. Developing and deploying new systems takes time, and thus a more thorough evaluation of the viability of the current system is warranted before embarking on an entirely new system. The National Cyber Director (or, in the absence of an NCD, the Federal Chief Information Security Officer) should lead this evaluation in coordination with OPM, NICE, CISA, the Office of Management and Budget (OMB), and other departments and agencies.

By the end of 2022, the dual system resulting from the Federal Cyber Workforce Assessment Act will have had seven years to take root. If external evaluation—for example by GAO—finds that this system is still not effectively ensuring that hiring authorities, pay flexibilities, and other personnel management tools are consistently available and utilized to strengthen the cyber workforce across all federal departments and agencies, the Commission recommends the implementation of multiple OPM occupational series designations specific to cyber. How these proposed occupational series would align to the NICE Framework deserves further study; the CSC offers a few points for consideration. First, the alignment between the NICE Framework and the series should not necessarily be one-to-one. That is, not all work roles described in the NICE Framework must be included in a cyber occupational series. For example, consider a cyber legal advisor (Framework Code 731). This position is likely to fall under the OPM series for attorneys (0905), and the standards and workforce needs specific to it will likely align as or more closely with other lawyers as with other cyber professionals. The system needs a way to identify that this lawyer is part of the cyber workforce, without divorcing the position from that of other legal professionals.

Conversely, even though the NICE Framework is remarkably inclusive, it is possible to imagine a work role that is not explicitly included—perhaps because the role is a very specific to an organizational mission or slightly divergent subset of an existing NICE Framework work role—but that hiring managers might nevertheless wish to include in a cyber-specific occupational series. Accordingly, occupations not specifically listed in the NICE Framework should not be summarily excluded. For example, the DoD Cyber Workforce Framework (DCWF) leans heavily on the NICE Framework but is tailored to the DoD mission.[32] While the DCWF diverges from the NICE Framework in some ways, its functions still fundamentally align with the core requirements of a cyber occupational series, and the occupational series designers should take an inclusive, rather than exclusive, approach in the case of such variances.

Given these considerations—and the fact that the utility of the NICE Framework extends far beyond simply coding work roles—if it becomes necessary to pivot to an alternative structure for classifying the workforce the two-track coding system should not be disbanded altogether. Rather, cyber leaders should continue to use the NICE Framework while updating the OPM occupational series codes so that they better align with the realities of cyber jobs. Determining the correct level of specificity (i.e., how many distinct cyber occupational series should there be?) and the classification of this update will require study, particularly because the existing high-level divisions of the NICE Framework ("categories" and "specialty areas") are expected to be phased out in a forthcoming update of the NICE Framework.[33] A recognized external authority in public-sector workforce issues, such as the National Academy of Public Administration, may be best positioned to do this research by virtue of being able to see past the experiences and preferences that might bias any one federal actor; however, the determination of the OPM occupational series structure should be dependent on significant engagement by stakeholders. Throughout the evaluation and update of the OPM occupational series, the NCD and other collaborators should be guided by the objective of ensuring that the cyber workforce can be identified and counted, that departments and agencies can identify the competencies needed to fulfill organizational mission, and that tools such as development opportunities, hiring authorities, and compensation tools are made available and are fully utilized across government to help ensure that departments and agencies can readily access and strengthen the talent they need.

Build a Federal Cyber Service

Addressing the immediate need to fill over 30,000 public-sector cybersecurity jobs will require more extensive and regular use of direct hire authorities to overcome challenges in hiring. The standard federal hiring process is cumbersome and slow, and it can significantly hamper the ability of hiring managers to quickly identify and employ candidates with highly competitive cyber skill sets. Most civil servants are hired through a process that typically stipulates requirements, including how the position is advertised and how hiring preference is given to different eligible demographic groups like veterans; but there are also personnel management systems that allow for variances in the government's standard human resource practices. In order to respond to its cyber needs and create greater flexibility, the federal government has begun to use these variances through direct hire authorities and excepted service systems. For example, DoD has begun to implement the Cyber Excepted Service (CES),[34] which permits such flexibilities as allowing hiring managers to advertise jobs anywhere—not just on USAJobs—and to make on-the-spot job offers at job fairs.[35]

The Department of Homeland Security has begun a similar effort to build hiring and career pathways through its Cyber Talent Management System (CTMS).[36] In an attempt to compete in the cybersecurity labor market, DHS is fundamentally reimagining "some of the foundational theories and structures that underlie how the Federal government has managed talent for decades to modernize the civil service for cybersecurity work."[37] This system allows improved hiring by extending the authorities given to the department to hire specialized talent with pay scales and promotion based on performance, thereby incentivizing cyber professionals to join the federal government and helping DHS to recruit from unconventional educational backgrounds.

The CES and CTMS systems are unique to DoD and DHS, and it is unclear how compatible they might be with cyber roles in other departments and agencies for which these systems and programs were not designed. Moreover, these hiring tools do not affect federal contractors, who are generally constrained by contracts that stipulate that employees must have at least a bachelor's degree, thus shutting out the wealth of talent represented by self-taught employees, employees with an associate's degree and industry certifications, and those with many other unconventional educational backgrounds. Employees below the bachelor's level who possess solid cyber skills have shown both an ability to make immediate and valuable contributions to critical cyber tasks and a propensity to embrace continuing professional development. Because such development ultimately yields advanced skill sets that the federal government has difficulty hiring directly from the private sector, identifying tools to engage these employees in public service is critical.

While department- and agency-specific personnel management systems are useful to the organizations that have them, their distribution creates have and have-not agencies. The impacts of this divide ripple throughout the federal cyber ecosystem, as the have-not agencies, many of which do have critical cyber missions, are unable to compete for talent against other federal entities, much less the private sector. Instead, the Commission recommends establishing a unified Federal Cyber Service that operates at an interagency level, working across government to serve as a central administrative resource on expanded direct hire authorities, excepted service, salary flexibilities, and other needs in managing talent that are unique to the federal cyber workforce (Recommendation 1.5). Positions eligible for the Federal Cyber Service would align with dedicated occupational series for cyber, as described in the previous section. Coordinating and standardizing these tools would create a coherent pool of talent that could move between departments and agencies with minimal bureaucratic impediments, thus making possible a greater exchange of knowledge and insight while improving retention by enriching employees' career paths with more diverse opportunities.

Establish Leadership and Coordination Structures

The organization of federal cyber workforce development goes beyond just the administrative systems that shape it. Effective organization also requires establishing clear structures to lead and coordinate workforce development efforts. If—as the Commission recommends—the position of National Cyber Director is established, that office would be a natural choice to lead the interagency efforts required to create substantive improvements and devise interconnected solutions to federal workforce challenges. However, the overall coordination of efforts must truly be an interagency function that takes into account variances in mission requirements, workforce size, and organizational needs. To steer this process, the office of the National Cyber Director should establish and chair two bodies. First, a Cyber Workforce Steering Committee consisting of OMB, OPM, NIST (NICE), CISA, and DoD would provide leadership-level strategic guidance and direct resources to ensure a coordinated approach to cyber workforce development across the federal government. Meanwhile, a Cyber Workforce Coordinating Working Group open to all departments and agencies with rotating leadership appointed by the Steering Committee could address day-to-day development and operation of programs and ensure that they are chartered, resourced, and in alignment with the strategic direction established by the Steering Committee. By institutionalizing these leadership and coordination structures, the government would ensure continuity of workforce efforts as specific priorities for cyberspace policy—and even administrations—change, while also ensuring that the current system of cybersecurity efforts is aligned with an overarching strategy.

2. RECRUIT

With agile hiring authorities and excepted service programs in place to provide the organizational tools for recruiting cyber talent, the government must next turn to the programs that make public service a prospect attractive to talented individuals. In many ways, the federal government's greatest tool for recruitment is the work itself, for "the cyber challenges the government confronts on a daily basis and the data and tools it uses to do so create a professional experience that is wholly unique. That experience, underpinned by a mission that cannot be replicated in the private sector, creates both a recruiting advantage and a foundation for lifelong productivity."[38]

Adding to the unique appeal of its work, the federal government also offers a particularly broad range of development opportunities. These are discussed at further length in Sections 3 (Develop) and 4 (Retain) of this paper, but they deserve to be mentioned here because of their role in bolstering recruitment. For example, a midcareer talent exchange program between the private and public sectors can be a valuable development tool for the public-sector participant, but it is also a demonstration that the federal government is thoughtful and innovative in its career development, which is an enticing prospect for a potential new hire. Adding to the value, an exchange can introduce both the private-sector participant placed in government and the employees of the company housing the government participant to the opportunities available in government work. Accordingly, while they are more relevant to employee development than to recruitment per se, professional development programs can serve to improve recruitment by demonstrating the opportunities available in government.

To capitalize on the advantages created by unique work and development opportunities, the government should invest in existing programs such as CyberCorps: Scholarship for Service and the Centers of Academic Excellence, which are ripe for expansion. Meanwhile, the government should also work to mitigate recruitment barriers that arise from personnel security clearance delays and unpredictability.

Expand CyberCorps: Scholarship for Service

Scholarship for Service (SFS) is a joint program between OPM, the NSF, and DHS that helps students finance their education in cyber-related topics in exchange for a term of service working for a federal or state, local, or tribal government upon graduation.[39] The program awards grants to participating universities, which then award scholarships to students while also using a portion of the funding to build out the university's cyber-focused programming. As a result, the program strengthens educational offerings on cyber topics at the same time that it recruits and develops students who are prepared for federal cyber service. Currently, there are 85 participating universities and community colleges offering SFS scholarships. The program requires that students pursue degrees that are a "coherent formal program that is focused on cybersecurity," and it has supported students working toward a bachelor's, master's, or research-based doctorate degree focused on cybersecurity.[40] The recent expansion of the SFS program through the Community College Cyber Pilot Program (C3P) extends eligibility to students pursuing an associate's degree or specialized program certifications in the field of cybersecurity as well, provided that the students already have a bachelor's degree or are military veterans.[41]

The program has graduated about 275 students per year in recent years,[42] and since its creation in 2000, it has placed 3,600 CyberCorps graduates in public-sector cybersecurity jobs in more than 140 different government organizations.[43] These graduates have brought cyber expertise to the government across a variety of cybersecurity areas, including cyber policy and strategy, security architecture, and cyber operations planning. Because a limited percentage of students can fulfill their service obligation in state, local, or tribal governments as well as in the federal government, the program also provides the opportunity for a limited percentage of graduates to work in public education. This helps address the national dearth of teachers able to provide cybersecurity instruction.[44]

Although the program has an impressive track record, the Commission believes that—given the country's inability to fill tens of thousands of cybersecurity jobs in the public sector—the number of SFS participants should be much higher (Recommendation 1.5). NSF awards multiyear grants under this program to participating colleges and universities, which in turn administer student scholarships. Accordingly, taking practical steps toward increasing the number of students also requires increasing the number of participating institutions and expanding university- and federal-level outreach about the program. The Commission recommends a goal of eventually graduating 2,000 CyberCorps students per year. To reach that target, the Commission advocates for SFS's budget to be increased 20 percent above inflation annually over a 10-year period to support scholarships to additional students and the programmatic efforts needed for expansion. To help jumpstart that budget growth, the Commission recommends increasing funding for the CyberCorps SFS program by $20 million in FY2021.

Build on Centers of Academic Excellence

Like CyberCorps: Scholarship for Service, the Centers of Academic Excellence (CAE) program works through universities to improve educational offerings and increase the cyber talent pool; however, it has a broader overall focus and serves as a tool that the federal government can use to stimulate growth of the national ecosystem, as discussed in Section D of this paper. The CAE program specifies that its goal is to "reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise."[45] While this does speak to a role that extends beyond the federal government, by growing the overall pie of cybersecurity talent the program also grows the federal government's slice of that pie.

Whereas the SFS program focuses on recruiting individuals into government through academic programs, the CAE program addresses cyber workforce development needs across the whole of the nation by strengthening postsecondary education in cyber. The joint NSA and DHS program designates as Centers of Academic Excellence those higher education institutions at which curricula meet certain criteria in teaching students to reduce vulnerabilities in our national information infrastructure. The CAE program thereby encourages the development of high-quality cyber programs nationwide. Such development helps expand the pool of candidates with an educational background in cyber, which does aid in federal hiring but more generally bolsters the national cyber workforce.

The original CAE designation focused on cyber defense (CAE-CD), but in more recent years CAE-CD has developed subsidiary programs to designate excellence in teaching cybersecurity educators (CAE-CDE), research (CAE-R), and two-year programs (CAE-2Y).[46] The CAE program has grown from 7 originally designated institutions in 1999 to 312 institutions in 2019.[47] The NSA also created a complementary CAE for Cyber Operations (CAE-CO) program, which is highly technical and focuses on knowledge of the techniques and tools needed for cyber operations. Overall these programs serve to improve the national security posture by increasing the number of colleges and universities able to produce knowledgeable graduates who are prepared to work in cyber roles.

The Commission recommends building on the work of the CAE program by expanding or replicating it in other disciplines that have significant areas of overlap with cybersecurity, such as law, business, and health care (Recommendation 1.5.1). There are many different types of skill sets required in the cyber workforce, and many areas of overlap with other disciplines. For example, the U.S. government needs lawyers who understand cybersecurity, medical and financial regulators who understand data security, and many others. The CAE program also enables schools that serve underrepresented populations to highlight their merit in educating cyber professionals, thus serving to bring greater diversity to the cyber workforce. Expanding the CAE programs would increase the breadth of talent available to the federal government.

Evaluate and Expedite the Personnel Security Clearance Process

The personnel security clearance process must be reformed in order to address a long-standing source of delays and bureaucracy that confound federal hiring. A 2019 GAO report found that the personnel security clearance process "faces significant challenges related to processing clearances in a timely fashion, measuring investigation quality, and ensuring information technology security."[48] However, the frequently cited metrics used to track progress in improving the clearance process—the length of delays and backlog of investigations—tell only a part of the story. Not only are delays in clearances and hiring a major hindrance in getting new hires working, they also harm recruitment. Prospective candidates avoid federal service because the clearance process is slow and unpredictable. In order to make meaningful change, decision makers need a better understanding of how the security clearance process actually affects recruitment in the context of a highly competitive cyber recruiting environment.

Personnel security measures are a necessary requirement of the field, and to some extent they may even serve as a short-term incentive to recruitment for prospective employees who wish to eventually leverage that clearance into work for federal contractors willing to pay top dollar for cleared professionals. But preventing the U.S. government from building a talented federal cyber workforce creates its own security risk. The government needs to ensure that the clearance process today is not doing more harm to national security than good. Further assessments must weigh the risk to national security of leaving critical cyber security jobs unfilled against the benefits of the security provided by the current process, which is plagued by delays, unpredictability, and frustrations. Better understanding the importance of these dynamics is the first step in making smart policy choices on how to improve national security through a robust and secure cyber workforce.

The Commission calls for an assessment of the impact of the personnel clearance process not just on hiring but on federal cyber workforce recruitment more generally (Recommendation 1.5), recommending that the Comptroller General conduct a review of the existing process and its impacts on recruitment and summarize these findings in a report to Congress. The assessment should include an estimate of how frequently candidates discontinue, or are deterred from, pursuing federal government jobs because of delays in personnel security clearance issuance, an evaluation of how effective the clearance process is at balancing the national security risk of insider threats and the national security risk of leaving cyber jobs vacant, and a recommendation for a lead agency to develop and implement a plan to address any gaps.[49]

Work to improve the security clearance process is under way. In 2019, the agency that formerly oversaw security clearance processing was dissolved, and its operations were handed off to the Defense Counterintelligence and Security Agency (DCSA).[50] The backlog of investigations has decreased significantly as new approaches have emerged under a framework called Trusted Workforce 2.0.[51] Although DoD cyber leadership has pointed to efforts to reduce clearance times to improve cyber hiring, clearance delays remain a major barrier.[52] As a stopgap while the larger clearance process is reformed, departments and agencies should consider a more focused approach of expediting clearances for certain cyber roles—for example, in positions hired under DoD's Cyber Excepted Service. However, doing so would raise potential concerns about whether the process would force non-cyber clearance investigations further down the queue of those waiting to be processed. Moreover, without systems like Cyber Excepted Service, other departments and agencies will be even less able to compensate for delays due to the security clearance process.

Beyond the issuance of clearances to new hires, challenges still exist in handling other categories of vetting. Present reforms to the security clearance process are expected to significantly alter clearance reinvestigations, but clearance transfers fall into a different category.[53] Therefore, delays in moving an employee from one organization to another, noted by department and agency leaders in cyber and beyond, may continue. Even though, with few exceptions, "[a]gencies shall accept national security eligibility adjudications conducted by an authorized adjudicative agency at the same or higher level,"[54] agencies have come to interpret reciprocity policies differently,[55] leading to persistent problems. These problems are compounded by ongoing requirements for suitability reviews, which are investigations separate from a security clearance process. While on the whole much shorter, suitability reviews can still add significant delays to interagency transfers, and—particularly for an individual transferring with a clearance—it is hard to view them as anything other than added bureaucracy. When it comes to the suitability review, interagency clearance reciprocity, and the bringing on of new cyber hires, federal leaders face more major changes in order to lessen the impacts of personnel security processes on the cyber workforce.

3. DEVELOP

The federal government has a strong history of recruiting extremely talented individuals. However, only about 24 percent of employers in cybersecurity feel that university graduates are well-prepared for workplace cybersecurity challenges;[56] thus even the most talented new hires will need further development to adapt to the specific tasks of any given work role. They will also need ongoing professional development throughout the course of their career in order to keep their skills sharp and up to date. Equally critically, federal employers must create opportunities for learning and development on the job because the federal government must tap into new sources of talent from a broad array of educational backgrounds. There are simply not enough people graduating with "conventional" educations—from four-year computer science and engineering degree programs—to fill the gap needed to secure our nation in cyberspace. Between the years of 2016 and 2017, U.S. universities and colleges conferred about 71,000 computer and information science degrees.[57] Presumably only a small percentage of these graduates went into security jobs. In contrast, as of August 2020 more than half a million cybersecurity jobs in the United States remain unfilled, and the number is rising.[58] The growth rate for cybersecurity jobs is significantly outpacing the growth in the supply of individuals qualified to fill them.[59]

It is imperative that the federal government identify more and different on-ramps—pathways that lead to entry-level positions in the federal cybersecurity workforce—and policies that encourage that workforce to remain in federal employment. To address this issue, the Commission recommends a number of actions that will help close the skills gap. Two of these recommendations, described below, illustrate the work-based learning opportunities that should characterize a national strategy.

Develop Apprenticeships

Apprenticeship programs, which couple classroom education with paid on-the-job learning, can help create new pathways into the cyber workforce for many individuals, offering them the opportunity to obtain job-specific skills and knowledge while earning a salary. Paid on-the-job learning ensures that cyber students receive a strong applied education in addition to the necessary theoretical foundations, and it provides the added socioeconomic benefit of reaching communities that may not be able to take advantage of unpaid internships. In the current hiring environment, it is clear that employers in government and industry alike cannot keep focusing on recruiting midcareer or senior-level talent with years of experience. Moreover, as older professionals retire, it becomes increasingly important to capture institutional knowledge, and pairing experienced mentors with incoming apprentices provides an opportunity to build knowledge and security skills sometimes difficult to transmit in texts or exercises. Rather, the Commission recommends that the U.S. government provide a proof of concept by creating programs that allow truly entry-level employees to gain the first years of experience critical to a career in cybersecurity (Recommendation 1.5).

Because cyber expertise takes time to develop, apprenticeships are a long-term approach with a long-term payoff. However, the current moment offers a unique opportunity to begin. In the context of the widespread unemployment resulting from the COVID-19 pandemic, connecting learners with the tools needed to build knowledge and expertise offers benefits on multiple fronts. Not only does apprenticeship create paid employment, but it also creates a pool of prospective cyber employees who have learned skills and tools tailored to their particular organization's needs. While some employers in government, worried about retention, may hesitate to invest in their employees for this kind of tailored training, there are a number of steps that the federal government can take to protect their investment, as discussed in Section 4 (Retain) below. In keeping with the service obligation common to many other education programs in government, which require employees to work in government for a period of time commensurate to their time being educated, federal apprenticeship program sponsors might consider incorporating a service term that corresponds to the hours of instruction that students receive.

Investing in apprenticeship programs will assist the federal government in filling cyber jobs while creating a proof of concept for state, local, tribal, and territorial (SLTT) governments and private-sector businesses that could benefit from similar models. In this way, federal leaders could demonstrate that the challenges to the implementation of apprenticeships can be overcome. For example, many of the logistical arrangements needed to design, register, and manage an apprenticeship program can be undertaken by experienced non-federal partners that can operate the program until the apprentice is ready for federal onboarding. Similarly, Department of Labor requirements like educational curricula can be provided by external partners.

In developing these programs, government departments and agencies should avoid duplicating efforts, and instead should consult existing communities of practice with expertise in establishing cyber apprenticeships. In order to prepare for successful on-the-job learning, programs should also ensure that structures are in place to reward and incentivize mentorship in the workforce. These mentorships form an essential part of the apprenticeship model and can provide an informal mechanism to retain critical system information within the enterprise. Implementers can also promote high-quality programs by ensuring that programs are registered with the Department of Labor or appropriate state apprenticeship agency,[60] that apprentices receive wages that increase as their skills improve, and that apprentices receive portable credentials—such as industry certifications—to document learning outcomes.[61] Finally, as is true of all workforce development programs, program managers should implement ongoing monitoring and evaluation efforts to identify opportunities to improve and to ensure that the program is producing the expected outcomes for both employers and apprentices.

Support Upskilling

Another way that the Commission recommends creating more skilled federal cyber workers is through a new pilot program designed for upskilling military veterans and transitioning military service members, in order to provide them a path into federal civilian cybersecurity jobs (Recommendation 1.5). These programs proposed by the Commission would be run by the Department of Veterans Affairs to support and train former service members looking for new ways to serve their country. Rather than building the infrastructure for this effort from the ground up, the pilot program should utilize existing virtual platforms created by departments and agencies for coursework and their other educational resources, like DHS's Federal Virtual Training Environment (FedVTE). Doing so will enable federal agencies to take advantage of the military training and security clearances possessed by recently transitioning veterans. To maximize the benefits to veterans and their future employers, programs should also incorporate work-based learning opportunities and portable credentials to demonstrate learning. Furthermore, upskilling programs should align with specific knowledge, skills, tasks, and—as appropriate—work roles in the NICE Cybersecurity Workforce Framework.

4. RETAIN

Efforts to retain the federal cyber workforce naturally overlap significantly with other elements of an effective workforce strategy. Professional development and career growth opportunities help keep workers interested in their roles. At the same time, the federal government's public service mission and the unique nature of the work provide their own argument in favor of continued government service, just as they are a compelling recruiting tool. Moreover, the same excepted service tools that aid in recruitment also can give greater flexibility in pay, and the more flexible salaries that help recruit new employees also help retain them. In many ways, effective federal workforce retention is an outgrowth of having an effective workforce development strategy more generally.

Viewed through a national security lens, the loss of federal employees to other sectors has a silver lining, because other parts of the national cybersecurity ecosystem benefit from an improved workforce as government-trained personnel take up positions with critical infrastructure firms, managed service providers, and other organizations. It may be tempting for understandably frustrated managers in the federal government to throttle spending on training for fear of losing their investment, but leaders in Congress and the executive branch should take a longer view, recognizing that investing in cyber workforce development is an excellent example of the proverbial tide that lifts all boats.

Another way for the government to capitalize on its workforce investment would be to alleviate the bureaucratic challenges associated with returning to federal service, thereby making it easier for employees to move back and forth between sectors. While efforts to remove barriers that inhibit talented employees from returning to federal service are certainly not unique to cyber, the urgent need for cyber professionals makes finding pathways for their return to federal service particularly critical. Such changes would allow the government to benefit from the new skills gained by employees after a stint of work in the private sector. Given this range of considerations, retaining the federal cyber workforce becomes a much more nuanced challenge than can be met by simply providing competitive salaries—though that is certainly a significant factor. Rather, federal workforce retention is a question of creating opportunities to keep talented individuals engaged throughout the duration of their careers.

Increase Pay Flexibility

Surveys show that half of cybersecurity employees who leave jobs cite better financial incentives among their reasons for leaving.[62] In the federal government, where pay is often determined by rigid criteria, offering competitive compensation can be a serious challenge. Pay and promotions are often tied to academic degrees and years on the job, an approach uniquely ill-suited to a field in which the distribution of skills and experience frequently correlates with neither academic degrees nor seniority. For example, in a number of cybersecurity roles, an associate's degree can be a very valuable credential, particularly as the Centers of Academic Excellence Program continues to certify two-year programs. But according to the standard federal pay scale (with no adjustments for a cyber role), a professional with an associate's but no bachelor's degree would likely enter the workforce at GS-5 or GS-7 level, meaning that they are likely to make between $39,000 and $63,000 per year in the Washington, DC, metro area.[63] To provide a rough comparison, in industry, the same individual might expect a median offer closer to $80,000 per year.[64] For many early-career employees a year or two into federal government service, this disparity in pay may make a compelling case for seeking other employment.

In order to offer competitive compensation to talented individuals who may be young or self-taught, or who possess the skills and abilities to be promoted quickly, managers need personnel systems that offer pay flexibility. As noted above in the case of recruiting flexibility, some departments have or are developing these tools. For example, DoD's Cyber Excepted Service offers two additional steps beyond the standard government pay scale to make possible salaries that are more competitive with private-sector compensation.[65] However—and again as is true of hiring flexibilities—these pay flexibilities are distributed unevenly across government. They can also create challenges or disincentives for individuals who may want to move from a position with these flexibilities to one without. DoD and DHS have congressional authorization for their own systems, including pay flexibilities, but other departments and agencies are more reliant on a mix of existing authorities. Outreach and education could increase to some extent the use of authorities that may be bypassed because federal cyber hiring professionals are not aware of them. But broader changes to implement coherent, tailored, cyber-specific measures—akin to what DoD or DHS use—across the federal government would require congressional approval.

Develop Career Pathways

Opportunities to grow and advance are critical to any career, and they seem to be particularly influential for members of the cyber workforce. Although data on retention is limited, results from a cross-sector survey of cybersecurity professionals suggest that limited promotion and development opportunities are just as likely to persuade a cybersecurity professional to leave their job as financial incentives.[66] Whereas the federal government may lack flexibility in pay, it has a great deal of room for creative solutions in designing attractive career paths. By dint of its size, the federal government is without a competitor in the number and diversity of work roles it offers. No other employer can offer so many different missions, working environments, or on-the-job learning opportunities. To take advantage of this strength, the federal government must be able to leverage all of its different career pathways: employees need to be able to cross between different departments and agencies during the course of their career. Enabling this flexibility depends in part on having standardized or reasonably interoperable personnel systems, as outlined in the prior discussion on a Federal Cyber Service. Beyond simply having the tools to promote flexibility, the federal government should work to map out potential pathways. An interagency group of employees, taking the initiative, has just published an articulation of federal cyber career pathways.[67] This effort, and others that could help support it, could be very beneficial in promoting employee satisfaction and retention.

Establish Rotational Programs and Talent Exchanges

To create opportunities to gain novel work experience, the Commission recommends two different types of programs—rotational programs within government and exchange programs with the private sector—that temporarily place employees in different working environments. Rotational programs would provide employees with an opportunity to gain experience working in a different department, agency, or office within the federal government. The 2019 Executive Order on America's Cybersecurity Workforce mandated the creation of a rotational program to provide developmental experience for employees in different departments and agencies.[68] While the program is currently quite small in scale, it stands as proof of concept that such developmental opportunities are possible.

Equally important, the continued development of talent exchange programs between the private sector and government would provide unique and enriching on-the-job learning experiences for all participants while encouraging improved collaboration focused on identifying systemic vulnerabilities that will reduce the future impact of cyberattack. The Commission recommends that Congress should direct and fund CISA to develop a program for one- to three-year exchange assignments of cyber experts from both CISA and the private sector (Recommendation 1.5). Part of the challenge in making the program successful is making it scalable. For example, the Department of Defense and the Department of Homeland Security both have had similar programs, but they are small.[69] The DoD program, for example, is capped at under 50 participants at any given time.[70] As a practical matter, bringing in participants involves a great deal of outreach to industry partners and does not affect large portions of either the DoD or DHS cybersecurity workforce.

Though a scalable program would be even more effective, exchanges benefit the federal government as a whole by opening new avenues for collaboration with the private sector to improve national security. Moreover, because much of national critical infrastructure is owned and operated by the private sector, the involvement of these private-sector employers where possible would offer additional benefits to national security, for protection of such infrastructure is itself a national security issue. In organizations like the national laboratories that support critical infrastructure, the infusion of new insights that can come from exchanges with researchers around the country and the world can be especially valuable.[71] Further, talent exchange programs offer opportunities for both the private sector and federal government to identify shared threats and vulnerabilities, an action that will reduce the future impact of cyber attacks. For CISA specifically, the program will provide insight into potential innovation based on fresh ideas. For employees, it creates the opportunity to learn about new threat actors, become familiar with different tools, and learn from mentors across sectors.

Beyond the Commission's specific recommendation on the idea of public-private workforce collaborations and exchanges more generally, a great deal of opportunity exists to develop creative initiatives that bridge sectors, communities, and even geographic regions.[72] These kinds of interesting and innovative programs do more than just enable employees to develop their skills and expand their experience: they could incentivize greater retention by providing interesting opportunities for professional development.

Address Systemic Inequities

Diversity, equity, and inclusion initiatives are critical to connecting with talented individuals who approach problems from different perspectives. In a variety of industries, a more diverse workforce demonstrably leads to better performance.[73] In cybersecurity particularly, such diversity also helps the government recruit from a larger pool of talent. While a focus on recruitment is critical, and tends to dominate diversity initiatives, it misses the importance of retaining employees from underrepresented groups. Their retention largely depends on fairness in opportunities for career advancement. This section will discuss the critical importance of retaining individuals from underrepresented groups in the federal workforce, while noting that there is also a larger conversation around how the federal government can and should spur investment in diversity in the national cyber workforce writ large. The latter issue is addressed in the section "Invest in Diversity, Equity, and Inclusion," below.

Some employees confront barriers moving up in the workforce. Research has identified a "broken rung" in the career ladder for women.[74] Similarly, research shows that while people of color are relatively well-represented in the cybersecurity industry in the aggregate, they are proportionally underrepresented in director-level positions relative to the percentage of directors in the overall U.S. minority workforce.[75] More generally, in the national cyber workforce, issues such as fair compensation consistently remain a problem.[76] These patterns suggest that systematic problems are inhibiting nonmale and nonwhite candidates from advancing in their positions. Employers can help address these barriers by taking deliberate steps such as seeking promotion reviews by diverse committees, establishing clear and consistent criteria for performance and promotion reviews, and ensuring that employees involved in hiring and performance review receive unconscious bias training.[77] By taking proactive steps to address the inequalities and unconscious bias that limit advancement and inhibit retention of underrepresented demographics, government managers can make significant strides in strengthening their workforce. Accordingly, the Commission recommends that departments and agencies develop training for managers to provide them with the tools to foster a more inclusive work environment and a diverse cyber workforce.

The Commission also recommends strongly encouraging federal contractors to follow the government's lead and implement workplace policies that are known to improve workforce retention. Practices such as paid family leave and flexible schedule options increase retention rates among employees who might otherwise leave the workforce or gravitate toward employers with more family-friendly policies. For example, analysis across a range of industries shows that women who have paid family leave are 93 percent more likely than those who do not to be in the workforce a year after giving birth, and Google, Accenture, and Aetna all report decreases in female attrition from their workforce after improving their paid family leave policies.[78] There are no quick fixes to the systemic problems that make it difficult to retain a diverse workforce; however, retaining a strong cyber workforce requires that government and employers across industries invest in meaningful steps to identify and address the barriers to advancement that underrepresented groups face.

5. STIMULATE GROWTH: EXPAND THE CYBER WORKFORCE NATIONWIDE

The civilian cyber workforce within the federal government cannot thrive independently of the larger national cyber workforce, including the military. This is true for several reasons: talent moves between sectors, the paths to entry to public- and private-sector jobs can overlap, and cybersecurity in the private sector and cybersecurity in government often have interconnected responsibilities and are reliant on one another. As a result, a strategy for building a strong federal workforce must take into account ways in which the federal government can support the larger system of national cyber workforce development. This is a shared responsibility: private-sector employers, academics, and many others have a stake in contributing to this shared system, which is critical to the functionality of all. At the same time, the military cyber workforce both shapes and is shaped by the available talent in the larger ecosystem. While all of these stakeholders can and should be thinking strategically about their contributions, this section discusses the steps that the federal government should take to systemically improve the foundations of the national cyber workforce by promoting diversity, supporting empirical research to better understand the cyber workforce, coordinating government efforts that support cybersecurity workforce development, bolstering cybersecurity education, and fostering the military cyber workforce as an influential part of the the larger national cybersecurity workforce.

Coordinate U.S. Government Efforts

There are a number of initiatives across the U.S. government focused on growing and improving the nation's cybersecurity workforce. While it is important to continue these programs in their current organizational homes, the Commission recommends assigning NICE the designated role of facilitating coordination among these efforts (Recommendation 1.5). Having a single coordinator will provide strategic alignment and pave the way for the development of a national cyber workforce strategy supported by the high-level strategic plan that NICE is already responsible for creating.[79] As noted in the 2009 report "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce,"[80] and then emphasized in the follow-up 2015 report, "the government still lacks the cyber workforce it needs and still does not have a comprehensive, enterprise-wide strategy to recruit and retain that workforce."[81] In the long term, the Office of the National Cyber Director would be the ideal place for developing and implementing a national cyber workforce strategy, in close collaboration with NICE, but having NICE facilitate this coordination in the interim is a good first step toward such a strategy.

Invest in Diversity, Equity, and Inclusion

A critical step in improving the national cyber workforce, both in government and beyond, is to promote diversity, equity, and inclusion in the workforce. Above, this paper discusses changes that the federal government might make to address systemic inequalities that may hinder its retention of individuals from underrepresented groups. But the opportunity in this area extends beyond the federal workforce and issues of retention. Cybersecurity affects the whole nation in ways that can be deeply personal and incredibly important. With all that is at stake, the U.S. government needs a national cybersecurity workforce that understands and has experienced these impacts from the perspectives of the people it aims to protect; the nation needs a cybersecurity workforce that reflects the population as a whole. While a lack of diversity in the federal government is by no means unique to cybersecurity, the demand for more people, and more diverse perspectives, in cyber makes the need especially acute. The federal government can and must help drive this change throughout the national cyber workforce. To that end, the Commission recommends that cyber workforce development policies and programs consistently and deliberately incorporate efforts to recruit and retain underrepresented populations including women, people of color, and the neurodiverse—that is, individuals with neurological differences such as autism, dyslexia, or social anxiety disorders[82] (Recommendation 1.5). Having teams of people who approach problems differently—whether those approaches are rooted in different personal, professional, and educational experiences or in variations in neurology—is an asset.

Diverse teams perform demonstrably better. They focus more on facts, process those facts more carefully, and are more innovative.[83] In fact, research shows that functionally diverse teams—that is, teams whose members think about problems differently—can even outperform teams composed of members whose individual ability is judged to be higher.[84] In protecting the nation from attacks of significant consequence in cyberspace, the United States cannot afford to field anything less than our strongest teams: and our strongest teams will invariably be those that value diversity. Moreover, demand for cybersecurity talent is so overwhelming that the U.S. government must, as a matter of national security, tap into underrepresented groups with nontraditional backgrounds as a source of potential cybersecurity aptitude.

In confronting complex problems, a workforce that can think through these challenges in different ways is at an advantage. Groups that are composed of individuals with a broad range of perspectives, skills, and backgrounds can see and solve problems by drawing on a collective brain trust that can accomplish what no single skill, however eclectic, can accomplish on its own. Neurodiverse individuals can contribute to such groups and environments in particularly valuable ways. For example, some individuals on the autism spectrum are exceptionally talented at spotting patterns, enabling them to uniquely contribute to the workforce.[85] Accordingly, military, national security, and health organizations of the U.K., Australian, and Israeli governments have developed special hiring programs to attract neurodiverse individuals. Both the Israeli Defense Forces and the Australian Defence Organization have programs specifically aimed at bringing individuals on the autism spectrum into the workforce.[86] The British General Communications Headquarters—an organization akin to the NSA—has three times the national average of dyslexic people in its apprenticeship programs, leading its director to observe that "with the right mix of minds anything is possible."[87] Underscoring the potential benefit these individuals can bring to an organization, the Australian Department of Human Services found that software testing teams made up of neurodiverse individuals were 30 percent more productive than other teams.[88] If given the opportunity and sufficient support, neurodiverse individuals can be an enormous asset to the cyber workforce.

While statistics on the demographics of the current workforce vary significantly between sources, the field's demographic diversity clearly offers an area for improvement. Recent studies have shown that the proportion of women in the global cyber workforce falls somewhere between 11 percent and 24 percent.[89] Throughout its ranks, the cybersecurity workforce does not currently reflect the demographics of the American public, which limits the degree to which it can benefit from differing viewpoints and voices that encourage vibrant and healthy debate. This problem is not unique to cybersecurity, but as many different fields and workplaces confront imbalanced power structures and systems permeated with implicit biases, the cyber field has an opportunity to make concerted changes and be an exemplary leader in enacting positive reforms.

Incentivize Empirical Research to Identify a Baseline and Measure Success

It is difficult to build a national cyber workforce strategy and to recognize best practices and predict future trends without good data to describe that workforce. While accurate statistics on the gap between cyber job vacancies and qualified candidates are increasingly available, for many other aspects of the cyber workforce there is a dearth of information needed to inform sound cyber workforce policy. These knowledge gaps are best highlighted by emphasizing examples of the fundamental questions about the workforce development ecosystem that are still unanswered:

- How many graduates from four-year degree programs in computer science or engineering are expected to go into cybersecurity disciplines per year?
- What is the average tenure for a federal cyber worker? for a private-sector worker? How many cyber professionals return to federal service after working for a period in the private sector?
- How do federal salaries compare to private-sector salaries at different levels of experience and in different work roles? How does this comparison change when additional employee experience, academic degrees, or other credentials are taken into account?
- Statistically speaking, at what points during recruitment, hiring, or career progression do cyber professionals from underrepresented demographics or backgrounds tend to fall out of the pipeline?
- What is the correlation between K-12 cybersecurity education or career awareness efforts and increased long-term professional or academic interest in cybersecurity? Do repeated interventions or different types of interventions increase a student's level of interest in or awareness of cybersecurity?

Unless these baselines for the cyber workforce are established, it is difficult or even impossible to determine which programs and policies are successful in strengthening the cyber workforce. Perhaps even more consequentially, the lack of metrics makes it significantly harder to demonstrate that investment in cyber workforce development is money well spent. In a 2017 report to the White House on cybersecurity workforce development, the Secretaries of Homeland Security and Commerce highlighted in particular that “[i]n all cases, to better inform sponsors and shape policy, more and better information needs to be collected regarding the inputs, outputs, outcomes, and impacts of efforts.”[90] But before sponsors of workforce development programs can measure their impact, or even design programs that address the right problems, they must have a firm understanding of the composition and dynamics of the cyber workforce.

To bridge this knowledge gap, incentivize research on the current state and development of the cyber workforce, and encourage the development of measurements of effectiveness, the Commission recommends that Congress fund the Director of the National Science Foundation to competitively award research grants to higher education institutions or eligible nonprofit organizations in order to address key cyber workforce issues (Recommendation 1.5). These entities would conduct studies to help analyze the current state of the cyber workforce, successful paths to entry, demographic trends, and other similar topics as approved by the director.

To avoid duplication of effort, this research should draw on prior research funded by NSF, as well as resources and collaborative opportunities at NIST, DHS, and other federal departments and agencies as deemed appropriate by the director. The research would align with or build on the NICE Cybersecurity Workforce Framework whenever possible and leverage the collective body of knowledge from existing cyber workforce development research and education activities.

Support Cyber Education

The Commission recognized that the federal government cannot merely cut itself a bigger slice of the cybersecurity workforce pie. Instead, the government must support growing the whole pie of talent needed throughout the nation. To that end, the Commission made several recommendations on a range of educational issues. The federal government’s role in education, particularly at the K-12 levels, is limited, because most education policy is determined by state and local governments; however, the federal government can provide resources and opportunities to lower barriers to cyber education nationwide. The federal government can also push for greater internet connectivity to ensure that educational opportunities are accessible in rural areas and other places where broadband access may be limited. This is necessary for providing cybersecurity education, but it is also necessary much more broadly in the era of COVID-driven virtual learning. The list of efforts mentioned here is certainly not exhaustive. For example, the NSF and NSA run the GenCyber program, which provides summer camps for K-12 students to help increase interest in cyber careers among diverse groups, teach basic online safety, and improve teaching methods.[91] Because this section focuses on possible changes to the educational ecosystem, it spends little time on programs that are working well. Rather than replace or modify these existing efforts, the Commission’s recommendations are intended to add to them. Implementing these recommendations will help address the growing need for cyber skills and will ensure that we have the right people with the right tools to confront current and emerging cyber challenges.

Clearinghouse for K-12 Resources. When we think about future careers, it is hard to imagine an industry that would not require both a basic and an ongoing education in cyber. Yet incorporating cybersecurity material into K-12 curricula can be difficult, as teachers work to enhance their own understanding of the material while balancing different educational priorities and limited classroom time. Moreover, educational priorities are generally established at local levels, which makes the process of scaling up change more complex. To help students gain this critical cyber knowledge while respecting these constraints, the federal government should focus on providing resources, tools, and incentives to encourage and assist educators working to incorporate these materials into their school systems.

The Commission recommends creating an easy-to-find clearinghouse of resources on K-12 cyber education (Recommendation 1.5.1). There are many groups creating school-age cyber educational content. Two examples are Code with Google, which provides a computer science curriculum free to all educators,[92] and the Virginia Cyber Range, which provides an introduction to cybersecurity course for high school students and K-12 educators, complete with a virtual environment to provide hands-on practice.[93] The challenge for the federal government is to further incentive the development of this content, curate it, and make it easy to add to different school systems' curricula. DHS, NIST, and others across government have begun work in this direction, and rather than replicate those efforts, the Commission seeks to build awareness of these resources and to get them into the hands of teachers. It is simply not enough to place these resources on a website. The impact of these K-12 cyber educational materials is realized when they are popular, accessible, and easy to use.

CETAP, Curricula, and Teacher Professional Development. In its report, the Commission advocated for exploring ways to support and expand existing programs that improve cybersecurity education on a national scale. In outreach following the report's publication, the cybersecurity community has voiced a clear need for this kind of national effort, particularly when it comes to curricula for teaching cybersecurity to different ages and the professional development required so that teachers can provide instruction on cybersecurity. Research shows that only 7 percent of teachers surveyed feel they know a lot about cybersecurity education.[94] However, just as federal employers face fierce competition from the private sector in offering competitive salaries for cyber talent, so too schools struggle to attract and retain employees with expertise in cybersecurity. Moreover, as schools balance competing educational priorities and limited class time, they often cannot manage to develop and teach specialized cybersecurity curricula.

To address this need, the Cybersecurity and Infrastructure Security Agency within DHS hosts the Cybersecurity Education and Training Assistance Program. CETAP's current implementer, CYBER.ORG, runs workshops for teachers and supports a cyber education certificate program, among other activities in K-12 cyber education and career awareness. The platform also supplies cybersecurity curricula tailored to different ages and subjects. Although these activities are extremely valuable, their reach is limited. Currently more than 18,500 teachers are enrolled in the CYBER.ORG content platform;[95] and while that is an impressive number, there are now about 3.6 million K-12 teachers in the United States.[96] Not all of these educators need cybersecurity professional development in equal measure, but it is still clear that CETAP has significant room to grow. Accordingly, the program should be authorized in law and funded to facilitate expansion of the professional development and other resources needed for supporting K-12 cybersecurity education.

Cybersecurity in School District Leadership. Schools are experiencing a significant number of cyberattacks, but few districts have the capabilities necessary to fully plan for, prevent, mitigate, and respond to these incidents. In 2019 there were 348 publicly reported cybersecurity incidents in public K-12 schools—three times the number reported in 2018.[97] Given that mandatory reporting requirements vary from state to state—and are for the most part very lax[98]—the actual number of cyberattacks is likely to be much higher. Despite this pressing concern, there is a distinct lack of cybersecurity leadership in K-12 education. According to the Consortium for School Networking's 2020 report on the state of educational technical leadership, out of 513 school system technology leaders and educational leaders questioned, less than one-fifth responded that their school system has a full-time employee devoted solely to cybersecurity, although they ranked cybersecurity as their number one priority.[99] However, among those same respondents there tended to be an inclination to underestimate the risk; less than one-fifth considered any particular threats to be high risk, and only 12 percent responded that their school district had a separate budget for cybersecurity.[100] Though school budgets are spread thin, cybersecurity, and specifically cybersecurity leadership, should be a priority—especially in the COVID era of remote teaching. Apart from the direct benefits of protecting student and staff data, a chief information security officer (CISO) or other IT cybersecurity leaders would be an advocate for teaching cybersecurity in classrooms (or virtual classrooms, as the case may be). As the Department of Education has begun to do in partnership with the nonprofit group Educause, the federal government can help state and local leaders by sharing threat information and best practices for protecting student data.[101]

Civics Education and Digital Literacy. In recent years, there has been a dramatic rise in the use of social media platforms by foreign governments as a tool to manipulate U.S. public opinion and sow discord. From 2017 to 2019 the number of countries waging political disinformation campaigns more than doubled to 70.[102] The Commission recognized this rising trend and wanted to help Americans become more resilient to cyber-enabled information operations. Often these foreign influence campaigns seek to convince Americans that their democracy is irreversibly corrupted, and success can lead to conflict out of frustration or to disengagement born of despair.[103] Education can serve as a tool for countering this influence by helping the population to better understand the democratic process and the role that each citizen plays in it. Moreover, instilling a greater sense of civic responsibility can also support a broader understanding of the responsibility borne by each individual for knowing and exercising best practices online to bolster not only their own security but that of their companies, communities, and country. The Commission therefore recommends that the U.S. government promote digital literacy, civics education, and public awareness to build societal resilience to these foreign cyber-enabled information operations (Recommendation 3.5).

It is important that Americans understand what democracy is, how individuals can hold their leadership accountable, and why democracy must be nurtured and protected. Placing government limitations on speech, even as a means of countering disinformation, risks infringing on the right to free speech; therefore, the Commission recommends developing curricula that build trust in our democratic institutions, and more tools to verify the accuracy of information found online. Specifically, the Commission recommends creating a grant program to enable nonprofits, private-sector entities, and SLTT education agencies to study how best to improve digital citizenship and to incorporate effective digital literacy curricula in American classrooms at the K-12 level and beyond (Recommendation 3.5).

Strengthening Postsecondary Education through Work-Based Learning Educational Opportunities and Cybersecurity Clinics. Research shows that employers feel colleges and universities focus too narrowly on theory at the expense of hands-on cybersecurity experience and practical skills.[104] In fact, a complaint often voiced by employers is that a four-year degree does not adequately prepare new hires for jobs in cybersecurity.[105] Work-based learning programs enable students to learn by directly applying their skills in a real-world context. Colleges and universities can incorporate these opportunities into their curricula by including cyber ranges and cybersecurity competitions.[106] In addition, programs such as cyber apprenticeships, fellowships, and internships provide opportunities to reinforce and instill cybersecurity theory and concepts in a tangible way. They also serve as a mechanism for students to demonstrate skills, competency, and experience, which are increasingly attractive to and required by employers. The Commission recommends that the U.S. government develop work-based learning programs to supplement existing curricula and hands-on opportunities in institutions of higher education (Recommendation 1.5.1). Finally, the Commission recommends that the U.S. government fund cybersecurity clinics at colleges and universities (Recommendation 1.5.1). These clinics serve as educational opportunities for students to gain real-world experience by completing activities such as risk assessments and security audits for vulnerable companies, civil society organizations, or nonprofits that request support.[107] Not only do these clinics serve the needs of the students by teaching them the tools and techniques that more theoretical classroom education does not cover, they also give back to local communities and help meet the cybersecurity needs of businesses that might not otherwise have access to these services.

Build the Military Workforce

The military cyber workforce is in the interesting position of being part of the national cyber workforce and a significant driver of talent throughout that workforce, as many of today's cyber professionals get their start in the military. Central to both the White House's 2018 National Cyber Strategy and the Department of Defense's 2018 Defense Cyber Strategy is successfully recruiting and retaining talent in the military cyber workforce.[108] While the military workforce will benefit from many of the broader education initiatives and security clearance reforms advocated for the federal civilian cyber workforce, it also presents unique challenges. These challenges of recruiting, training, and retaining a military workforce are different because it has a fundamentally different purpose in U.S. cyber strategy than do its civilian counterpart. Members of the armed services conduct cyber defense, cyber intelligence, and offensive cyber operations as uniformed military personnel, and these service members support military campaigns, operational plans, and intelligence preparation of the combat environment. Sometimes military cyber operators work beside civilian intelligence counterparts far from conflict, but at other times they are embedded within traditional combat units on ships, air wings, and on the ground. Because of both the legal authorities of their positions and the physical risk of many of their duties, military cyber personnel have different requirements to serve than do members of the federal civilian workforce, and they often attract different recruits.

Indeed, bringing these individuals into the armed forces can be even more difficult than the already challenging process of hiring cyber talent into the civilian workforce. Military personnel must meet physiological requirements—whether physical fitness tests or baseline health assessments. Military services normally require candidates to go through military entrance processing stations and then complete basic military training. Top cybersecurity professionals with asthma, certain dental implants, joint deformities (scoliosis), or problems with foot pronation may not be medically qualified to serve in the armed forces; nor would those who have suffered from depression within the past three years or have allergic reactions to fish, insects, or nuts. The number of individuals medically disqualified is not inconsequential. Joe Schuman notes that "in 2012, according to the Department of Defense's Accession Medical Standards Analysis & Research Activity (AMSARA) Annual Report, 38,000 of 200,000 active duty applicants (or 19 percent) across all military services were medically disqualified from service."[109]

Medical disqualifications are not the only challenge. More than two-thirds of American youth would be disqualified from military service of any kind because of their failure to meet educational, behavioral, or physical standards.[110] Each layer of requirements, including physical fitness and body shape, narrows the pool of potential talent. In cyber roles, however, issues like obesity have less impact on effectiveness than in other areas of warfighting. Further, the hierarchical and longevity-based promotion structures of military organizations mean that almost all individuals—regardless of talent or expertise—must start their military careers at the lowest ranks. This makes it difficult to recruit mid-level or senior talent into military positions.[111] To that end, the recruitment and professional development of cyber talent may benefit from emulating the practices of the military's legal, medical, and certain engineering career tracks, which make reasonable accommodations for physiological deficiencies that do not preclude useful career service and employ waivers for entry at more senior ranks.[112] To further address recruitment challenges, the services have begun to explore direct commission options to provide greater flexibility.[113] Similar flexibility in the enlisted ranks would further expand cyber recruitment.

Recruiting and retaining this small pool of talent are uphill battles for DoD. It is easy to blame differences in the pay of military and civilian cybersecurity professionals, but surveys suggest that many top technologists are willing to sacrifice compensation for work satisfaction. While DoD can offer meaningful missions and often opportunities to work on technologies not accessible to civilians, it has a long way to go to create a satisfying work environment. Service members, who are salaried, often spend 10 to 12 hours a day on their missions and are asked to perform extended temporary additional duty and remote deployments. On top of their mission requirements, service members are asked to deal with an unwieldy bureaucracy, including an overly complicated Defense Travel System, human resources applications that are often inaccessible from standard internet browsers, and time-consuming computer-based training that functions more as a risk mitigator than a skill enhancer. Often these applications are parochial DoD technology, making it less likely that skills are transferable between civilian technology and DoD-built and DoD-administered systems.

In addition, the accessions and promotion system for deep technical skills like those critical to cybersecurity missions struggles with nontraditional candidates and provides little flexibility for career progression—a major disincentive for younger candidates. The National Defense Authorization Act for Fiscal Year 2019 did make some improvements to enhance career progression issues, allowing service credit for training or experience gained in the private sector. This change provided authorities—similar to those that allow the accession of more senior medical and dental officers—to be used on other critical skills, such as cybersecurity.[114] In the two years since this has passed, the services have only recently (and lightly) embraced this provision's use for cyber accessions.[115] Such measures are intended to help address barriers in bringing in and keeping technology talent; however, the military lifestyle itself can be a challenge for retaining individuals with cyber knowledge and experience. The traditional military family life, which calls on members and their families to move to new stations every one to three years, poses significant challenges for dual-career couples, who are common among high-technology talent. Also, unlike many of the major technology firms, which have prioritized family services, DoD does not have sufficient high-quality child care at all military installations (and is especially short of care that covers the extended hours of duty days).[116]

To tackle this particular challenge, DoD will need to undertake further cultural, organizational, and technological changes that will go beyond cyber talent and extend across its military workforce. From promotion to training, technology for administrative support, family care, and physical fitness requirements, the best way to solve the cyber talent gap within the armed forces is to continue to evolve how DoD approaches manpower.[117] The solutions to these problems within the active duty force will be pivotal to solving the military cyber talent needs identified by the Commission, but they have ramifications throughout the entire armed services. Therefore, while the Commission stops short of recommending major service-wide overhauls in readiness standards, promotion procedures, or family care options, it recognizes that without these reforms to the military personnel system, it will be hard for the U.S. military to compete and to retain sufficient cyber talent.

Military Cyber Reserve. Though the issues highlighted for the entire military cyber force may require changes broader than the scope of the Commission, Congress can take some first steps to experiment with military manpower support to cyber operations. In particular, the Commission recommends an examination of the military reserve's cyber forces as an alternative and more flexible model for cyber talent within the armed forces. Because these reserve forces are often employed in the civilian sector, they benefit from cutting-edge training and experience. The reserve also offers more flexible options for personnel who want to serve but are looking for short-term or part-time alternatives to active duty service.

As it examined the reserve as a talent solution, however, the Commission identified some reservations about the current use of the reserve as a way to fill the talent gap. First, employers in private-sector critical infrastructure have expressed concern that reliance on a military cyber reserve might mean that they lose a portion of their cyber talent—reservists who get called up—during periods of instability or risk when those employees are needed most. Such impacts would be limited, because reservists make up a relatively small portion of private-sector workforces. In particular, private-sector employers are able to hire talented individuals who are ineligible or disinclined to pursue security clearances. Nevertheless, before mobilizing the reserve, decision makers certainly must consider any impacts on the private-sector critical infrastructure.

A second concern stems from the attractiveness of the reserve to nontraditional candidates. Over the past 15 years, the reserve and the National Guard force have experienced operational deployment cycles similar to that of the active component. While that has solved many of the difficulties of fighting multiple wars with an all-volunteer active duty force, it has also made the Reserves and National Guard potentially less useful for attracting nontraditional talent. This creates a challenge for using the Reserves to reduce the U.S. military's cyber talent gap.

To address these issues, the Commission recommends that Congress request an assessment from DoD on the need for and requirements of a military cyber reserve, including its possible composition and structure (Recommendation 6.1.7). This assessment may help DoD in preparing to mobilize a surge capacity in times of crisis or conflict, but it should also explore new uses of the military reserve to respond to time-specific needs or to hold on to future talent. For example, a strategic cyber reserve might be developed that maintains nontraditional cyber talent in true reserve and allows individuals to serve in specific, limited projects or situations, rather than on recurring weekends or two week activations, when necessary and as the talents of strategic reserve members allow. Congress should therefore explore in this assessment both the current use of the military reserves to support existing cyber initiatives and possible future changes to the reserve force. Among the changes to consider is the expansion of the Individual Ready Reserve, as recommended by the National Commission on Military, National, and Public Service.[118] The assessment should also include current initiatives within Defense Innovation Unit and AFWERX—which is an Air Force innovation effort, not an acronym—to retool Category (CAT) "E" Reservist programs.[119] The Cat-E program allows civilians who are employed full-time to participate in military programs like the Civil Air Patrol Reserve.[120] Using these programs, the military can create a bullpen of talent ready to partner with active duty units via technological applications that match reservists with funded projects. While many of these initiatives are unique to a particular service, the Commission recommends that the military cyber reserve study find best practices across the services, find ways in which the services can share technology or lessons learned, and ultimately tailor each service's cyber reserve force to its specific missions.

Title 10 Professors. To ensure that the United States continues to possess the world's most effective fighting force, the next generation of military leaders must be educated on cyber issues.[121] Cyber security and information operations are central to military planning and guidance and will only grow in importance in the future. The Commission therefore recommends the establishment of Title 10 professors specializing in cyber at the Professional Military Education (PME) institutions. within each service branch and at the National Defense University, to communicate how cyber strategy, policy, and operations affect the armed forces (Recommendation 6.1.8). These professors would be responsible for establishing and implementing the curricula for both cyber and information warfare national strategy at the Command, Staff, and Planners Colleges of each service branch. These professors would play a crucial role in institutionalizing and coordinating cyber and information warfare education across each service branch, including through distance education. Responding to the evolution of the character of war requires the United States to expand and change its PME institutions and the education available to its students in order to meet the challenge of operating in the information and cyber domains.

D. CONCLUSION

For the federal government, having the structures in place to create and implement a cyber workforce development strategy is critical. While numerous individual efforts have emerged across the federal government to address various pieces of the workforce challenge, there is limited coordination between them. Without a clear plan to distribute resources and designate responsibilities—and meaningfully hold departments and agencies to account for their commitments on cyber workforce improvements—progress will remain dangerously slow. This paper lays out five elements to guide development of a federal cyber workforce strategy.

First, federal departments and agencies must have flexible tools to ***organize*** and manage their workforce that can adapt to each organization's individual mission while also providing coherence across the entirety of the federal government. To appropriately organize the federal cyber workforce, the CSC recommends **properly identifying and utilizing cyber-specific occupational classifications** to allow more tailored workforce policies, **building a federal cyber service** to provide clear and agile hiring authorities and other personnel management tools, and **establishing coordination structures** to provide clear leadership for federal workforce development efforts.

Second, federal leaders must improve tools to ***recruit*** new talent, in particular by focusing on the programs that make public service an attractive prospect to talented individuals. In many ways, the federal government's greatest tool for recruitment is the mission and unique learning opportunities inherent in federal work. To capitalize on these advantages, the government should invest in existing programs such as **CyberCorps: Scholarship for Service** and **the Centers of Academic Excellence**, while also working to mitigate recruitment barriers that stem from the **personnel security clearance process**.

Third, the federal government must provide opportunities to ***develop*** the cyber workforce. The federal government, like all cyber employers, cannot expect every new employee to have hands-on experience, a four-year degree, and a list of industry certifications. Rather, the federal government will be stronger if it draws from a broad array of educational backgrounds and creates opportunities for employees to gain knowledge and experience as they work. This effort will call for many innovative approaches, among which the Commission particularly recommends **apprenticeship programs** and **upskilling opportunities** to support cyber employee development.

Fourth, a federal cyber workforce strategy must help ***retain*** existing talent, though leaders should take a nuanced view of retention, recognizing that enabling talent to move flexibly between the public and private sectors enables a stronger cyber workforce overall. However, federal employers can take steps to encourage their employees to increase the time they spend in public service. Improving **pay flexibility** is a major consideration, but continuing the development of **career pathways** and providing interesting career development opportunities like **rotational and exchange programs** also can be critical. Of particular note, federal employers can increase retention of underrepresented groups through the **removal of inequities** and barriers to advancement in the workplace.

Fifth, the federal government cannot simply recruit a larger share of the existing national talent pool. Rather, leaders must take steps to ***stimulate growth*** in the talent pool itself in order to increase the numbers of those available for federal jobs. To promote growth of the talent pool nationwide, the federal government must first **coordinate government efforts** working toward this goal. Executive branch and congressional leaders should also invest in measures to **promote diversity** across the national workforce and **incentivize research** to provide a greater empirical understanding of cyber workforce dynamics. Finally, federal leaders must work to **increase the military cyber workforce**, which has a significant impact on the national cyber workforce because it serves as both a source and an employer of cyber talent.

By following the structure laid out here to **organize**, **recruit**, **develop**, and **retain** a federal cyber workforce and **stimulate growth** throughout the national and military cyber workforce, the federal government can begin to lay the groundwork for an effective cyber workforce development strategy to grow its own workforce and the pool of talent from which it recruits. While they are by no means the entirety of what is required, the actions recommended here as a part of this structure can serve as examples of the types of changes needed, and can begin to drive progress toward a strategy for ensuring that the cyber workforce is equipped to serve its critical national security role.

The cyber workforce is the very foundation upon which cybersecurity is built. If the United States cannot find a way to bolster that foundation, American security and prosperity in cyberspace will become increasingly precarious. Such insecurity is unacceptable, especially as the country continues to move businesses and daily life onto digital platforms. However, with ongoing investment, sustained political will, and a clear strategy, the federal government can drive meaningful change by filling cyber jobs, whether in the federal government, the military, or the nation as a whole.

NOTES

[1] U.S. Cyberspace Solarium Commission, "Joint Letter by the Cyberspace Solarium Commission, National Security Commission on Artificial Intelligence, and the National Commission on Military, National, and Public Service to the Senate and House Armed Services Committees on National Security Workforce Recommendations," Press Release, May 7, 2020, https://www.solarium.gov/public-communications/joint-commission-workforce-letter.

[2] As of publication, the public sector has 31,669 cybersecurity job openings, and a total employed cybersecurity workforce of 52,273. See "Cybersecurity Supply/Demand Heat Map," CyberSeek, accessed August 20, 2020, https://www.cyberseek.org/heatmap.html.

[3] "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce" (Partnership for Public Service and Booz Allen Hamilton, July 2009), 19, https://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In-Security__Strengthening_the_Federal_Cybersecurity_Workforce-2009.07.22.pdf.

[4] "Cybersecurity Supply/Demand Heat Map," CyberSeek, accessed August 20, 2020, https://www.cyberseek.org/heatmap.html.

[5] "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce."

[6] At the direction of Office of Management and Budget Memorandum M-16-04, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government," the Obama administration set into motion planning for a cyber workforce strategy would "identify possible actions . . . to help the Federal Government recruit, develop, and maintain a pipeline of cybersecurity talent." In part because of its timing, this effort has had little meaningful impact as a strategy in driving federal workforce efforts. The Office of Management and Budget notes, "There are a number of existing Federal initiatives to address this challenge, but implementation and awareness of these programs are inconsistent." Accordingly, the strategy lists a number of governmentwide efforts and the organizational homes for those individual efforts, but it does not describe any leadership or coordination structure for the collection of efforts as a whole to drive implementation or support ongoing awareness of these initiatives. See Shaun Donovan, Beth F. Cobert, and Tony Scott to Heads of Executive Departments and Agencies, July 12, 2016, Executive Office of the President, Office of Management and Budget, "Federal Cybersecurity Workforce Strategy," 3, 2, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-15.pdf. The Department of Defense Chief Information Officer did address the workforce in their cyber strategy, which pertains only to DoD. See "Cyber Workforce Strategies," Chief Information Officer, U.S. Department of Defense, https://dodcio.defense.gov/Cyber-Workforce/CWS.aspx.

[7] "Cybersecurity Enhancement Act of 2014," Pub. L. No. 113-274, 15 U.S.C. § 7421 (2014).

[8] "Consolidated Appropriations Act, 2016," Pub. L. No. 114–113, 5 U.S.C. § 301 (2016); https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf.

[9] The White House, "Executive Order on America's Cybersecurity Workforce" (May 2, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/.

[10] NICE was authorized in the 2014 Cybersecurity Enhancement Act but originally created in 2010.

[11] U.S. Cyberspace Solarium Commission, *Report of the United States of America Cyberspace Solarium Commission* (March 2020), https://www.solarium.gov/home.

[12] "Cybersecurity Supply/Demand Heat Map" (accessed August 20, 2020).

[13] U.S. Cyberspace Solarium Commission, *Report of the United States of America Cyberspace Solarium Commission*.

[14] For more information, see "NICE Cybersecurity Workforce Framework Resource Center," National Institute of Standards and Technology, accessed July 7, 2020, https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center; U.S. Government Accountability Office, "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs" (March 2019), https://www.gao.gov/assets/700/697462.pdf.

[15] Aspen Cybersecurity Group, "Principles for Growing and Sustaining the Nation's Cybersecurity Workforce" (The Aspen Institute, November 2018), 7, https://assets.aspeninstitute.org/content/uploads/2018/11/Aspen-Cybersecurity-Group-Principles-for-Growing-and-Sustaining-the-Nations-Cybersecurity-Workforce-1.pdf.

[16] For details on the Commission's recommendation for a National Cyber Director, see "Hearing on U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act, before the Committee on Oversight and Reform," 116th Congress (2020) (testimony of James R. Langevin, Mike Gallagher, Michael J. Rogers, J. Michael Daniel, Amit Yoran, Suzanne Spaulding, and Jamil N. Jaffer), https://oversight.house.gov/legislation/hearings/hr-7331-the-national-cyber-director-act-1.

[17] For more on shaping the cyber ecosystem to improve security, see Pillar Four of the Cyberspace Solarium Commission Report: U.S. Cyberspace Solarium Commission, *Report of the United States of America Cyberspace Solarium Commission*, 71–95.

[18] Mark D. Reinhold, Associate Director, Employee Services, OPM, to Human Resources Directors, April 2, 2018,"Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need," https://chcoc.gov/content/guidance-identifying-addressing-and-reporting-cybersecurity-work-roles-critical-need; National Institute of Standards and Technology, "Federal Cybersecurity Coding Structure," October 18, 2017, Version 2.0, https://www.nist.gov/file/394236.

[19] GAO, "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs, 10.

[20] U.S. Office of Personnel Management, "Introduction to the Position Classification Standards" (rev.August 2009), https://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/positionclassificationintro.pdf.

[21] The definition of cybersecurity work used by OPM to delineate these positions is taken from the NICE Framework: "Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure." See U.S. Office of Personnel Management, "Interpretive Guidance for Cybersecurity Positions: Attracting, Hiring and Retaining a Federal Cybersecurity Workforce" (October 11, 2018), 6, https://www.opm.gov/policy-data-oversight/classification-qualifications/reference-materials/interpretive-guidance-for-cybersecurity-positions.pdf.

[22] U.S. Government Accountability Office, "Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions" (June 2018), https://www.gao.gov/assets/700/692498.pdf.

[23] GAO, "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs," Highlights. The "non-IT" code referenced is "000," used to indicate a position that "[d]oes NOT involve work functions in information technology (IT), cybersecurity, or cyber-related areas." See NIST, "Federal Cybersecurity Coding Structure," 11.

[24] In addition to written interpretive guidance from 2017 and 2018, OPM has been engaged in outreach on these topics. For example, see the series of informational webinars on cyber workforce topics: Office of Personnel Management "Federal Cybersecurity Workforce Four-Part Webinar Series," Eventbrite, https://www.eventbrite.com/e/federal-cybersecurity-workforce-four-part-webinar-series-registration-109857843768.

[25] Jim H. Crumpacker to Gregory C. Wilshusen, February 13, 2019, Appendix X in GAO, "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs,"65.

[26] NIST, "Federal Cybersecurity Coding Structure," 6.

[27] Kathryn A. Francis and Wendy Ginsberg, "The Federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security," Congressional Research Service (January 8, 2016), https://fas.org/sgp/crs/natsec/R44338.pdf.

[28] Chase Gunter, "OPM Issues Final Rule on Direct-Hire for Cyber," *FCW* (April 3, 2019), https://fcw.com/articles/2019/04/03/opm-direct-hire-authority.aspx; Office of Personnel Management, "Rules and Regulations, 5 CFR Part 337," *Federal Register* 84, no. 64 (April 3, 2019): 12873, https://www.govinfo.gov/content/pkg/FR-2019-04-03/pdf/2019-06396.pdf.

[29] "Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals," 20, https://www.opm.gov/policy-data-oversight/pay-leave/reference-materials/handbooks/compensation-flexibilities-to-recruit-and-retain-cybersecurity-professionals.pdf.

[30] Certain flexibilities are also available to specific positions in the occupational series that encompass computer engineers, computer scientists, and electrical engineers. See "Hiring Information: Direct Hire Authority," OPM.gov, https://www.opm.gov/policy-data-oversight/hiring-information/direct-hire-authority/#url=Governmentwide-Authority.

31 Crumpacker to Wilshusen, in "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs," 65.

32 "DoD Cyber Workforce Framework," DoD Cyber Exchange Public, https://public.cyber.mil/cw/dcwf/.

33 "NICE Framework Draft Revision," National Institute for Standards and Technology (July 22, 2020), https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-draft-revision.

34 "DoD Cyber Excepted Service (CES) Personnel System," Chief Information Officer, U.S. Department of Defense, accessed July 1, 2020, https://dodcio.defense.gov/Cyber-Workforce/CES.aspx.

35 Leslie Weinstein, "Cyber Excepted Service: Bolstering DoD's Cyber Workforce," *Federal News Network*, November 27, 2019, https://federalnewsnetwork.com/commentary/2019/11/cyber-excepted-service-bolstering-dods-cyber-workforce/.

36 Jordan Smith, "DHS Seeks Feedback on Cyber Talent Personnel System," *MeriTalk*, December 2, 2019, https://www.meritalk.com/articles/dhs-seeks-feedback-on-cyber-talent-personnel-system/.

37 Smith, "DHS Seeks Feedback on Cyber Talent Personnel System."

38 Joe Heck and John C. "Chris" Inglis, "Creating a More Secure Nation Means Public Service Hiring Practices Need an Overhaul," *The Hill*, July 18, 2020, https://thehill.com/blogs/congress-blog/politics/507954-creating-a-more-secure-nation-means-public-service-hiring.

39 "CyberCorps: Scholarship for Service," Office of Personnel Management, accessed July 7, 2020, https://www.sfs.opm.gov/default.aspx.

40 "CyberCorps: Scholarship for Service, Overview," Office of Personnel Management, accessed August 4, 2020, https://www.sfs.opm.gov/ProspectiveStud.aspx; "CyberCorps: Scholarship for Service, Students: Participating Institutions," Office of Personnel Management, accessed August 4, 2020, https://www.sfs.opm.gov/ContactsPI.aspx.

41 "Community College Cyber Pilot Program (C3P)," National Science Foundation, Division of Graduate Education, https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505573.

42 More specifically, CyberCorps SFS is projected to graduate 380 students in 2020. It graduated 307 students in 2019, 324 in 2018, 290 in 2017, 245 in 2016, and 211 in 2015. Data provided by NSF.

43 OPM, "CyberCorps: Scholarship for Service: History/Overview." At the time of access, the data cited was available at https://www.sfs.opm.gov/Overview-History.aspx; it now can be found at https://web.archive.org/web/20200608183458/https://www.sfs.opm.gov/Overview-History.aspx and https://www.nass.org/sites/default/files/2019%20Summer/presentations/presentation-sfs-summer19.pdf.

44 In fact, legislation has been proposed for inclusion in S.4049, the National Defense Authorization Act for Fiscal Year 2021, explicitly permitting up to 10 percent of SFS graduates to fulfill their service obligation in education roles in higher education institutions that participate in the SFS program.

45 "National Centers of Academic Excellence," National Security Agency Central Security Service, https://www.nsa.gov/resources/students-educators/centers-academic-excellence/.

46 "Centers of Academic Excellence in Cybersecurity: What Is a CAE?," CAE in Cybersecurity Community, accessed July 7, 2020, https://www.caecommunity.org/content/what-is-a-cae.

47 National Security Agency and Department of Homeland Security, *Celebrating 20 Years with the Centers of Academic Excellence in Cyber Defense* (2019), 3, accessed July 7, 2020, https://www.caecommunity.org/sites/default/files/CAE_Book_Version_1.6-2.pdf.

48 U.S. Government Accountability Office, "High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas" (March 2019), Highlights, https://www.gao.gov/assets/700/697245.pdf.

49 United States Cyberspace Solarium Commission, *Legislative Proposals* (July 2020), https://www.solarium.gov/report/legislative-proposals.

50 Jack Corrigan, "The Pentagon Has Officially Taken Over the Security Clearance Process," NextGov (October 1, 2019), https://www.nextgov.com/cio-briefing/2019/10/pentagon-has-officially-taken-over-security-clearance-process/160294/.

51 Aaron Boyd, "The Security Clearance Process Is About to Get Its Biggest Overhaul in 50 Years," Nextgov (February 28, 2019), https://www.nextgov.com/cio-briefing/2019/02/security-clearance-process-about-get-its-biggest-overhaul-50-years/155229/.

52 Lauren C. Williams, "Why the Cyber Fast Track Is Stalled at DOD," *FCW* (February 26, 2019), https://fcw.com/articles/2019/02/26/dod-it-oversight-williams.aspx.

53 Boyd, "The Security Clearance Process Is About to Get Its Biggest Overhaul in 50 Years."

54 Daniel R. Coats, "Reciprocity of Background Investigations and National Security Adjudications," Security Executive Agent Directive 7, Office of the Director of National Intelligence (November 9, 2018), 3, https://fas.org/sgp/othergov/intel/sead-7.pdf.

55 Charlie Allen, "The Process for Security Clearance Reciprocity Needs to Change," WorkScoop (December 17, 2019), https://workscoop.com/2019/12/17/security-clearance-reciprocity-charlie-allen-insa.

56 "State of Cybersecurity 2019, Part 1: Current Trends in Workforce Development," ISACA (2019), https://www.isaca.org/bookstore/state-of-cybersecurity-2019/whpsc191.

57 Digest of Education Statistics, "Table 325.35. Degrees in Computer and Information Sciences Conferred by Postsecondary Institutions, by Level of Degree and Sex of Student: 1970–71 through 2016–17," National Center for Education Statistics (September 2018), https://nces.ed.gov/programs/digest/d18/tables/dt18_325.35.asp.

58 "Cybersecurity Supply/Demand Heat Map," accessed August 20, 2020.

59 Aspen Cybersecurity Group, "Principles for Growing and Sustaining the Nation's Cybersecurity Workforce," 5.

60 About half of states register their own apprenticeship programs. The rest work through the federal Department of Labor. All such programs, however they are registered, are part of the national system of Registered Apprenticeship. See "State Apprenticeship Agencies," Department of Labor, Employment and Training Administration, https://www.dol.gov/agencies/eta/apprenticeship/contact/state-agencies.

61 For more on portable credentialing, see Deborah Everhart, Evelyn Ganzglass, Carla Casilli, Daniel Hickey, and Brandon Muramatsu, *Quality Dimensions for Connected Credentials* (American Council on Education, 2016), https://www.acenet.edu/Documents/Quality-Dimensions-for-Connected-Credentials.pdf.

62 ISACA, "State of Cybersecurity 2020, Part 1: Global Update on Workforce Efforts and Resources."

63 "Salary Table 2020-DCB," Office of Personnel Management, January 2020, https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2020/DCB.pdf.

64 "Cyber Forensics Analyst in Washington, District of Columbia," Salary.com, accessed August 4, 2020, https://www.salary.com/tools/salary-calculator/cyber-forensics-analyst/washington-dc?edu=EDLEV3. More information on the average offers in federal government based on existing hiring authorities and pay flexibilities would make possible a more accurate comparison. The comparison is also contingent on Salary.com's methodology. Given the importance of this question, developing better and more authoritative data on these points is critically important, as discussed in a later section, "Incentivize Empirical Research to Identify a Baseline and Measure Success."

65 "Cyber Excepted Service: Frequently Asked Questions (FAQs)," U.S. Department of Defense Defense Civilian Personnel Advisory Service, January 2018, 3, https://dl.dod.cyber.mil/wp-content/uploads/dces/pdf/GeneralCESFAQs.pdf. The standard federal personnel system—the General Schedule (GS)—is divided by "grades" and "steps," and each increase in step corresponds to an increase in pay. Conventionally, each grade has 10 steps; thus, a particular individual might be a GS-14, step 10. If this GS-14, step 10, individual cannot be promoted to GS-15 for whatever reason, under CES they could be moved to a step 11 or step 12, to allow additional pay increases.

66 ISACA, "State of Cybersecurity 2020, Part 1: Global Update on Workforce Efforts and Resources."

67 National Initiative for Cybersecurity Careers and Studies, "Cyber Career Pathways Tool," Cybersecurity and Infrastructure Security Agency, Department of Defense, and the Department of Veterans Affairs, https://niccs.us-cert.gov/workforce-development/cyber-career-pathways?core=1; Megan Caposell, Chris Paris, and Matt Isnor, "Interagency Federal Cyber Career Pathways Initiative" (presentation, National Initiative for Cybersecurity Education Annual Conference, Phoenix, AZ, November 18–20, 2019), https://niceconference.org/uploads/2019/InteragencyFederalCyberCareerPathwaysInitiative.pdf.

68 The White House, "Executive Order on America's Cybersecurity Workforce."

69 "Cyber Information Technology Exchange Program (CITEP)," Chief Information Officer, U.S. Department of Defense, https://dodcio.defense.gov/Cyber-Workforce/CITEP/; "Exemplar," Department of Homeland Security (updated July 15, 2020), https://www.dhs.gov/exemplar.

70 Chief Information Officer, DoD, "Cyber Information Technology Exchange Program (CITEP)."

71 For example, see "Exchanges: Academic Visitors/Visiting Researchers," Idaho National Laboratory, https://inl.gov/inl-initiatives/education/university-exchanges/.

72 For example, the Center for Long-Term Cybersecurity at the University of California, Berkeley, proposes a cyber workforce incubator as a "way to get top West Coast technologists focused on critical mission work." See Jesse Goldhammer, Steve Weber, and Betsy Cooper, *Cyber Workforce Incubator* (Berkeley: Center for Long Term Cybersecurity, April 6, 2017), 2, https://cltc.berkeley.edu/wp-content/uploads/2017/04/Cyber-Workforce-Incubator.pdf.

73 Scott E. Page, *The Difference: How the Power of Diversity Creates Better Groups, Firms, Schools, and Societies* (Princeton: Princeton University Press, 2007); Cristian L. Dezsö and David Gaddis Ross, "Does Female Representation in Top Management Improve Firm Performance? A Panel Data Investigation" (March 9, 2011), Robert H. Smith School Research Paper No. RHS 06-104, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1088182; Margaret McDonagh and Lorna Fitzsimons, "Women Count 2020: Role, Value, and Number of Female Executives in the FTSE 350" (The Pipeline, 2020), https://www.execpipeline.com/wp-content/uploads/2020/07/The-Pipeline-Women-Count-2020-FINAL-VERSION.pdf.

74 Rachel Thomas et al., "Women in the Workplace: 2019" (McKinsey & Company and LeanIn.Org), esp. 10–18, https://wiw-report.s3.amazonaws.com/Women_in_the_Workplace_2019.pdf.

75 "Innovation through Inclusion: The Multicultural Cybersecurity Workforce" (Frost & Sullivan, 2018), 3–4, https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx.

76 "Women in Cybersecurity: Young, Educated and Ready to Take Charge" ((ISC)², 2019), 5–6, https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx.

77 Thomas et al., "Women in the Workplace: 2019." This research examined gender diversity across industries; while some of the conclusions that apply to improving gender diversity can be generalized more broadly, the Commission recognizes that different underrepresented demographic groups also face different challenges.

78 Trish Stroman, Wendy Woods, Gabrielle Fitzgerald, Shalini Unnikrishnan, and Liz Bird, "Why Paid Family Leave Is Good Business" (Boston Consulting Group, February 2017), 13, http://media-publications.bcg.com/BCG-Why-Paid-Family-Leave-Is-Good-Business-Feb-2017.pdf.

79 National Initiative for Cybersecurity Education, "Strategic Plan," National Institute of Standards and Technology (updated November 2019), https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan.

80 "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce."

81 "Cyber In-Security II: Closing the Federal Talent Gap" (Partnership for Public Service and Booz Allen Hamilton, April 2015), 2, https://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In-Security_II__Closing_the_Federal_Talent_Gap-2015.04.13.pdf.

82 Robert D. Austin and Gary P. Pisano, "Neurodiversity as a Competitive Advantage," *Harvard Business Review* 95, no. 3 (May–June 2017): 96–103, https://hbr.org/2017/05/neurodiversity-as-a-competitive-advantage.

83 David Rock and Heidi Grant, "Why Diverse Teams Are Smarter," *Harvard Business Review*, November 4, 2016, https://hbr.org/2016/11/why-diverse-teams-are-smarter?referral=00563.

84 Lu Hong and Scott E. Page, "Groups of Diverse Problem Solvers Can Outperform Groups of High-Ability Problem Solvers," *Proceedings of the National Academy of Sciences* 101, no. 46 (November 16, 2004): 16385–89, https://sites.lsa.umich.edu/scottepage/wp-content/uploads/sites/344/2015/11/pnas.pdf.

85 Oscar Williams, "Is Autism an Asset to UK Cyber Security?" *New Statesman*, October 19, 2018, https://www.newstatesman.com/spotlight/cyber/2018/10/autism-asset-uk-cyber-security.

86 Robert D. Austin, Michael Fieldhouse, Aiyaswami Mohan, and Peter Quinn, "Why the Australian Defence Organization Is Recruiting Cyber Analysts on the Autism Spectrum," *Harvard Business Review,* December 7, 2017, https://hbr.org/2017/12/why-the-australian-defence-organization-is-recruiting-cyber-analysts-on-the-autism-spectrum.

87 Vincent Wood, "GCHQ Targeting Dyslexic and Neurodiverse People in Recruitment Drive, Spy Chief Says," *Independent*, October, 21, 2019, https://www.independent.co.uk/news/uk/home-news/gchq-jobs-recruitment-intelligence-spy-jeremy-fleming-dyslexia-disability-neurodiversity-a9163996.html.

88 Robert D. Austin and Gary P. Pisano, "Neurodiversity as a Competitive Advantage," *Harvard Business Review* 95, no. 3 (May–June 2017): 96–103, https://hbr.org/2017/05/neurodiversity-as-a-competitive-advantage.

89 For 11 percent, see "The 2017 Global Information Security Workforce Study: Women in Cybersecurity" (Frost & Sullivan, 2017), 6, https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2019/01/women-cybersecurity-11-percent.pdf; for 24 percent, see (ISC)², "Women in Cybersecurity: Young, Educated and Ready to Take Charge," 3. Few studies have examined the demographics of the cyber workforce, whether in government, in the nation, or in the world, and their results vary significantly; it is thus almost impossible to independently verify findings or identify a baseline for longitudinal research. This is one of the gaps that a later section, "Incentivize Empirical Research to Identify a Baseline and Measure Success," aims to address.

90 "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future," U.S. Department of Commerce and U.S. Department of Homeland Security (November 16, 2017), 19, https://www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf.

91 "Inspiring the Next Generation of Cyber Stars: About," GenCyber, https://www.gen-cyber.com/about/.

92 "Code with Google," Google, https://edu.google.com/code-with-google/?modal_active=none&story-card_activeEl=enhance-any-subject.

93 Prem Uppuluri and Joseph Chase, "Introduction to Cybersecurity for High School Students and K12 Educators," Virginia Cyber Range, https://www.virginiacyberrange.org/courseware/introduction-cybersecurity-high-school-students-and-k12-educators.

94 EdWeek Research Center, "The State of Cybersecurity Education in K-12 Schools: The Results of a National Survey" (CYBER.ORG, June 23, 2020), 3, available at https://cyber.org/news/state-cybersecurity-education-k-12-schools.

95 "Our Impact," CYBER.ORG, https://cyber.org/about-us/our-impact.

96 Digest of Education Statistics, "Table 208.20. Public and Private Elementary and Secondary Teachers, Enrollment, Pupil/Teacher Ratios, and New Teacher Hires: Selected Years, Fall 1955 through Fall 2028," National Center for Education Statistics (December 2019), https://nces.ed.gov/programs/digest/d19/tables/dt19_208.20.asp.

97 Douglas A. Levin, "The State of K-12 Cybersecurity: 2019 Year in Review, Part III: Cybersecurity Incidents: 2019"(EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center, 2020), https://k12cybersecure.com/year-in-review/2019-incidents/.

98 Douglas A. Levin, "The State of K-12 Cybersecurity: 2019 Year in Review, Part I: Introduction" (EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center, 2020), https://k12cybersecure.com/year-in-review/2019-intro/.

99 Paula Maylahn, "The State of Ed Tech Leadership in 2020*"* (CoSN, 2020), 4, https://www.ed-fi.org/assets/2020/05/CoSN_EdTechLeadership_2020.pdf.

100 Maylahn, "The State of Ed Tech Leadership in 2020," 15, 16.

101 Betsy Foresman, "Ed. Dept., Educause Partner to Promote Cybersecurity Collaboration," EdScoop (December 17, 2019), https://edscoop.com/education-department-educause-cybersecurity-information-sharing/.

102 Davey Alba and Adam Satariano, "At Least 70 Countries Have Had Disinformation Campaigns, Study Finds," *New York Times,* September 26, 2019, https://www.nytimes.com/2019/09/26/technology/government-disinformation-cyber-troops.html.

103 Suzanne Spaulding, Devi Nair, and Arthur Nelson, *Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System* (Center for Strategic and International Studies, May 2019), available at https://www.csis.org/analysis/beyond-ballot-how-kremlin-works-undermine-us-justice-system.

104 William Crumpler and James A. Lewis, "The Cybersecurity Workforce Gap" (Center for Strategic and International Studies, 2019), 2–5, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf.

105 Department of Commerce and Department of Homeland Security, "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce," 15; Tim Herbert, Matt Loeb, Will Markow, and Debbie Sagen (moderator, Adam Sedgewick), "Workshop on Cybersecurity Workforce Development: Panel 1" (National Institute of Standards and Technology and the Department of Homeland Security, Chicago, August 2, 2017), https://www.nist.gov/news-events/events/2017/08/workshop-cybersecurity-workforce-development.

106 Crumpler and Lewis, "The Cybersecurity Workforce Gap," 4–5.

107 For an example, see "Citizen Clinic," University of California, Berkeley, Center for Long-Term Cybersecurity, https://cltc.berkeley.edu/about-us/citizen-clinic/.

108 The White House, "National Cyber Strategy of the United States of America" (September 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; U.S. Department of Defense, "Summary: Department of Defense Cyber Strategy" (2018), 1, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

109 Joe Schuman, "Department of Disqualified: Fixing the Broken Military Medical Accessions Process," *War on the Rocks*, November 20, 2018, https://warontherocks.com/2018/11/department-of-disqualified-fixing-the-broken-military-medical-accessions-process/.

110 Miriam Jordan, "Recruits' Ineligibility Tests the Military: More Than Two-Thirds of American Youth Wouldn't Qualify for Service, Pentagon Says," *Wall Street Journal*, June 27, 2014, https://www.wsj.com/articles/recruits-ineligibility-tests-the-military-1403909945?mod=e2tw.

111 Though in the military services there is some precedent for giving waivers in such circumstances.

112 A similar concept underpins the change allowing the military to retain older talent as needed. See John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 [FY2019 NDAA], § 506, 132 Stat. 1636 (2018).

113 Nina Kollars and Emma Moore, "Every Marine a Blue-Haired Quasi-Rifleperson?" *War on the Rocks*, August 21, 2019, https://warontherocks.com/2019/08/every-marine-a-blue-haired-quasi-rifleperson/.

114 See FY2019 NDAA, §§ 502.

115 Kyle Rempfer, "Direct Commissions for Army Cyber Officers Finally Gaining Steam, Two-Star Says," *Army Times,* August 17, 2020, https://www.armytimes.com/news/your-army/2020/08/17/direct-commissions-for-army-cyber-officers-finally-gaining-steam-two-star-says/.

116 Some bases are extending to 14-hour coverage, but shifts can fall outside of even those hours. See Karen Jowers, "More Bases Offering Extended Child Care Hours," *Military Times, October 6, 2017*, https://www.militarytimes.com/pay-benefits/2017/10/06/more-bases-offering-extended-child-care-hours/.

117 For further discussion of these issues, see Jacquelyn Schneider, "Blue Hair in the Grey Zone," *War on the Rocks*, January 10, 2018, https://warontherocks.com/2018/01/blue-hair-gray-zone/.

118 National Commission on Military, National, and Public Service, *Inspire to Serve: The Final Report of the National Commission on Military, National, and Public Service* (March 2020), 104–5, available at https://inspire2serve.gov/reports.

119 "AFWERX," U.S. Air Force, https://www.afwerx.af.mil/.

120 Timm Huffman, "Flexible Reserve Opportunities Supporting Air Force Auxiliary," Air Force Reserve Command (March 21, 2017), https://www.afrc.af.mil/News/Article-Display/Article/1125084/flexible-reserve-opportunities-supporting-air-force-auxiliary/; "Who We Are," Civil Air Patrol, https://www.gocivilairpatrol.com/about/who-we-are;

121 Office of the Chairman of the Joint Chiefs of Staff, *Joint Publication 3-12: Cyberspace Operations* (June 8, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

COMMISSIONERS

CO-CHAIRMEN

Angus S. King Jr., U.S. Senator for Maine

Michael "Mike" J. Gallagher, U.S. Representative for Wisconsin's 8th District

COMMISSIONERS

Frank J. Cilluffo, Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security

Thomas A. "Tom" Fanning, Chairman, President, and Chief Executive Officer of Southern Company

John C. "Chris" Inglis, U.S. Naval Academy Looker Chair for Cyber Studies

James R. "Jim" Langevin, U.S. Representative for Rhode Island's 2nd District

Patrick J. Murphy, Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District

Samantha F. Ravich, Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Benjamin E. "Ben" Sasse, U.S. Senator for Nebraska

Suzanne E. Spaulding, Senior Adviser for Homeland Security at the Center for Strategic and International Studies

STAFF

SENIOR STAFF

Mark Montgomery, Executive Director

Deborah Grays, Chief of Staff

Erica Borghard, Senior Director and Task Force One Lead

John Costello, Senior Director and Task Force Two Lead

Val Cofield, Senior Director and Task Force Three Lead

Cory Simpson, Senior Director and Directorate Four Lead

Benjamin Jensen, Senior Research Director and Lead Writer

WHITE PAPER LEAD WRITER

Laura Bate, Senior Director for Cyber Engagement

FULL TIME STAFF

Tatyana Bolton, Policy Director

Gregory Buck, Deputy Chief of Staff

Madison Creery, Cyber Strategy and Policy Analyst

Matthew Ferren, Cyber Strategy and Policy Analyst

Chris Forshey, Facility Security Officer

Karrie Jefferson, Director for Cyber Engagement

Ainsley Katz, Cyber Strategy and Policy Analyst

Alison King, Strategic Communications and Congressional Advisor

Sang Lee, Director for Cyber Engagement

Robert Morgus, Senior Director for Research and Analysis

Diane Pinto, Cyber Strategy and Policy Analyst

Brandon Valeriano, Senior Advisor

LEGAL ADVISORS

Stefan Wolfe, General Counsel

Corey Bradley, Deputy General Counsel

Cody Cheek, Legal Advisor

David Simon, Chief Counsel for Cybersecurity and National Security

PRODUCTION SUPPORT

Alice Falk, Editor

Laurel Prucha Moran, Graphic Designer

U.S. CYBERSPACE SOLARIUM COMMISSION

E PLURIBUS UNUM