CSC 2.0

June 2022

Workforce Development Agenda for the National Cyber Director

Laura Bate
RADM (Ret.) Mark Montgomery

Table of Contents

Executive Summary

Nearly 10 years ago, researchers hypothesized that market forces would correct the U.S. shortage of cyber professionals over time.[1] This has not occurred, and the cybersecurity community is out of time. The pervasiveness of avoidable cyber problems such as misconfigured systems, slow patching, and insufficient attention to risk management can frequently be directly tied to cyber staffing shortages.[2] Not only are these problems expensive to remediate after incidents occur, but they are also a threat to national security, particularly when they occur in critical-infrastructure systems or in the supply chains upon which that infrastructure depends.

For more than a decade, report after report has documented the growing number of unfilled cyber positions, both in the U.S. government and nationwide, offering strategies and recommendations to address the shortfall. These strategies and recommendations have too often gone ignored. The congressionally mandated Cyberspace Solarium Commission published a white paper on the cyber workforce in September 2020, identifying systemic barriers stymieing existing workforce development efforts.[3] A lack of centralized leadership, insufficient coordination across the federal government, a nonexistent federal strategy to guide priorities and resources, and ineffective organizational structures all combined to limit the potential of the very programs designed to strengthen and diversify the federal and national cyber workforces.

No clear focal point for interagency coordination existed at the time of the Commission's report, but the July 2021 confirmation of the first-ever national cyber director (NCD)[4] has created a new opportunity to overcome these pervasive barriers. The first section of this memorandum outlines a path forward for the NCD to grow and strengthen the federal cyber workforce and coordinate federal support for national cyber workforce development.

In many cases, the NCD will need legislative support, so the second section of the memorandum recommends actions Congress can take to support federal efforts to grow the cyber workforce. These actions include extending the Federal Cybersecurity Workforce Data Collection Act, establishing a Federal Cyber Workforce Development Institute, and authorizing a Federal Excepted Cyber Service

While these recommendations focus on the federal government in the first instance, the federal and national cyber workforces ultimately draw from the same community of professionals, so effective approaches must address both. Accordingly, the third section of this memorandum outlines actions that private-sector leaders can take to support the NCD's priorities and national cyber workforce development more generally.

Recommendations for the National Cyber Director

Recommendation 1: Establish a Process for Ongoing Cyber Workforce Data Collection and Evaluation

1.1 – NCD and OPM should provide expanded support for cyber workforce data collection

1.2 – NCD should work with heads of federal departments and agencies to ensure accountability for data mandates

1.3 – NCD should work with OPM to share data on the federal cyber workforce

1.4 – NCD should work with NSF to add to data on the national cyber workforce

Recommendation 2: Establish Leadership and Coordination Structures

2.1 – NCD should establish and chair a cyber workforce steering committee

2.2 – NCD should establish a cyber workforce coordinating working group

Recommendation 3: Review and Align Cyber Workforce Budgets

3.1 – Working with OMB, NCD should review budgets for cyber workforce programs

Recommendation 4: Create a Cyber Workforce Development Strategy for the Federal Government

4.1 – NCD should establish a cyber workforce development strategy for the federal government

Recommendation 5: Revamp Cyber Hiring Authorities and Pay Flexibilities Government-Wide

5.1 – NCD should work with OPM to modernize cyber-specific coding structures, hiring authorities, and special pay rates government-wide

5.2 – NCD should work with OPM to establish a cadre of human resource specialists trained in cyber hiring and talent management

5.3 – NCD should work with OPM, OMB, and the appropriations committees to ensure adequate resourcing

Recommendations for Congress

6.1 – Congress should amend the federal cybersecurity workforce assessment act of 2015

6.2 – Congress should increase support for the CyberCorps: Scholarship for Service program

6.3 – Congress should provide incentives to develop entry-level employees into mid-career talent

6.4 – Congress should strive for clarity in roles and responsibilities for cyber workforce development

6.5 – Congress should exercise oversight of federal cyber workforce development in each department and agency

6.6 – Congress should establish cyber excepted service authorities government-wide

6.7 – Congress should expand appropriations for existing efforts in cyber workforce development

Recommendations for the Private Sector

7.1 – Partners in the private sector should increase their investment in the cyber workforce

7.2 – Partners in the private sector should develop shared resources

Acronyms

- CBO – Congressional Budget Office
- CEDI – Cybersecurity Education Diversity Initiative
- CETAP – Cybersecurity Education and Training Assistance Program
- CES – Cyber Excepted Service
- CISA – Cybersecurity and Infrastructure Security Agency
- CTMS – Cybersecurity Talent Management System
- CySP – Cyber Scholarship Program
- FCWAA – Federal Cybersecurity Workforce Assessment Act of 2015
- GAO – Government Accountability Office
- NCAE-C – National Centers of Academic Excellence in Cybersecurity
- NCD – National Cyber Director, also used herein to refer to the Office of the National Cyber Director
- NCSES – National Center for Science and Engineering Statistics
- NDAA – National Defense Authorization Act
- NICCS – National Initiative for Cybersecurity Careers and Studies
- NICE – National Initiative for Cybersecurity Education
- NIST – National Institute of Standards and Technology
- NSF – National Science Foundation
- OMB – Office of Management and Budget
- OPM – Office of Personnel Management
- RAMPS – Regional Alliances and Multistakeholder Partnerships Stimulating
- SFS – CyberCorps: Scholarship for Service
- SRMA – Sector Risk Management Agencies

A Vision for the Future of the Federal Cyber Workforce

Effective cybersecurity relies on proper investments in technology, processes, and people. These elements form a three-legged stool; without any one leg, the structure topples. The United States undeniably excels at fielding cutting-edge technology, and processes and policies governing the cybersecurity ecosystem are improving.[5] However, these strengths alone cannot provide meaningful protection from cyberattacks when the national cybersecurity workforce[6] is less than two-thirds staffed.[7] Ensuring cyber jobs are filled with highly competent individuals will not by itself guarantee success in protecting national cybersecurity, but not filling those positions will certainly result in failure.

The country's cyber professionals are dedicated and skilled, but there are not enough of them. In the United States, there are almost 600,000 open cybersecurity jobs across the private sector and federal, state, and local governments — a remarkable gap considering that the field currently employs just over a million professionals. A comparable shortfall exists in the government's cyber workforce, with nearly 39,000 openings compared to a total employed public-sector cybersecurity workforce of just over 75,000.[8] This gap continues to grow despite a decade of studies that identify the same recurrent problems,[9] and despite years of valuable initiatives by dedicated champions for cyber workforce development from the National Institute for Standards and Technology (NIST), the Department of Homeland Security (DHS), the Department of Defense (DoD), the National Science Foundation (NSF), and beyond.

Meanwhile, lawmakers and their congressional committees have attempted to prioritize this issue for years, passing laws such as the Cybersecurity Enhancement Act of 2014[10] and the Federal Cybersecurity Workforce Assessment Act of 2015 (FCWAA).[11] Bills currently under consideration, such as the America COMPETES Act of 2022[12] and the Federal Cybersecurity Workforce Expansion Act,[13] also contain provisions designed to boost the cyber workforce. Similarly, congressional appropriators continue to demonstrate their ongoing support for cyber workforce development.[14]

The recommendations in this memorandum are driven by a vision for the future in which the U.S. government's approach to building a highly skilled and qualified cyber workforce is coordinated, prioritized, and diversified. The policies that shape this future workforce will be based on clear data and consistent metrics. Hiring managers in all federal departments and agencies will have the authorities needed to exercise agility and flexibility in hiring team members and determining compensation. Policies and practices will be structured to foster inclusiveness, recognizing that teams perform better when they draw on demographically and geographically diverse populations with many sources of learning and professional experience.[15] Employees will move fluidly between different federal agencies and follow career paths that cross back and forth between the private and public sectors. Human-capital officers across government will draw on shared resources for employee learning and professional development, which they can augment with additional options tailored to their organization's specific mission and needs. Finally, and critically, all these stakeholders will benefit from multiple, varied pathways into federal government jobs that draw on entry-level candidates with an enthusiasm for the work, seasoned cyber employees, and the myriad professionals from diverse backgrounds that land in between.

This vision builds on the Cyberspace Solarium Commission's 2020 findings.[16] It also draws heavily on the important work of many others in government, the private sector, and the non-profit and academic spheres. In particular, many elements reflect the 2020 Federal CIO Council's drivers for the information technology (IT) workforce,[17] the National Initiative for Cybersecurity Education (NICE) Strategic Plan,[18] and the Federal Cyber Workforce Management and Coordinating Working Group's Strategy and Implementation Plan.[19]

Characteristics of the Current Environment

While many human resources (HR) teams often — and understandably — hesitate to treat talent management in any one field differently than the rest of an organization, a sense of exceptionalism in cyber workforce development is well-founded. The confluence of discipline-specific barriers to effective talent management and the urgent imperative to mitigate cybersecurity risks warrants extraordinary measures in cyber workforce development. The current federal cyber workforce development environment is characterized by challenges in the following areas:

Diversity: As a whole, the cyber workforce struggles with diversity at all levels, particularly in leadership roles, as federal leaders have identified.[20] While exact numbers vary by source, the available data indicates that Black, Hispanic, American Indian, Alaska Native, and Native Hawaiian professionals are underrepresented in the cyber workforce relative to their percentage of the U.S. population.[21] Meanwhile, women make up only about 24 percent of the cybersecurity workforce.[22] The average federal worker is more likely to be older, male, and possess a college degree relative to the rest of the U.S. labor force.[23]

Coordination: Across the federal government, there are many projects underway, communities of practice, and examples of good work. For example, NICE — an office within NIST — has developed both community and interagency coordinating councils[24] and an implementation plan toward shared goals.[25] Likewise, the Federal Cyber Workforce Management and Coordinating Working Group focuses on modernizing cyber career development programs, tools, and resources to improve mobility and skill portability across the federal government. Accordingly, it would be inaccurate to say that there is no coordination across federal or national cyber workforce development efforts. However, existing efforts and practitioners generally sit *within* rather than *across* departments and agencies, meaning that while they provide a valuable channel for communication, none has the crosscutting authority needed to bring meaningful prioritization and high-level coordination.[26] This has led to duplication of effort, conflicting guidance, and missed opportunities. Moreover, with no federal government-wide strategy, there is limited basis to determine how resources should be allocated across different lines of effort.

Data: Cyber workforce development experts lack accurate data to measure and understand the impact of different efforts and policy interventions on the federal cyber workforce. CyberSeek — a data visualization platform supported by NICE and industry partners — provides high-level insight into the national cybersecurity hiring landscape,[27] but more data is needed to understand, for example, demographic and retention trends in the workforce. The 2015 Federal Cybersecurity Workforce Assessment Act[28] began work toward this goal. In practice, however, inconsistencies in data collection between departments and agencies, along with the lack of a mechanism to share findings, limit the utility of existing data. Moreover, the legislation did not require departments and agencies to report their target hiring level, making budgeting for future workforce needs an exercise in guesswork unless individual organizations implement their own data-gathering efforts beyond those required by law. The legislation is also limited to the federal, not national, cyber workforce.

Talent Management Capabilities and Capacity: Some departments and agencies — particularly DoD and DHS — have developed their own systems to create greater agility in hiring and other personnel actions while still observing federal laws that, for example, ensure fair hiring practices. However, similar capabilities generally do not exist for other federal agencies,[29] which exacerbates an already difficult cyber hiring challenge as those agencies compete for qualified people.[30]

Limited Hiring and Personnel Management Staff: Innovative hiring cannot happen at scale when the personnel management teams themselves are too small. This is true across the government, where a group of experts within the Office of Personnel Management (OPM) is charged with cultivating innovation from within a remarkably inflexible bureaucracy in order to build systems that work for the many — and very different — federal departments and agencies. Even federal agencies that focus on cyber hiring, particularly the Cybersecurity and Infrastructure Security Agency (CISA), simply do not have the mission support they need to hire at the requisite scale.

Structural Constraints: Assumptions that candidates must have a certain academic degree or certification to qualify for a job or that promotions should be based on time-in-service rather than competence are a hindrance and unhelpful in most fields. Within the cyber workforce, these assumptions severely undermine hiring and effective talent management. Cyber professionals often come from unexpected backgrounds; skills are often self-taught, acquired on the job, or an outgrowth of military service. Accordingly, cyber career paths can take many different turns, and professionals can advance at different speeds depending on their context and background. Conventional assumptions about hiring, pay, and advancement sharply limit the flexibility needed to adjust to these many variances and may create systems that disadvantage already underserved communities.

In addition to these challenges, the public-sector and private-sector workforces are tightly interwoven because, ultimately, the federal workforce is just a subset of the national talent pool. The private sector faces similarly daunting challenges in filling cyber jobs. In recognition of the cyber talent pool's interconnectedness, the NCD will need to focus beyond just the federal workforce because (1) national security and private-sector cyber resilience are mutually dependent and (2) cyber professionals do — and should — move between government and the private sector.

Efforts Currently in Motion

Although they are not operating at the scale needed to meet current, much less future, demand for cyber talent, many current programs inside and outside of government have the potential to grow to meet a considerable portion of that need if given appropriate authorities, provided with adequate funding, and held accountable. Examples in federal workforce development include:

National Initiative for Cybersecurity Education: A federal office that operates in partnership with other government stakeholders, academia, and industry, NICE works to "energize, promote, and coordinate" the cybersecurity education and workforce development community.[31] Through the development of the Workforce Framework for Cybersecurity (NICE Framework),[32] the office has created a shared lexicon to describe cybersecurity work and the knowledge and skills that cyber professionals must possess, not just in the federal government but across the private sector and even internationally.[33] The NICE program office serves as a hub for cybersecurity education and workforce development by hosting annual conferences, working groups, and communities of interest. The NICE program office has continued to undertake new initiatives (for example, the Cyber LEAP program)[34] even as usage of its core product, the NICE Framework, grows. Both because congressional legislation has required its use in federal workplaces and as a natural result of industry uptake, more stakeholders are using the NICE Framework, necessitating personnel dedicated to outreach and upkeep. Despite this track record of growth and success, NICE's budget has not changed since its original appropriation of $4 million in FY14,[35] making it overdue for an increase in funding to bolster personnel and right-size the office relative to its expanded body of work.

Efforts by the Office of Personnel Management: As the federal agency tasked with HR functions, OPM has played a key role in federal cyber workforce development. Most notably, that includes defining the various qualifications, classifications, and requirements that give structure to federal cyber personnel actions,[36] and establishing the rules for various flexibilities that help respond to the high demand for cyber professionals. For example, OPM has established direct-hire authority and pay flexibilities that can be used to alleviate some of the challenges of federal cyber hiring.[37] OPM has also provided pivotal guidance to departments and agencies as they implement the requirements of the Federal Cyber Workforce Assessment Act of 2015, which leverages the NICE Framework to provide a count of federal cyber work roles of critical need.[38] OPM also provides cybersecurity and IT program management competency models, interpretive guidance, and a range of training efforts to improve cyber hiring. Many of these can be improved, but it should be noted that it is only because of OPM's years of commendable work on these topics that an incumbent system exists to improve upon. Moreover, the mission and particularly the hands-on experience that OPM experts have cultivated dictate that OPM must continue to be a core partner in federal cyber workforce development efforts.

OPM plays a key role in federal cyber workforce development, including by establishing rules that help respond to the high demand for cyber professionals.

Federal Cyber Workforce Management and Coordinating Working Group: This working group serves as an interagency operational coordinating body that develops best practices, tools, and resources to address shared challenges, enhance workforce management capabilities, and reduce siloes. The working group comprises the practical implementors of the Federal Cyber Workforce Management Act of 2015 and other cyber workforce policies from across the federal government.[39] To date, the working group has produced a career pathway specific to each NICE Work Role, created a dynamic tool (called the "Career Pathway and Career Roadmap") for the public and private sectors on the National Initiative for Cybersecurity Careers and Studies (NICCS) website, and shared resources across the interagency on guidance and procedures to implement requirements. The working group's Multi-Year Strategy and Implementation Plan is set for FY22-24, designed to build on these successes and drive high-priority, federal-wide cyber workforce initiatives.

CyberCorps: Scholarship for Service: The CyberCorps: Scholarship for Service (SFS) program works through colleges and universities nationwide to provide scholarships to students in cyber fields in exchange for a government service term. Most scholarship recipients serve this term working for federal agencies, but some support state, local, tribal, and territorial governments, where the demand for cyber professionals and educators is steep. The SFS program provides grants to universities, which then provide both stipends and coursework directly to students. This approach allows for an increased number of participating institutions and for an increased number of students per participating institution, graduating a total of about 400 students per year.[40] SFS directly feeds into public-sector recruiting efforts while also helping participating institutions expand post-secondary educational offerings for all students.[41] Despite the tens of thousands of cyber jobs currently unfilled in the public sector,[42] the SFS budget has grown modestly in recent years, totaling $55.09 million in FY18,[43] $55.33 million in FY19,[44] $55 million in FY20, $60 million in FY21,[45] and $63 million in FY22.[46] In fact, in many of those years, the president's budget request did not include an increase for the program. The FY21 request actually would have shrunk the program's budget had congressional appropriators not decided otherwise.[47] For 20 years, federal leaders across numerous administrations have called cybersecurity workforce recruitment and development a priority and cited its importance for national security[48] but failed to fund the SFS program appropriately. The Cyberspace Solarium Commission recommended that the program be resourced to graduate 2,000 students per year, with its budget growing 20 percent annually for the next decade.[49]

Cybersecurity Education and Training Assistance Program (CETAP): CETAP is a grant awarded by CISA to a non-profit partner (currently Cyber.org) to support cybersecurity education in K-12 classrooms through the development of cybersecurity curricula and instructor training. The program has been active for more than a decade, and Congress codified the program in the National Defense Authorization Act (NDAA) for Fiscal Year 2021.[50] At its current funding level, the program provides training to approximately 5,000 new teachers per year, impacting 500,000 students annually. This track record is impressive, especially for a relatively small program. Not only does it encourage the general population to be more conscientious about their personal security, but it also boosts awareness of career opportunities in cybersecurity, helping to put future cyber professionals on the path to their careers.

An estimated 1.2 million educators in the United States work in relevant specialties and thus would benefit from the training funded by CETAP. These are predominantly teachers in science, technology, engineering, mathematics (STEM) as well as career counselors and administrators. At the current funding rate, however, it would take roughly 95 years to train these educators.[51] For an already established program with proven success, this timeline is unacceptable and represents an opportunity missed with each passing year.

Despite these benefits and statements from government officials linking K-12 cybersecurity education to long-term national cyber resilience,[52] the executive branch has regularly proposed eliminating funding for the program.[53] Congressional appropriators have made clear that "any proposed reductions to cybersecurity education will not be considered unless CISA provides a clear plan for how the previously funded activities would be fully realigned within other agencies in a manner that sustains the objectives of this critical effort."[54] In FY22, appropriators set aside $6.8 million for CETAP.[55] CISA's FY23 budget request, however, again recommends eliminating the program, adding only that "CISA will work with the National Science Foundation (NSF) to build and strengthen the national cybersecurity workforce to include K-12 programs."[56] Given its discrepancy with the FY22 appropriation, CISA's request will likely be ignored by Congress.

Though the increase in CETAP's FY22 appropriation is welcome, the program's budget will need to continue to increase dramatically. That additional funding is necessary both to allow for outreach to a much larger group of educators and potentially to expand the program to work with school administrators to support the uptake of cybersecurity education in schools. Incremental funding increases calculated to reach $20 million per year by FY26 would help achieve the needed scale.[57]

Regional Alliances and Multistakeholder Partnerships: Section 9401(f) of the FY21 NDAA requires NIST to establish Regional Alliances and Multistakeholder Partnerships Stimulating (RAMPS) cybersecurity education, training, and workforce development. These partnerships, previously piloted by NICE,[58] would identify and strive to fill local workforce needs.[59] RAMPS can create a diverse and geographically distributed array of programs, all with the shared goal of bolstering the cybersecurity workforce. The Congressional Budget Office (CBO) estimated that the HACKED Act — the bill that originally proposed these partnerships before it was incorporated into the FY21 NDAA — would require $50 million to implement over its first five years, with an obligation of $12 million ($10 million for grants and $2 million for administrative costs) in its first year of implementation.[60] However, the Department of Commerce justification for the president's FY22 budget request did not specify funding for this program, and overall increases in NIST's cybersecurity and privacy budget were modest relative to funding increases for other NIST priorities.[61] The FY22 Consolidated Appropriations Act subsequently specified that no less than $500,000 should go toward the new program.[62] The president's FY23 budget request asked for $7 million to support the program in the coming year,[63] far below the original CBO estimate of program costs.

National Centers of Academic Excellence in Cybersecurity (NCAE-C): This program has been operating since 1999 to promote high-quality cyber education at colleges and universities across the country. In the last five years, NCAE-C academic and student development requirements have shifted to emphasize collaboration between institutions, competency-based education, and development of graduates ready for careers in cybersecurity. Additional funding in the past three years has accelerated program growth and helped the NCAE-C program leverage collaboration with partner institutions to achieve workforce goals in communities across the nation and prepare teachers and faculty to teach cybersecurity. The funding has also allowed NCAE-C to create a curriculum repository, curate the quality of cybersecurity curricula nationwide, create a career pathway from middle school to post-secondary education to the workforce, and begin nine community-based initiatives to develop local cybersecurity education and economic development.

Through the NCAE-C program, an established community and network of regional hubs support more than 370 institutions.[64] Recently, the program has also developed the Cybersecurity Education Diversity Initiative (CEDI), which works to connect minority-serving institutions with mentorship and assistance to advance their educational offerings in cybersecurity.[65] The NCAE-C Program Office is also the executive administrator for DoD's Cyber Scholarship Program (CySP).[66] CySP provides support for education at NCAE-C institutions as a recruitment benefit to students who are not currently DoD employees and as a retention incentive to current employees and military members.

Across all these initiatives, the level of funding invested dictates the breadth and impact of the work. Additional funding can thus scale these initiatives to support the continued growth and innovation of this important driver of cybersecurity education. Notably, there is currently no authorizing legislation for the NCAE-C program, although Congress could address this gap to ensure the program's continuity.

Additional highlights — though not an exhaustive list — are outlined in Figure 1.[67]

FIGURE 1: A Selection of Federal Cyber Workforce Initiatives

Department/Agency	K-12	Post-Secondary	Employee Training	Workforce Ecosystem
CISA/DHS	CETAP	Public Infrastructure Security Cyber Education System[68]	President's Cup, Federal Virtual Training Environment	NICCS Website, Non-Traditional Training Providers,[69] Industrial Control Systems Training
Department of Education	Presidential Educator Award, CTE CyberNet[70]			
Federal Chief Information Officer (CIO)			Reskilling Academy[71] (*co-sponsored with DHS*)	
NIST	Cybersecurity Career Awareness Week, NICE K12 Conference, NICE K12 Community of Interest	NICE Challenge Project	Federal Information Systems Security Educators[72]	NICE Framework, NICE Conference, NICE Community Coordinating Council, CyberSeek, U.S. Cyber Games, NICE RAMPS
NSA/DoD	GenCyber (*co-sponsored with NSF*)	N-CAEC (*co-sponsored with DHS*), CEDI, CySP		NCAE-C Community (*co-sponsored with DHS*)
NSF		CyberCorps: SFS (*in collaboration with DHS and OPM*)		
OPM				Federal Cyber Workforce Assessment Act of 2015, Various Guidance
Interagency			Federal Rotational Program (*co-sponsored with OPM*)	Cyber Careers Pathway Tool, NICE Interagency Coordinating Council, Working Group Multi-Year Strategy and Implementation Plan, Federal Cybersecurity Workforce Summit and Webinar Series

Recommendations for the National Cyber Director

The NCD position and associated office were established by the FY 2021 NDAA in order to "serve as the principal advisor to the President on cybersecurity and policy and strategy," to include the personnel and management programs of federal departments and agencies.[73] Congress intended for the NCD to have a leadership role in addressing the cyber workforce challenge. The following section provides recommendations to help the NCD address the challenges of cyber workforce development for the federal government and coordinate the federal role in nationwide workforce development:[74]

Recommendation 1: Establish a Process for Ongoing Cyber Workforce Data Collection and Evaluation

Establishing priorities and distributing resources across the interagency requires an accurate measure of cyber workforce requirements.[75] To fulfill the NCD's statutory responsibility to make recommendations "relevant to changes in the organization, personnel, and resource allocation" of federal departments and agencies,[76] the NCD must be able to identify components or mission areas that are experiencing particular limitations due to the quality or quantity of their staffs. Relatedly, identifying federal cyber workforce development programs that best address workforce gaps requires reliable longitudinal data on the workforce predating the programs and continuing through their interventions.[77]

In an attempt to address the data gap, Congress passed FCWAA in 2015.[78] Unfortunately, the legislation lacks a requirement for projected vacancy data. Moreover, the data collected is inconsistent, in part because federal departments and agencies have struggled to map existing positions to work roles consistently.[79] While FCWAA circumscribes cybersecurity work roles through the commonly-used NICE Framework,[80] the hiring processes within departments and agencies have evolved based upon — and largely continue to use — OPM's occupational classifications, driving departments and agencies to navigate and interpret connections between the two.[81] Furthermore, a full-time employee may fill more than one cybersecurity work role, so a particular work-role shortage likely represents less than one full-time employee. This nuance compounds the already significant challenge of producing an accurate count of federal workforce vacancies.

OPM is making inroads in educating departments and agencies to adopt the new cyber designations, but the challenge remains. Moreover, the legislation mandating this data collection effort has limited enforcement options. Federal departments and agencies are required to "identify information technology, cybersecurity, or other cyber-related work roles of critical need in the agency's workforce."[82] But as the Government Accountability Office (GAO) reported in 2019, not all actually did so accurately and according to the specified timeline.[83]

Beyond challenges in implementing FCWAA, Congress can improve the legislation itself to require the provision of data that is more useful and more consistent, as discussed in the following section. In its current form, the legislation requires department and agency heads to provide information only on work roles of critical need. The law does not actually mandate a count of the total number of all cyber professionals required to bring the department or agency up to target staffing levels.[84]

Simply identifying open cyber billets is useful but faces two limitations. First, such a count can be biased by a tendency to generalize position descriptions for the sake of creating flexibility in agency-wide staffing, leading to an undercount of positions that have cyber work roles as compared to positions with IT work roles generally. Second, although the legislation is designed to identify gaps in the cyber workforce, the manner in which the data has been collected leaves elements of this goal unaddressed. In order to carry out long-range workforce planning, departments and agencies will need to identify more than just work roles of critical need or even the scale of their staffing shortages (that is, their authorized and funded positions that are currently vacant). In addition to counting those current vacancies, departments and agencies must address the harder question of pinpointing the optimal number of cyber professionals needed to achieve their respective missions, both currently and in the future. This latter figure requires identifying unfunded positions, raising difficult questions for agency leadership about why the agency is underfunding cyber staffing. The dynamic makes this data both very difficult to get and very important for planning for the future.

For any metric to be useful, data collected across departments and agencies must strike a careful balance between consistency and relevance to the source. Because each department and agency has been responsible for delivering its own count in response to FCWAA, the data is susceptible to systematic inconsistencies. This is partly a reflection of the tension between designing metrics that are useful for a particular organization versus for the government as a whole. For a metric to be useful within a particular department or agency, the organization in question should be measuring criteria specific to its individual challenges and mission. However, to be useful across agencies, metrics must also be standardized.

To address the necessity for standardization, FCWAA tasks departments and agencies with mapping their current positions to work roles outlined in the NICE Framework. While the intended goal of standardization is clear, the exercise is more complicated in practice. Position descriptions have evolved according to individual agency needs and an incumbent system of occupational classifications. As a result, individual position descriptions rarely map neatly onto standards and often draw on competencies that may apply to a number of different work roles (as described by a 2020 revision to the NICE Framework that introduced competency areas as another application of the framework).[85] Although OPM has worked with NIST to provide guidance,[86] most decisions on whether and how to code these many hybrid positions fall to the judgment of the individual, office, agency, and department accounting for that position. As each link in the chain of data collection makes these determinations, the data as a whole becomes subject to inconsistencies even though each decision is informed by the same implementation guidance.[87] Accordingly, the data's usefulness comes into question.

Since the federal government recruits from a talent pool shared by every other cyber employer and funds efforts to grow and sustain that shared talent pool, the NCD will also need detailed, reliable longitudinal data on the entire national cyber workforce, particularly data that provides information on the outcomes and impacts of federally funded efforts. In pursuing this objective, the NCD will be able to draw on existing exemplars of data tools "helping to close the cybersecurity talent gap."[88] CyberSeek, a NIST-funded project, has already begun to leverage job postings nationwide to gain insight into what employers are seeking in their hiring.[89] Whether through expansion of that effort or the development of complementary initiatives, the NCD can support nationwide cyber workforce development by addressing remaining data gaps.

The need for better data has been a key part of the Cyberspace Solarium Commission's workforce development recommendations. In its March 2020 report, the Commission called for research "into the current state of the cyber workforce, paths to entry, and demographics."[90] A subsequent Commission white paper encouraged NSF to fund further research.[91] Similarly, the National Academy of Public Administration called on the NCD to "ensure data relevant to cyber workforce challenges and needs are collected and available for use in developing strategy, creating educational programs, and assessing the impact and effectiveness of workforce development initiatives."[92] That report suggested that the Bureau of Cyber Statistics, an organization recommended by the Commission but not yet established, could be a good source for this data. Until the bureau is established, however, there are still very impactful steps the NCD can take to improve the quality of data on the cyber workforce. Specific actions include:

1.1 – NCD and OPM Should Provide Expanded Support for Cyber Workforce Data Collection

To the greatest extent possible, the NCD — working with federal department and agency heads and hiring managers — must strive for consistent standards in classifying occupations, job requirements,[93] and other means of measuring the workforce. Doing so will require an ongoing review of the data collected as well as centralized, easily accessible support for departments and agencies conducting that review. OPM has filled this role in the past, but the NCD can help bolster resources to ensure OPM has the personnel necessary to rapidly address requests for support or information from departments and agencies.

1.2 – NCD Should Work With Heads of Federal Departments and Agencies to Ensure Accountability for Data Mandates

As departments and agencies continue to conduct and improve data collection efforts, the NCD can ensure that high-level attention is directed to resolving challenges that may emerge, addressing barriers causing delays in the provision of data, and improving accountability across government. In particular, the NCD can work with OPM, departments, and agencies to ensure that workforce assessments include a count of the number of cyber professionals needed to reach staffing goals (funded and unfunded), in addition to a count of open billets (vacancies) and work roles of critical need.

1.3 – NCD Should Work With OPM to Share Data on the Federal Cyber Workforce

High-level, aggregated data on federal cyber workforce trends should be made publicly available to allow partners in education, stakeholders across government, and jobseekers to identify areas of greatest need. For federal stakeholders, a more detailed version of this data should be shared on a regular basis. An interactive federal cyber workforce dashboard would provide hiring managers with a much-needed baseline for evaluating the effectiveness of current workforce development efforts and would provide data-driven insights into new recruitment and workforce development initiatives. A digital dashboard could also be coupled with a reporting platform to assist OPM in gathering data on the cyber workforce from federal departments and agencies. The NCD can work with OPM to expand existing nascent efforts to build a dashboard, identify and overcome bureaucratic and budgetary hurdles to implementation, and ensure adequate resourcing to maintain the initiative.

1.4 – NCD Should Work With NSF to Add to Data on the National Cyber Workforce

As is true in the federal government, across the national cyber workforce, data on workforce composition and dynamics is sparse. To their credit, industry and professional associations have made strides in addressing this gap.[94] But industry surveys are not designed to evaluate the impacts of federal policy over time. In particular, evaluating the dynamics of demographic underrepresentation has been challenging,[95] which significantly hampers data-driven efforts to promote diversity in the cyber workforce. NSF is home to the National Center for Science and Engineering Statistics (NCSES), which Congress tasked with providing statistical information on the science and engineering workforce.[96] The NCD should work with NSF to ensure NCSES has the personnel needed to provide statistical information on the national cyber workforce.[97] In addition, the NCD should work with NSF to ensure that grant funding is made available to enable academic study of the drivers and dynamics of the cyber workforce. In each of these initiatives, a key priority should be ensuring that collected data is aligned to the NICE Framework to the greatest extent possible and is complementary to the existing NIST-funded CyberSeek efforts.[98] By engaging with the Office of Management and Budget (OMB), the NCD can work to ensure that resourcing needs are reflected in the president's budget requests. Congressional appropriators can further enable progress by ensuring that these efforts are properly resourced.

Recommendation 2: Establish Leadership and Coordination Structures

As shown in Figure 1 above, the federal government has built many cyber education and workforce development initiatives. Leadership of these efforts is diffuse. The structure is further complicated by the array of congressional committees that can claim jurisdiction over a component of cyber workforce development. As the National Academy of Public Administration noted, "Congress has not been given a coherent picture of federal goals for national workforce development or the funds and support needed to accomplish those goals because there has not been a single leader in the executive branch to provide clarity and consistency of goals and coordinate funding to support them."[99] Many committees — to their credit — are eager to authorize new work on this topic.

The ad hoc structure of federal cyber workforce efforts is a function of motivated stakeholders devising innovative and impactful solutions based on the resources at hand in their respective organizations. These efforts do not align with a centralized plan. Despite many genuine attempts to share information, collaborate, reduce duplication, and increase effectiveness across the interagency, problems persist. Unproductive competition for resources, missed opportunities, and duplication of efforts all erode the effectiveness of the work as a whole. In the extreme, they can even inhibit progress as stakeholder groups jostle over which department or agency should hold jurisdiction for a particular project.

> ***"The NCD should create leadership and coordination structures for federal cyber workforce development efforts. To provide high-level alignment of efforts while still allowing the innovative ecosystem of current initiatives to flourish, the new structure needs to provide both a capability for authoritative direction and a forum to foster transparency and participation."***

To get the most out of available resources and pave the way for more efficient interagency coordination, the NCD should create leadership and coordination structures for federal cyber workforce development efforts. To provide high-level alignment of efforts while still allowing the innovative ecosystem of current initiatives to flourish, the new structure needs to provide both a capability for authoritative direction and a forum to foster transparency and participation. As recommended by a September 2020 Cyberspace Solarium Commission white paper titled "Growing a Stronger Federal Cyber Workforce," and in alignment with the National Academy of Public Administration's January 2022 recommendation for increased leadership,[100] the NCD should establish a two-part structure for providing leadership and coordination:

2.1 – NCD Should Establish and Chair a Cyber Workforce Steering Committee

The steering committee would provide leadership-level strategic guidance while "coordinating with and specifying roles and responsibilities between and among agencies," as noted by the National Academy of Public Administration.[101] The committee would also advise on the distribution of resources and ensure accountability for and progress toward strategic priorities. The committee would be composed of a fixed membership with representation from the NCD (chair), OMB, OPM, NIST (NICE), DHS (CISA), NSF, DoD, the Department of Education, and the Department of Labor.

2.2 – NCD Should Establish a Cyber Workforce Coordinating Working Group

The working group would be responsible for ensuring that cyber workforce development efforts are implemented in concert with one another, taking advantage of collaborative opportunities, sharing information and resources when possible, and identifying potential new lines of effort. The working group would also be responsible for ensuring that the steering committee charters all new cyber workforce development programs, and that all efforts are aligned with the steering committee's strategic guidance and are resourced appropriately given their role with respect to an overall strategy (as outlined in Recommendation 4).

The steering committee would appoint the working group's chair(s), who would serve on a rotating basis, and the working group's membership would be open to all federal departments and agencies. The NCD may also consider providing mechanisms for the working group to engage with partners from outside the federal government. Recognizing the potential to trigger the Federal Advisory Committee Act, the NCD should consider existing engagement through the NICE Community Coordinating Councils as a means to engage with such stakeholders.[102] The NCD, the steering committee, and the working group should seek input from state, local, tribal, and territorial governments as well as from academia and members of the private sector involved in federal workforce issues (major federal contracting firms, for example).[103] They should also engage with the Federal CIO Council, the Chief Human Capital Officer Council, and the Chief Learning Officer Council.

A strong model for the working group already exists. In recent years, the Federal Cyber Workforce Management and Coordinating Working Group has been drawing input from across the interagency to address shared problems, such as a tool to clarify possible federal cyber career pathways.[104] In establishing the proposed Cyber Workforce Coordinating Working Group, the NCD should work with the existing group to ensure continuity and a smooth transition to the structure described in this recommendation. If the existing group can serve as the foundation for the new working group, the NCD will be better positioned to enable the current group's future progress and benefit from its deep experience and working relationships.

Recommendation 3: Review and Align Cyber Workforce Budgets

By law, the NCD is responsible for "monitoring and assessing the effectiveness, including cost-effectiveness," of the implementation of cyber policies, and also for "reviewing the annual budget proposals for relevant Federal departments and agencies."[105] Furthermore, the NCD's deputy for federal cybersecurity also serves as the federal chief information security officer, based in OMB. This "dual-hat" arrangement allows that official to leverage their expertise when "review[ing] agencies' cybersecurity budgets and recommend[ing] changes that will align spending plans" across the federal government.[106] This will be a powerful collaboration for ensuring the federal government is maximizing its investment in the cyber workforce.

Because cyber workforce initiatives have tended to take root and grow wherever stakeholders found resources available, the availability of funding — rather than overall strategic impact — has been a primary driver of program growth. As the expenditure of funding becomes further entrenched through budgeting and appropriations processes that refer heavily to prior years' expenditures, changing these patterns once established takes very deliberative action. The NCD, in cooperation with OMB,[107] should ensure the dynamic is flipped to enable strategy, rather than availability, to be the primary driver of resource allocation. Moreover, to the greatest extent possible, evidence and data should inform the NCD's assessment of strategically aligned and impactful programs, as outlined in Recommendation 1 above. Impactful programs also include those that support specific, often underserved or underrepresented communities and aim for long-term impact rather than short-term return. The current ecosystem of programs benefits from this diversity of efforts and approaches.

The review of budgets should also look for opportunities to bolster support for initiatives that advance the ecosystem of efforts as a whole, whether by advocating for tools that can drive greater coordination, platforms that can be shared, or other efficiencies stemming from greater coherency. To provide several examples, a program such as CETAP has the potential to provide long-term benefit to the entire national cyber workforce, not least the federal workforce. However, CETAP's budget has regularly been recommended for elimination. Similarly, the White House's FY22 budget request did not include the NICE RAMPS program, and the FY23 request asked for only about half of what the CBO estimated the project would cost.[108] Finally, the CyberCorps: Scholarship for Service program infuses the entire federal government with cyber talent while strengthening cybersecurity educational programs nationwide, yet for decades the program has seen only limited funding growth.[109]

3.1 – Working With OMB, NCD Should Review Budgets for Cyber Workforce Programs

The NCD should work with OMB to highlight and address misalignments between strategic goals, outcomes, and current expenditures through a thorough review of project budgets for cyber workforce programs. Moreover, by providing a clearer picture of the overall connection between funding and strategic goals, the executive branch — through the NCD — can better explain to congressional appropriators where and how funding can be used. Leveraging the NCD's perspective is all the more necessary because quantifying return on investment in the cyber workforce — a critical part of building any budget — requires a firm grasp of the strategic landscape of American cybersecurity. Assigning a dollar figure to the risk incurred by federal cyber staffing shortages requires extensive knowledge of the potential cost of cyber incidents and the manner in which each department, agency, component, office, and individual contributes to incident prevention, response, and resilience. OMB and congressional appropriations committees must balance many competing priorities, and the comprehensive insight the NCD provides on cyber risk will be essential for identifying and advocating for appropriate levels of investment in the cyber workforce.

Recommendation 4: Create a Cyber Workforce Development Strategy for the Federal Government

The call for a cyber workforce development strategy for the federal government is not an especially new one. Research going back more than a decade,[110] as well as a recent report from the National Academy of Public Administration, has called for the same.[111] The NCD's cyber workforce development strategy for the federal government can draw on the important foundational work of other stakeholders. In particular, the NCD should leverage a July 2016 OMB memo that set forth the first Federal Cybersecurity Workforce Strategy. The memo outlined general aims (such as "Identify Cybersecurity Workforce Needs" and "Expand the Cybersecurity Workforce through Education and Training") and improvements to existing programs.[112] The CIO Council Workforce Committee, which has continued to bring greater attention and energy to federal IT workforce issues,[113] also deserves commendation, as does the NICE Strategic Plan, which draws on the wider national cybersecurity workforce development community for input.[114]

The NCD's strategy must be distinct from the work done by these prior and current efforts. In particular, the NCD must observe the difference between a strategy for the federal government and a national strategy. Whereas the former is created by the federal government to set plans, priorities, and areas of responsibility for the federal government, the latter brings together perspectives from the full gamut of national workforce development stakeholders, including the private sector; academia; state, local, tribal, and territorial governments; and the federal government. The NICE Strategic Plan serves the latter function, engaging extensively with partners and working with interagency and community coordinating councils to develop "the vision, mission, values, goals, and objectives for both the organization and the greater NICE community."[115]

The NCD should take care to avoid duplicating NICE's community-driven work on national cybersecurity workforce development. However, the NICE strategic plan and the priorities articulated by the national cybersecurity workforce development community should help inform the NCD's work to establish a strategy for cyber workforce development efforts across the federal government. Such a plan should not (and in all practicality cannot) come from within a single department or agency, because successfully establishing priorities, roles, and resources among departments and agencies requires the imprimatur of the White House. To illustrate, if two agencies, both operating within their congressionally authorized role, undertake initiatives that fulfill very similar (or, conversely, conflicting) functions, neither is in a position to dictate which effort should be prioritized. In such cases, a strategy determined within one department is unlikely to significantly change the planned activities of another department. While there certainly are many situations where multiple departments and agencies can work toward similar goals with positive effects, the NCD can greatly improve the overall effectiveness of the system by working with departments and agencies to produce a federal government-wide strategy to bring clarity, prioritization, and coherence to cyber workforce education and development efforts (including efforts to benefit both the federal workforce and the national workforce).

Others have observed this lack of clarity surrounding the way efforts fit together as a part of a larger federal whole. For example, the National Academy of Public Administration noted that "CISA could benefit from a clear understanding of its role in cybersecurity workforce development in relation to other federal agencies."[116] The NCD can help provide this clarity by developing a cyber workforce strategy for the federal government that establishes priorities among many lines of effort, ameliorates questions regarding areas of responsibility between different departments when congressionally authorized roles overlap or converge, establishes and enforces requirements and common practices across departments, and makes recommendations regarding the distribution of resources. Such issues can best (and often only) be addressed at the White House level. The NCD can also provide the powerful advocacy needed to ensure that the United States is making plans now to educate the professionals who will defend federal networks decades into the future.

4.1 – NCD Should Establish a Cyber Workforce Development Strategy for the Federal Government

Working with OMB, Congress, and the steering committee and in consultation with the working group proposed in Recommendations 2.1 and 2.2, the NCD should develop a new strategy that should, at a minimum:

- Establish priorities in federal cyber workforce development efforts, including efforts to promote diversity in the federal cyber workforce;
- Clarify roles and responsibilities across federal departments and agencies;
- Set requirements and timelines outlining expectations for cyber workforce development efforts to drive accountability within departments and agencies and ensure feasibility given available resources;
- Outline long-term investments to build educational capacity and bolster cyber career awareness;
- Identify outside stakeholder groups that may be developing adjacent strategies — such as state, local, tribal, and territorial governments — and provide a plan to engage and coordinate with these efforts;
- Highlight priority areas for potential innovation in cyber workforce development approaches; and
- Identify resourcing requirements to support the strategy.

Given the many stakeholders and initiatives in this space, a cyber workforce development strategy for the federal government may tend to gravitate toward cataloging all the various programs underway[117] and articulating support for each. It may also tend toward establishing major lines of effort in cyber workforce development generally. While cataloging efforts and defining general goals are necessary parts of developing a strategy, much of this work has already been done, as discussed above. Moreover, a strategy that achieves only these two functions will miss the opportunity to bring real coordination and focus to federal efforts. By comparison, the process of establishing clear priorities and roles — particularly if done with participation by key stakeholders and with full transparency — will allow champions for cyber workforce development across departments and agencies to maximize comparative advantages and plan around long-term investments. In turn, this will allow the federal government as a whole to continue pursuing a diverse portfolio of efforts but with maximum efficiency and impact.[118]

Recommendation 5: Revamp Cyber Hiring Authorities and Pay Flexibilities Government-Wide

DHS made news in 2021 by bringing online the Cybersecurity Talent Management System (CTMS).[119] The system is based on legislation authorizing the secretary of homeland security to "establish, as positions in the excepted service, such qualified positions in the Department as the Secretary determines necessary to carry out the responsibilities of the Department relating to cybersecurity," "appoint an individual to a qualified position," and "fix the compensation of an individual for service in a qualified position."[120] Similarly, DoD also has specific authorizing legislation that allows for the creation of excepted service positions, direct-hire authority, and pay flexibilities to fulfill the Pentagon's cyber mission.[121] DoD's authorization forms the basis of its Cyber Excepted Service (CES).[122] While these systems have their own challenges — for example, CTMS was established without dedicated vacant billets, limiting its immediate impact, and hiring into the new system has been slow — they are nevertheless very powerful tools.

Outside DHS and DoD, departments and agencies have more difficulty using cyber-specific hiring authorities, exacerbating hiring and retention challenges. Organizations such as the FBI, State Department, and Treasury Department all must rely on more limited hiring authorities and pay flexibilities. Per 5 U.S.C. §3304, the president, acting through OPM, has the authority to establish direct-hire authority when there is a critical hiring need or a severe shortage of candidates. OPM has used this authority to provide agencies with greater flexibility when hiring IT and cyber professionals, but these authorities are far more limited than those DoD and DHS have used to establish a cyber-specific excepted service system. OPM has also established government-wide guidelines for direct hiring for positions that fall within designated IT-specific categories, known as federal occupational series:

- 2210 – IT management (information security) at the GS-9 level and above
- 2210 – IT cybersecurity specialist at the GS-12 level and above when they "require IT knowledge and IT competencies," the work is coded to include cybersecurity functions according to both the NICE Framework-aligned codes and OPM's Guide to Data Standards, and cybersecurity work is performed the majority of the time
- 0854 – computer engineers (cybersecurity) at the GS-12 level and above
- 1550 – computer scientists (cybersecurity) at the GS-12 level and above
- 0855 – electronics engineers (cybersecurity) at the GS-12 level and above[123]

While these direct-hire authorities cover many positions, qualification requirements limit their real-world impact. In all four categories, candidates must qualify at the GS-9 level or above, meaning candidates must have relevant education (typically a master's or doctorate degree), experience, or training (such as certifications or skills training). Officially, OPM stipulates that entry-level candidates may qualify for 2210 cyber positions with an associate's or bachelor's degree or even with informal education.[124] However, in practice, many hiring managers report that the GS-9 floor to qualify for cyber direct-hiring authorities is interpreted as a degree requirement. Three of the four categories require GS-12 qualifications, an even higher bar. Although the underlying problem may be a misapplication of classification and qualifications policy related to cyber work, the overall effect is that departments and agencies have struggled to develop effective entry-level hiring pathways that align with the types of candidates they are designed to attract.

Given that often unavoidable security clearance requirements already narrow the field of potential applicants in federal cyber hiring, degree- and experience-based requirements for cyber positions (whether due to misinterpretation of guidance or actual bureaucratic limitations) serve only to further shrink the applicant pool and limit the opportunity to develop entry-level hiring pathways. These requirements are unnecessarily constraining in a field where associate's degrees, industry certifications, and other informal education are both common and valued, and where demonstrations of experience come in vastly different forms and timelines. They also compound the challenge of promoting diversity in the federal workforce by steering hiring toward graduates of STEM degree programs, which also struggle with diversity.[125]

Additionally, the existing direct-hire authorities do not help hiring managers fill roles that fall outside these occupational series but work on cyber policy, privacy, stakeholder engagement, or many other fields that are core to the cyber mission and are reflected as such in the NICE Framework. These positions often require specialized experience or technical competencies but usually do not require technical work.

Finally, the occupational coding structure for cyber positions often drives hiring managers to label many of these non-technical roles as "2210 – IT specialist," which deters potentially qualified applicants from considering these federal cyber jobs because the job announcements are off-putting, implying that applicants need to write code, analyze malware, or architect a secure IT network, for example. Officially, policy does permit departments and agencies to prescribe alternative titling to be used. In particular, a series of parenthetical designations can add some clarity to position titles.[126] However, hiring managers continue to report concerns that the titles assigned to their vacant positions do not accurately reflect the work.

Much like how some direct-hire authorities exist but fall short of the mark, compensation flexibilities exist but do not fully meet the needs of departments and agencies. OPM has created pay flexibilities that serve as important tools for cyber recruitment and retention. Benefits such as federal student loan repayment programs and other incentives can be tied to criteria outside of these IT-specific occupational series. For example, federal employers can offer a group of positions aligned to the NICE Framework a retention incentive of up to 10 percent of basic pay.[127] However, recruitment and retention incentives are distinct from special pay rates, which would raise the base pay rate for a subset of employees. Without a pre-established special pay rate, hiring managers have a limited ability to increase the base rate of pay for their cyber workforce, despite the competition for these in-demand employees from the private sector.

OPM staff are to be sincerely commended for providing the direct-hire authorities and pay flexibility options currently available while still meeting the complex system of requirements and constraints that govern federal hiring. Amid frustrations in cyber hiring, this achievement often goes unrecognized but reflects sincere dedication, persistence, and knowledge. However, the process of implementing direct-hire authority and pay flexibilities continues to stymie cyber hiring managers, especially those attempting to hire cyber professionals who fall outside IT-specific positions. Direct-hire authorities for many positions in cyber policy, risk management, or partner engagement remain unavailable. Where direct-hire authorities and pay flexibility are available, further support is needed to help understaffed offices and their HR teams navigate the process.

5.1 – NCD Should Work With OPM to Modernize Cyber-Specific Coding Structures, Hiring Authorities, and Special Pay Rates Government-Wide

The NCD, OMB, and OPM should, working together and in continual consultation with department and agency leaders, implement one of the following three options to improve the flexibility and agility of federal cyber hiring, engaging Congress as needed:

- Expand the coverage of existing government-wide cyber direct-hire authorities to include all positions that carry at least one NICE Framework cybersecurity work role, thus expanding the authority beyond the 2210, 0854, 1550, and 0855 occupational series.[128] With the support of the NCD and department and agency leaders, OPM would need to significantly expand outreach to hiring and HR managers to ensure that experience, industry certifications, and other indicators are actively used to help applicants without a bachelor's degree meet qualification standards for 2210 cyber positions and related direct-hire authorities. The resulting system would also need to be augmented with special pay rates for the most in-demand roles.
- Create an entirely new family of occupational classifications for cyber work, dispensing with 2210 as an umbrella for cyber work. The new classifications would encompass positions working on cyber issues that fall within other existing classifications (federal professionals working on policy, law, etc.) and should align with the NICE Framework for these areas to the greatest extent possible. In this case, direct-hire authorities and special pay rates would need to be expanded across all the newly created positions (except those already considered to be excepted service positions). This could be reinforced with a congressional mandate. In this option, special attention should be given to the ability of individuals to move in and out of the new job family. Because cyber work spans numerous existing occupational series, an individual's career path might move between some roles within a cyber series and others outside of it. Accordingly, the establishment of a new occupational series that groups those many cyber roles together would require very carefully designed, flexible requirements. Similarly, adjacent roles in non-cyber classification series would likely also require adjustment to accommodate this increased flexibility.
- Work with congressional authorizers to create an overarching program for cyber excepted service positions, decoupling hiring and pay from educational and time-in-job requirements. In essence, this option would take the authorities that underpin CTMS and CES and expands them to the whole of the federal government.

The first solution improves the incumbent system by alleviating a major challenge to federal hiring managers but does not fundamentally change the structural challenges with the system. The second would alleviate many of those challenges by updating the existing system. Both of these options would be significant, yet nevertheless partial, fixes. The third solution, while initially the most difficult to enact, would provide useful and lasting results.

5.2 – NCD Should Work With OPM to Establish a Cadre of Human Resources Specialists Trained in Cyber Hiring and Talent Management

In any of the pathways for restructuring policies, tools, and flexibilities described above, federal HR experts across departments and agencies will need a thorough understanding of the new systems to use them to best effect. As such, the NCD and OPM should expand efforts to build a cadre of HR specialists government-wide who are responsible for filling positions with cyber talent and for providing HR support to those positions. Having these HR specialists would reinforce many of the recommendations in this section. For example, they would help improve consistency in data collection and strengthen the connective tissue between departments and agencies needed to advance the work of the leadership structures proposed above. Departments and agencies can further support this cadre and the overall effort by ensuring HR offices are staffed adequately to enable knowledge transfer throughout staff turnover. The NCD should work with OPM and in consultation with the Chief Human Capital Officers Council, the Chief Information Officers Council, and the Chief Learning Officers Council to establish a training program for this cadre of HR specialists. Furthermore, the NCD should work with OMB to provide additional funding, program administration personnel, and other resources to establish and maintain the program.

5.3 – NCD Should Work With OPM, OMB, and the Appropriations Committees to Ensure Adequate Resourcing

In any of the three options presented in Recommendation 5.1, OPM will need support from congressional appropriators to fund the additional personnel and resourcing needed to create these new structures. OPM will also need the NCD to serve as its champion as it works to reconcile discrepancies between how hiring has conventionally been done in the federal government and the agility that departments and agencies require in their cyber talent management. Recommendation 5.2 will be key to ensuring that new structures are implemented effectively but will also add to the staffing requirements stacking up on OPM's doorstep.

Recommendations for Congress

While this report focuses predominantly on recommendations for the NCD, the executive branch cannot operate without authorization and appropriation from Congress.

Historically, Congress has played a central role in specific areas of cyber workforce development. For example, congressional appropriators have annually stepped up to reject CISA's request to eliminate the CETAP budget. However, Congress could take a more active role in other areas. For example, the GAO has twice reported concerns about department and agency efforts to implement FCWAA and has separately raised issues regarding DHS implementation of the Homeland Security Cybersecurity Workforce Assessment Act of 2014.[129] GAO issued these reports in 2018 and 2019, yet Congress has neither authorized nor demanded major changes in the subsequent years. The GAO further notes that "[n]one of the 24 Chief Financial Officers (CFO) Act agencies have fully implemented best practices for information technology (IT) or cybersecurity workforce planning, including ensuring staff have the skills to address cybersecurity risks and challenges in areas such as industrial control systems supporting the electric grid and avionics cybersecurity."[130] Congress' track record in establishing and continuing existing programs is strong; however, there is much more Congress could do in terms of providing oversight, improvement, and growth for cyber workforce activities in the federal government.

As such, to support federal cyber workforce development, Congress should take the following actions:

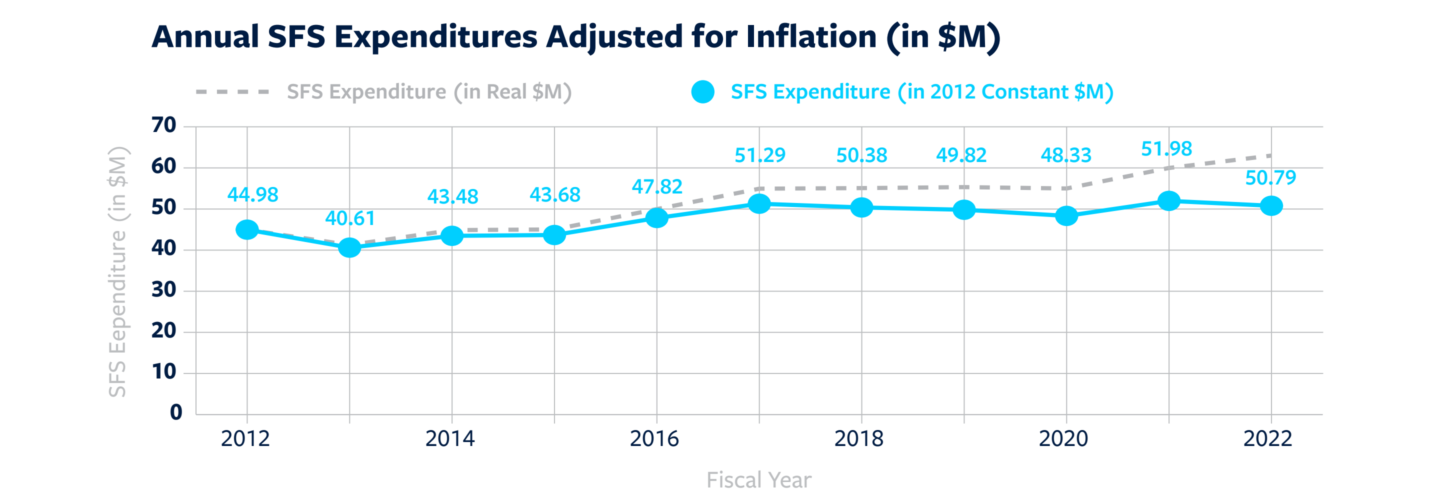
6.1 – Congress Should Amend the Federal Cybersecurity Workforce Assessment Act of 2015

As discussed in Recommendation 1, changes to FCWAA would significantly improve the quality of data available on the federal cyber workforce. As a first order, Congress should extend FCWAA, which is due to sunset this year,[131] to at least 2027. Congress should then require departments and agencies to include an estimate of the number of cyber professionals needed to reach staffing goals (funded and unfunded) and the number of vacant cyber positions, in addition to the currently required information on work roles of critical need. This requirement to estimate the number of personnel needed to reach target staffing levels would help improve long-term workforce planning efforts. To the extent that there is a gap between funded positions and target staffing levels, Congress should anticipate funding requests from department and agency leaders working to close those gaps.

6.2 – Congress Should Increase Support for the CyberCorps: Scholarship for Service Program

To advance this critical program, Congress can take several individual actions:

- **Appropriate for Long-Term Growth**: Adjusting for inflation, the SFS program saw a total budget increase of $5.81 million from FY12 to FY22.[132] In light of the obvious national security implications of the current cyber workforce shortage, such limited program growth for a central pillar of the federal response to that shortage is alarming. The program's structure scales well, building long-term capacity for cyber education even as it graduates workers in the immediate future. It is long past time for Congress to appropriate funds to enable real growth of the SFS program. H.R. 5421, the America COMPETES Act of 2022, outlines an appropriations plan that would reach $90 million by FY26.[133] The Cyberspace Solarium Commission previously recommended a much more ambitious increase, growing the program's budget by $20 million in a single year rather than over five.[134] Nevertheless, any significant increase is welcome after years of minimal growth in this critical cyber workforce development program.
- **Expand Rather Than Replicate**: As a testament to the success of SFS, proposals have emerged to replicate the idea in adjacent fields of study.[135] Rather than creating redundant core structures and risking dividing already scarce resources, NSF should incorporate other areas of emerging technology into the existing SFS program. In fact, SFS has already added new programs incorporating these topics. For example, Oakland University is now home to Cyber Defense of Intelligent Systems;[136] Fordham University received a grant for a program called Preparing Future Cybersecurity Professionals with Data Science Expertise;[137] and Georgia State University now hosts a program for Cybersecurity Workforce Preparation in the Age of Artificial Intelligence.[138] Not only can the current program be adapted to incorporate new fields of study — it is already moving in that direction. However, every addition of new fields of study must be accompanied by additional funding increases for the overall SFS program.



Data sourced from the National Science Foundation

- **Focus on Distributed, Not Centralized, Education**: SFS is known for graduating federal cyber talent, but it also serves a secondary function. Through SFS, grants are awarded to institutions, which in turn may use a small portion of the award to build their cyber programs. The rest must go to scholarships for participating students. While the program-building portion may be smaller than the scholarship,[139] it can significantly improve national cyber educational capacity when used to build on participating institutions' existing infrastructure. Using this distributed model to build capacity across all its grantees, the SFS program offers benefits to students and communities across the country. Moreover, by improving the cybersecurity programs of participating institutions, the program serves to infuse talent throughout the national cybersecurity ecosystem at no extra cost to taxpayers. Most importantly, it does all this using existing academic infrastructure, with no need to invest in new construction or start-up costs.

6.3 – Congress Should Provide Incentives to Develop Entry-Level Employees Into Mid-Career Talent

While many elements of cyber workforce development have presented persistent challenges, one of the most intractable has been employers' reticence to hire and train entry-level candidates, instead focusing on the perceived shortage of experienced professionals. This preference for mid-career talent is visible in industry surveys indicating overwhelming preference for hands-on experience relative to other job candidate qualities.[140] It also appears in patterns of demand for professional certifications, with mid- and late-career certifications far more in-demand than their early-career counterparts.[141] The effect is a disconnect between jobseeker qualifications and the experience employers are seeking. To increase the supply of mid-career talent, employers necessarily must invest in hiring and developing entry-level employees until those employees become mid-career talent.

Congress can incentivize employers to hire and invest in early-career employees as a way to increase the future pool of mid-career professionals. Examples of such incentives could include grants for employers that invest in cyber training programs targeting early-career individuals.[142] In particular, grant funding could prioritize non-traditional programs that would provide a beneficial proof-of-concept for other employers. Similarly, Congress could direct funding to a training partner rather than to employers to spur the development of experienced partners and make such options more available to other private-sector employers. Other incentives could include awarding federal contracting preference to companies that invest in significant training capabilities.

Much like their private-sector counterparts, federal employers would also benefit from a push to invest in early-career talent development. To address this, Congress could authorize a Federal Cyber Workforce Development Institute. By centralizing cyber workforce development resources such as curricula and providing work role-specific training, such a program can make it easier for federal employers to prepare newly hired early-career personnel for federal cyber work roles. Federal programs could also include additional support for upskilling and reskilling.[143] In any of these options, a key consideration must be outreach and engagement to ensure potential beneficiaries are aware of the incentive.

6.4 – Congress Should Strive for Clarity in Roles and Responsibilities for Cyber Workforce Development

As discussed above, one of the major challenges facing the NCD regarding cyber workforce development is the lack of clarity between the respective roles of different federal departments and agencies. Through a clear strategy and leadership structures, the

NCD can address much of this challenge; however, it cannot be done without congressional support, because the authorization of these roles is fundamentally congressional jurisdiction. As different committees and members work to address the cyber workforce gap, an abundance of good intentions and informed efforts can still manifest as the authorization of duplicative and competing programs. Much as there is no clear committee of jurisdiction for cyber issues, there is no clear committee of jurisdiction for cyber workforce issues, which exacerbates the intermingling of roles currently playing out among departments and agencies.

The Cyberspace Solarium Commission recommended the establishment of House Permanent Select and Senate Select Committees on Cybersecurity.[144] Cyber workforce development is one of many examples that illustrate the necessity of such a drastic change. Recognizing that such a change is not imminent, Congress can still work to build greater awareness across committees of existing cyber workforce development efforts underway in different departments and agencies. The consolidation of coordination under the auspices of the NCD can serve as a key resource for ensuring Congress has a single point of contact from which to obtain the information necessary to avoid duplication or confusion of federal roles in cyber workforce development.

6.5 – Congress Should Exercise Oversight of Federal Cyber Workforce Development in Each Department and Agency

In the absence of a single congressional authorizing committee for cybersecurity, congressional focus on federal cyber workforce development tends to fall to a collection of committees that have a major oversight role in various aspects of cybersecurity. However, these are not the only committees that have a responsibility for cyber workforce oversight. Every federal department and agency has a role to play in cybersecurity, and thus each should be considering its resources for cyber workforce development. In the larger federal agencies, this role can grow to encompass hundreds or even thousands of cyber-specific employees. In addition, departments that serve as Sector Risk Management Agencies (SRMAs) in support of national critical infrastructure cybersecurity need specific in-house cyber talent to manage public-private collaboration. SRMAs include organizations as diverse as the Department of Agriculture, the Environmental Protection Agency, and the General Services Administration. In execution of its oversight role, Congress should be asking each federal department and agency about its cyber workforce capabilities and resource requirements. Congress can further support the NCD by exercising its oversight role to encourage cross-agency workforce practices, awareness, collaboration, and innovation.

6.6 – Congress Should Establish Cyber Excepted Service Authorities Government-Wide

As discussed in Recommendation 5, the structure of OPM's occupational designations for cybersecurity work significantly limits the utility of existing direct-hire authorities. Recommendation 5.1 lays out three possible paths forward for OPM and the NCD. Two of these three options could be carried out without new authorizing legislation (although a congressional mandate could be helpful in any case). However, the most beneficial option, creating a government-wide cyber excepted service, cannot be done without new authorizing legislation from Congress. This option would maximize the federal government's flexibility in hiring and managing cyber talent, by creating systems built for the cyber workforce. Such an approach could dramatically improve the federal government's ability to attract and retain self-taught talent, community college graduates, and the many public service-minded professionals for whom the greatest recruitment incentive is the ability to constantly develop and improve their skills but who cannot justify the pay cut that leaving the private sector would entail. When aligned to the NICE Framework to the greatest extent possible, this system would also mitigate challenges in measuring and planning for the cyber workforce. Although this option has its own drawbacks — for example, employees hired into excepted service roles may encounter difficulties moving to competitive service jobs later in their careers — ultimately, the flexibility outweighs the drawbacks given the magnitude and urgency of the cyber hiring challenge. There is strong precedent for this change, as DHS and DoD have enjoyed similar authorities since 2014 and 2015, respectively.[145] Drawing on these precedents, Congress should make these authorities available across the federal workforce.

6.7 – Congress Should Expand Appropriations for Existing Efforts in Cyber Workforce Development

While innovation and the establishment of new federal workforce programs will be essential, Congress should also focus on supporting programs it has already authorized. Recommendation 6.1 above discusses appropriations for the CyberCorps: Scholarship for Service program. Congress has authorized several other very promising programs, but many still lack sufficient funding. For example, in 2020, the Cyberspace Solarium Commission recommended that Congress codify CETAP within CISA.[146] With the hard work and support of members of Congress and their staffs, lawmakers did so under Section 1719 of the FY21 National Defense Authorization Act[147] and reinstated the budget for the program in the FY22 omnibus bill.[148] As discussed above, however, funding for this program has often been in question. As the National Academy of Public Administration recommends, DHS, CISA, and OMB "should sustain funding for CETAP in the President's budget request."[149] Such funding, of course, requires support from congressional appropriators, who will need to continue to set aside the executive branch's inexplicable decisions to eliminate the program or move it to NSF.[150] Similarly, the newly authorized RAMPS program will require attention from congressional appropriators in order to achieve results. The CBO estimated this program would cost $12 million per year,[151] but the FY22 omnibus bill report specified only $500,000 for the new program.[152] As with many cyber workforce development provisions, real progress will take real investment.

Recommendations for the Private Sector

Progress on cyber workforce development cannot advance in a government silo. The public-sector cyber workforce is a subset of the larger national workforce, so the NCD must be a part of the community of federal departments and agencies working with private-sector partners to address national cyber workforce challenges. Moreover, the NCD's strategic intent includes working with "the private sector to inform and drive initiatives that depend on the expertise, authorities, and resources of all parties."[153] This is a fundamentally two-sided exercise, and so this memo offers the recommendations below for private-sector partners.

The private sector can play an important role in providing job experience, hiring entry-level talent, and growing these employees into mid-career professionals. To a certain extent, this will require the private sector to accept a greater degree of risk in its HR functions as companies incorporate new hiring and professional development practices. Spending more to develop each employee increases the risk of losing that investment to poaching by a competing employer. But as more employers invest in the cyber workforce, particularly in the early-career years, the risk to the community as a whole is diminished. By facilitating collaboration across sectors and interfacing with other elements of the federal government, the NCD can reduce the risk to the community as a whole and support this transition.

7.1 – Partners in the Private Sector Should Increase Their Investment in the Cyber Workforce

The NCD cannot address the shortfall of cyber professionals without proactive and invested partners in the private sector. Some exemplary companies are already rising to this challenge:

- Microsoft, for example, has pledged to provide financial assistance to students pursuing community college degrees and industry certifications.[154] The company will also offer training for faculty at community colleges and provide them with free cybersecurity curricula and materials. This endeavor's ultimate goal is to recruit an ambitious 250,000 people into the workforce by 2025.[155] The Microsoft Philanthropies Technology Education and Literacy in Schools program sets another valuable precedent by bringing computer science educational resources to over 500 high schools per year.[156]
- The Cyber Talent Initiative, a collaborative effort between Accenture, Mastercard, Microsoft, and Workday, is a public-private coalition that offers tuition assistance and work experience in both public- and private-sector workplaces.[157]
- As a part of its Global University Programs, IBM has provided training on technology-related topics, including cybersecurity, to more than 247 faculty members at Historically Black Colleges and Universities.[158]

As private-sector leaders begin to distinguish themselves by investing in their early-career cyber workforce, the NCD can help pave the way for others to join. For example, the NCD could ensure that contracting requirements do not limit federal contractors' ability to hire graduates from community colleges, apprenticeship programs, or other alternatives to a bachelor's degree. By helping to cut through this type of red tape, which inhibits the federal government from aligning with innovative solutions emerging from academia and the private sector, the NCD can help these new private-sector investments and solutions achieve success.

7.2 – Partners in the Private Sector Should Develop Shared Resources

One of the best ways that employers can lower the costs of investing in their own workforce, and particularly in early-career talent, is to collaborate with one another. Many small companies that require only small teams of cyber professionals may not have the time or money to invest in a bespoke in-house training program. But when that burden is shared across several similar organizations with a shared geography, industry, or personnel need, consortium-based investment in the cyber workforce becomes more viable.

Pockets of innovative workforce investments are already emerging. For example, apprenticeship programs are beginning to gain real traction nationally.[159] Many of these programs are sponsored by an educational institution — often a university, community college, or local workforce development agency — that partners with several local employers to provide on-the-job training for early-career professionals. By participating in such programs, even small employers can develop a process for building early-career employees into seasoned, mid-career assets to their companies. Employers who are ready to step up to the challenge and grow cyber talent internally should reach out to their local cyber apprenticeship program sponsors.

Appendix: Model Legislative Text

Federal Cybersecurity Workforce Data Collection

Legend: This proposal extends the Federal Cybersecurity Workforce Assessment Act of 2015 and adds a requirement that federal departments and agencies shall provide information not only on the number of cybersecurity professionals employed and the number of posted jobs open, but also on the number of cybersecurity employees needed by the department or agency to optimally staff cybersecurity mission areas. The proposal also tasks the National Cyber Director, in cooperation with the Director of the Office of Personnel Management, with reviewing the assignment of cyber-specific employment codes to ensure consistent application of the codes across departments and agencies, and requires a GAO report after three years.

SEC. _. FEDERAL CYBERSECURITY WORKFORCE DATA COLLECTION

(a) The Federal Cybersecurity Workforce Assessment Act of 2015 (5 U.S.C. 301 note) is amended—

(1) In Section 304 in the matter preceding Subsection (a) by adding "And Projected Vacancy Data" before the period at the end;

(2) In Section 304(a)—

(A) in the matter preceding paragraph (1) by—

(i) striking "2022" and inserting "2028"; and

(ii) inserting "the National Cyber Director," after "in consultation with the Director,";

(B) redesignating paragraph (2) as paragraph (3);

(C) in paragraph (1) striking the word "and"; and

(D) adding the following new paragraph (2):

"(2) provide a count of projected funded and unfunded vacancies, regardless of critical need, for positions that—

"(A) require the incumbent to perform, manage, or supervise functions that execute information technology, cybersecurity, or cyber-related responsibilities, and

"(B) have been assigned an employment code according to Section 303 of this Title; and"

(3) In Section 304(a)(3) (as so designated)—

(A) in the matter preceding subparagraph (A) by inserting "and the National Cyber Director" after "to the Director";

(B) in subparagraph (A), by striking "and" at the end;

(C) in subparagraph (B), by striking the "." at the end and inserting ";" at the end; and

(D) by inserting after subparagraph (B) the following new subparagraphs (C) and (D):

"(C) provides the number of vacancies identified per paragraph (2); and

"(D) provides the number of additional positions within the agency that would need to be funded in order to enable the agency to fulfill its cybersecurity mandate to the fullest extent possible.".

(4) By adding after Section 304(c)(2), a new Subsection (d):

"(d) Federal Cybersecurity Workforce Data Dashboard.—Not later than one year after the enactment of this act, the Director, in coordination with the National Cyber Director, will establish and make available to federal departments and agencies an interactive digital resource to share information gathered pursuant to Subsection (a). The digital resource shall—

"(1) Present data updated no less frequently than once per year to align with the reports submitted per Subsection (a), and the Director is encouraged to work with departments and agencies to update the data with greater frequency;

"(2) Provide data on each cybersecurity work role in the federal government coded according to the structure established in Section 303 (b) including vacancy rates and skill gaps;

"(3) To the greatest extent possible, provide the data needed to inform department and agency cybersecurity workforce policies with empirical analytics;

"(4) Provide a central repository of Office of Personnel Management materials relevant to cybersecurity workforce management, including relevant guidance, tools, coding structures, resources, and other materials as the Director, in coordination with the National Cyber Director, deems appropriate; and

"(5) Such other functions as the Director, in coordination with the National Cyber Director, deems necessary.".

(b) Review of Employment Coding.—Not later than 18 months after the date of enactment of this section, the National Cyber Director, in coordination with the Director of the Office of Personnel Management, shall provide an assessment of the process for, and findings of, the National Cybersecurity Workforce Measurement Initiative required by Section 303 of the Federal Cybersecurity Workforce Assessment Act of 2015 that—

(1) describes the degree of consistency in the process used by heads of Federal departments and agencies in identifying the positions required and assigning employment codes;

(2) identifies barriers to applying the required employment codes according to a consistent interpretation of the work roles described in the coding structure;

(2) outlines any limitations on the utility of the employment codes and subsequent data collection efforts resulting from the methodology and consistency of the initiative; and

(3) recommends actions, legislative changes, and/or policy changes that may be taken to improve consistency in the assignment of the employment codes and improve data collection on the federal cybersecurity workforce.

(c) GAO Review.—Not later than three years after the date of enactment of this section, the Comptroller General of the United States shall submit a report to the appropriate congressional committees that describes the status of—

(1) implementation of the Federal Cybersecurity Workforce Assessment Act of 2015; and

(2) any changes recommended by the National Cyber Director and Director of the Office of Personnel Management pursuant to the reporting requirement in Subsection (b).

Federal Cyber Workforce Development Institute

Legend: This proposal requires the National Cyber Director to develop a plan to establish an institute within the federal government that will serve as a centralized resource and training center for federal cyber workforce development.

SEC. _. FEDERAL CYBER WORKFORCE DEVELOPMENT INSTITUTE

(a) Requirement.—

(1) In General.—Not later than 180 days from the date of enactment of this section, the National Cyber Director, in consultation with the Secretary of Homeland Security, the Secretary of Defense, the Secretary of Commerce, the Director of the Office of Personnel Management, and such other department and agency heads as the National Cyber Director determines necessary, shall produce a plan for a federal institute to provide training for personnel hired for cyber work roles and other federal cyber workforce development tools.

(2) Institute Functions.—The federal workforce development institute described in the plan required under paragraph (1) shall—

(A) provide work role-specific training, including hands-on learning and skill-based assessments, to prepare personnel from a wide variety of academic and professional backgrounds to perform effectively in federal cyber work roles;

(B) coordinate with the Secretary of Homeland Security, the Secretary of Defense, and other federal department and agency heads as the Director deems necessary to develop work role-specific curriculum for the training required in subparagraph (A);

(D) prioritize entry-level positions in the provision of curriculum and training, but may also include curriculum development and training for mid- to late-career positions, and may include upskilling and reskilling efforts;

(D) incorporate work-based learning in personnel training; and

(E) develop a badging system to communicate qualification and proficiency for individuals who successfully complete training through the institute.

(3) Plan Elements.—The plan required under paragraph (1) shall—

(A) recommend an organizational placement for the institute, which may include a single federal department or agency or a combination of federal departments and agencies;

(B) to the greatest extent possible, align training and tools described with the taxonomy, including work roles and competencies and the associated tasks, knowledge, and skills, from the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity (NIST Special Publication 800–181, Revision 1), or successor framework.

(C) identify—

(i) elements of the institute and its functions that can draw on existing facilities, resources, and programs in the federal government, and

(ii) elements of the institute and its functions that cannot effectively be implemented using existing facilities, resources, and programs in the federal government and therefore would need to be newly established in order to implement the plan required under paragraph (1);

(D) describe the recruitment considerations, pay flexibilities, and hiring authorities required to ensure federal departments and agencies can effectively recruit, enroll individuals in training, and place individuals who have successfully completed training in positions appropriate to the individual's qualifications and training received through the institute;

(E) recommend a governance structure for the institute to ensure ongoing interagency coordination on the development of curriculum, provision of training, and such other considerations as the Director deems appropriate; and

(F) provide an estimate of the funding required to establish and operate the institute.

(b) Briefing.—Not later than 270 days from the date of enactment of this section, the National Cyber Director shall provide to the appropriate congressional committees a briefing on the plan required under Subsection (a) including an estimate of the funding and such authorities as may be necessary to implement the plan.

(c) Definitions.— In this section:

(1) Appropriate Congressional Committees.— The term "appropriate congressional committees" means—

(A) the Committee on Armed Services of the Senate;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate;

(C) the Committee on Armed Services of the House of Representatives;

(D) the Committee on Homeland Security of the House of Representatives; and

(E) the Committee on Oversight and Reform of the House of Representatives.

(2) Director.— The term "Director" means the National Cyber Director.

(3) Work-Based Learning.—The term "work-based learning" has the meaning given the term in Section 3 of the Carl D. Perkins Career and Technical Education Act of 2006 (20 U.S.C. 2302).

(4) Work Role.— The term 'work role' means a specialized set of tasks and functions requiring specific knowledge, skills, and abilities.

Federal Cyber Excepted Service

Legend: This proposal mandates the establishment of a government-wide excepted service for cyber-specific roles as designated by the (pre-existing) cyber role coding structure aligned to the NICE Cybersecurity Workforce Framework. This proposal is adapted from existing legislation and draws extensively from the model put forward in Section 3 of the Border Patrol Agent Pay Reform Act of 2014 and in Section 1107 of the National Defense Authorization Act for Fiscal Year 2016.

SEC. _. FEDERAL CYBER EXCEPTED SERVICE ACT

(a) Short Title.—This section may be cited as the "Federal Cyber Excepted Service Act".

(b) Definitions.—In this section:

(1) Appropriate committees of Congress.—The term "appropriate committees of Congress" means the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the House Committee on Oversight and Reform and the Committee on Appropriations of the House of Representatives.

(2) Director.—The term "Director" means the National Cyber Director.

(3) Collective bargaining agreement.—The term "collective bargaining agreement" has the meaning given that term in Section 7103(a)(8) of Title 5, United States Code.

(4) Excepted service.—The term "excepted service" has the meaning given that term in Section 2103 of Title 5, United States Code.

(5) Preference eligible.—The term "preference eligible" has the meaning given that term in Section 2108 of Title 5, United States Code.

(6) National Initiative for Cybersecurity Education.—The term "National Initiative for Cybersecurity Education" means the initiative under the national cybersecurity awareness and education program, as authorized under Section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451).

(7) Work Roles.—The term "work roles" means a specialized set of tasks and functions requiring specific knowledge, skills, and abilities.

(8) Qualified position.—The term "qualified position" means a position—

(A) in which the incumbent performs, manages, or supervises functions that execute information technology, cybersecurity, or cyber-related responsibilities, and

(B) aligned to a work role, or sharing the majority of necessary duties, tasks, or competencies with a work role, in the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity (NIST Special Publication 800–181, Revision 1), an expansion of that framework, or successor framework.

(9) Senior executive service.—The term 'Senior Executive Service' has the meaning given that term in Section 2101a of Title 5, United States Code.

(c) Sense of Congress.—It is the sense of Congress that—

(1) Flexibility in federal cyber hiring has seen only limited improvement, despite efforts such as the Federal Cybersecurity Workforce Assessment Act of 2015, which was intended to address underlying systemic challenges to addressing the shortfall of cyber professionals in the federal government;

(2) While Section 3 of the Border Patrol Agent Pay Reform Act of 2014 and Section 1107 of the National Defense Authorization Act for Fiscal Year 2016 have become important tools for hiring cyber talent at the Department of Homeland Security and Department of Defense, respectively, comparable flexibilities are not available outside these two departments;

(3) Current government-wide direct hire authorities for cyber positions are predicated on occupational classifications that are not well-suited to cyber hiring, and thus current direct hire authorities for cyber are unduly limited; and

(4) Government-wide pay flexibilities limited to recruitment, relocation, and retention are important tools in cyber talent management, but these temporary solutions cannot fully address federal cyber hiring without creating flexibility in setting base pay rates for cyber positions.

(d) General Authority.—

(1) Provide guidelines, establish positions, appoint personnel, and fix rates of pay.—

(A) General authority.—The Director, in coordination with the Director of the Office of Personnel Management and the Federal Chief Information Officer, shall—

(i) establish a Federal Cyber Excepted Service;

(ii) coordinate with the Secretary of Defense and the Secretary of Homeland Security to ensure the Federal Cyber Excepted Service established in clause (i) benefits from the lessons learned from the establishment of—

(I) the Cyber Talent Management System authorized by Section 3 of the Border Patrol Agent Pay Reform Act of 2014, and

(II) the Cyber Excepted Service as authorized by National Defense Authorization Act for Fiscal Year 2016; and

(iii) prescribe regulations for the administration of this section, including for–

(I) establishing qualified positions in the Federal Cyber Excepted Service,

(II) appointing individuals to qualified positions,

(III) fixing the compensation of an individual for service in a qualified position, and

(IV) other such regulations as the Director determines appropriate.

(B) Federal departments and agencies.—In accordance with the guidance established in subparagraph (A), each head of a Federal department or agency may—

(i) establish, as positions in the excepted service within that Federal department or agency, such qualified positions as the head of that Federal department or agency determines necessary to carry out responsibilities relating to cyber, including positions formerly identified as—

(I) senior level positions designated under Section 5376 of Title 5, United States Code; and

(II) positions in the Senior Executive Service;

(ii) appoint an individual to a qualified position (after taking into consideration the availability of preference eligibles for appointment to the position); and

(iii) subject to the requirements of paragraphs (2) and (3), fix the compensation of an individual for service in a qualified position.

(C) Construction with other laws.—The authorities provided under this subsection apply without regard to the provisions of any other law relating to the appointment, number, classification, or compensation of employees.

(2) Basic pay.—

(A) Authority to fix rates of basic pay.—In accordance with this section and the guidance established in subparagraph (1)(A), the head of a Federal department or agency shall fix the rates of basic pay for any qualified position established under paragraph (1)—

(i) in relation to the rates of pay provided for employees in comparable positions in that Federal department and agency in which the employee occupying the comparable position performs, manages, or supervises functions that execute cyber responsibilities,

(ii) and subject to the same limitations on maximum rates of pay established for such employees by law or regulation.

(B) Additional Compensation, Incentives, and Allowances.—

(i) The Secretary may provide employees in qualified positions compensation (in addition to basic pay), including benefits, incentives, and allowances, consistent with, and not in excess of the level authorized for, comparable positions authorized by Title 5.

(ii) An employee in a qualified position whose rate of basic pay is fixed under Subsection (2)(A) shall be eligible for an allowance under Section 5941 of Title 5 on the same basis and to the same extent as if the employee was an employee covered by such section, including eligibility conditions, allowance rates, and all other terms and conditions in law or regulation.

(3) Additional compensation, incentives, and allowances.—

(A) Additional compensation based on Title 5 authorities.—The Secretary may provide employees in qualified positions compensation (in addition to basic pay), including benefits, incentives, and allowances, consistent with, and not in excess of the level authorized for, comparable positions authorized by Title 5, United States Code.

(B) Allowances in nonforeign areas.—An employee in a qualified position whose rate of basic pay is fixed under paragraph (2)(A) shall be eligible for an allowance under Section 5941 of Title 5, United States Code, on the same basis and to the same extent as if the employee was an employee covered by such Section 5941, including eligibility conditions, allowance rates, and all other terms and conditions in law or regulation.

(4) Plan for execution of authorities.—Not later than 270 days after the date of enactment of this section, the Director, in consultation with the Director of the Office of Personnel Management, the Federal Chief Information Officer, and the heads of such federal departments and agencies as the Director determines relevant, shall submit a report to the appropriate committees of Congress with a plan for the use of the authorities provided under this subsection.

(5) Collective bargaining agreements.—Nothing in paragraph (1) may be construed to impair the continued effectiveness of a collective bargaining agreement with respect to a Federal department or agency, or any office, component, subcomponent, or successor thereof.

(e) Annual Report.—Not later than 2 years after the date of enactment of this section, and every year thereafter for 4 years, the Director shall submit to the appropriate committees of Congress a detailed report that—

(1) discusses the process used by heads of Federal departments and agencies in accepting applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by an individual for a qualified position;

(2) describes—

(A) how the Director, working with heads of Federal departments and agencies, plans to fulfill the critical need to recruit and retain employees in qualified positions;

(B) the measures that will be used to measure progress; and

(C) any actions taken during the reporting period to fulfill such critical need;

(3) discusses how the planning and actions taken under paragraph (2) are integrated into the Director's strategic workforce planning;

(4) provides metrics on actions occurring during the reporting period, including—

(A) the number of employees in qualified positions hired by occupation and grade and level or pay band;

(B) the placement of employees in qualified positions by Federal department or agency, including information on subcomponents of Federal departments and agencies as applicable;

(C) the total number of veterans hired;

(D) the number of separations of employees in qualified positions by occupation and grade and level or pay band;

(E) the number of retirements of employees in qualified positions by occupation and grade and level or pay band; and

(F) the number and amounts of recruitment, relocation, and retention incentives paid to employees in qualified positions by occupation and grade and level or pay band;

(5) describes the training provided to supervisors of employees in qualified positions on the use of the new authorities; and

(6) describes the impact of the new authorities on diversity and access recruitment and retention efforts.

(f) Three-Year Probationary Period.—The probationary period for all employees hired under the authority established in this section shall be 3 years.

(g) Incumbents of Existing Competitive Service Positions.—

(1) In general.—An individual serving in a position on the date of enactment of this section that is selected to be converted to a position in the excepted service under this section shall have the right to refuse such conversion.

(2) Subsequent conversion.—After the date on which an individual who refuses a conversion under paragraph (1) stops serving in the position selected to be converted, the position may be converted to a position in the excepted service.

(h) Authorization of Appropriations.—There is authorized to be appropriated $1,500,000 for each of fiscal years 2021 and 2022, the use of which may include additional personnel or contract support at the Office of Personnel Management as may be necessary to establish and administer regulations for the administration of this section.

(i) Conforming Amendment.—Section 3132(a)(2) of Title 5, United States Code, is amended in the matter following subparagraph (E)—

(1) in clause (iii), by striking “or” at the end;

(2) in clause (iv), by inserting “or” after the semicolon; and

(3) by inserting after clause (iv) the following new clause:

> “(v) any position established as a qualified position in the excepted service by the National Cyber Director under the Federal Cyber Excepted Service Act;”.

Endnotes

1. Martin C. Libicki, David Senty, and Julia Pollak, "Hackers Wanted: An Examination of the Cybersecurity Labor Market," *RAND Corporation*, 2014. (https://www.rand.org/pubs/research_reports/RR430.html)

2. "A Resilient Cybersecurity Profession Charts the Path Forward," *International Information System Security Certification Consortium*, 2021, page 21. (https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx)

3. U.S. Cyberspace Solarium Commission, "Growing a Stronger Federal Cyber Workforce," September 2020. (https://www.cybersolarium.org/public-communications/workforce-white-paper)

4. For the purposes of this memorandum, "NCD" refers to both the national cyber director and the Office of the National Cyber Director.

5. See, for example, the indicators of progress detailed in: U.S. Cyberspace Solarium Commission, "2021 Annual Report on Implementation," August 2021. (https://www.cybersolarium.org/public-communications/2021-annual-report-on-implementation)

6. This memorandum notes that the *cyber* workforce and the *cybersecurity* workforce are very closely related but different groups. While the memorandum will not attempt to provide a definition of each, it generally refers to the cybersecurity workforce as a subset of the cyber workforce and is primarily concerned with this broader population. Note, however, that when drawing on data, quotations, initiatives, or other references to external work, the memorandum will use the terminology from those sources to avoid misconstruing original intent. Although this approach allows the report to draw from the best sources available while still keeping references in context, readers should note that it does, in some cases, impact the way information should be interpreted. For example, the memorandum's introduction cites data on the size of the *cybersecurity* workforce and *cybersecurity* workforce gap. The cyber workforce, by contrast, is not as well studied but is larger. In short, throughout the paper, the authors use the best available information, noting that it does lead to variability in definitions.

7. Figure based on 597,767 total cybersecurity job openings nationally compared to 1,053,468 total employees in the cybersecurity workforce. Data sourced from: "Cybersecurity Supply/Demand Heat Map," *CyberSeek*, accessed May 4, 2022. (https://www.cyberseek.org/heatmap.html)

8. Ibid.

9. See, for example: "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce," *Partnership for Public Service and Booz Allen Hamilton*, July 2009, page 19. (https://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In-Security__Strengthening_the_Federal_Cybersecurity_Workforce-2009.07.22.pdf); "Cyber In-Security II: Closing the Federal Talent Gap," *Partnership for Public Service and Booz Allen Hamilton*, April 2015, page 2. (https://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In-Security_II__Closing_the_Federal_Talent_Gap-2015.04.13.pdf); U.S. 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: Building the Foundation for a More Secure American Future," November 16, 2017. (https://www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf); U.S. Cyberspace Solarium Commission, "Growing a Stronger Federal Cyber Workforce: CSC White Paper #3," September 2020. (https://www.cybersolarium.org/public-communications/workforce-white-paper)

10. Cybersecurity Enhancement Act of 2014, Pub. L. 113-274, 128 Stat. 2971, codified as amended at 15 U.S.C. §7421. (https://www.congress.gov/bill/113th-congress/senate-bill/1353/text)

11. Consolidated Appropriations Act of 2016, Pub. L. 114-113, 129 Stat. 2975, codified as amended at 5 U.S.C. §301. (https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf)

12. America Creating Opportunities for Manufacturing, Pre-Eminence in Technology, and Economic Strength Act of 2022, H.R. 4521, §§10304(f)–(h), 117th Congress (2022). (https://www.congress.gov/bill/117th-congress/house-bill/4521)

13. Federal Cybersecurity Workforce Expansion Act, H.R. 5138, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/house-bill/5138/text?r=28&s=1); Federal Cybersecurity Workforce Expansion Act, S. 2274, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/senate-bill/2274/text)

14. See, for example: U.S. Senate Committee on Appropriations, "Explanatory Statement for the Homeland Security Appropriations Bill, 2022," 2021, page 82. (https://www.appropriations.senate.gov/imo/media/doc/DHSRept_FINAL.PDF)

15. See, for example: 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," *Robert H. Smith School of Business*, 2011. (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.nedaglobal.com/assets/files/New_site_PDFs/The-Pipeline-Women-Count-2020-FINAL-VERSION.pdf)

16. See: U.S. Cyberspace Solarium Commission, "Report of the U.S. Cyberspace Solarium Commission," March 2020. (https://www.cybersolarium.org/reports-and-white-papers); U.S. Cyberspace Solarium Commission, "Growing a Stronger Federal Cyber Workforce: CSC White Paper #3," September 2020. (https://www.cybersolarium.org/public-communications/workforce-white-paper)

17. "Future of the Federal IT Workforce Update," *Federal CIO Council*, May 2020. (https://www.cio.gov/assets/resources/Future_of_Federal_IT_Workforce_Update_Public_Version.pdf)

[18] U.S. Department of Commerce, National Institute of Standards and Technology, “Strategic Plan (2021-2025),” accessed May 4, 2022. (https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan)

[19] U.S. Federal Cyber Workforce Management Working Group, “State of the Federal Cyber Workforce: A Call for Collective Action,” Forthcoming 2022.

[20] See, for example: Nicole Sganga, “Women make up just 24% of the cyber workforce. CISA wants to fix that.” *CBS News*, March 20, 2022. (https://www.cbsnews.com/news/cyber-workforce-cisa-director-jen-easterly); Jory Heckman, “Cyber workforce ranks among least diverse segments of federal government,” *Federal News Network*, January 25, 2022. (https://federalnewsnetwork.com/workforce/2022/01/cyber-workforce-ranks-among-least-diverse-segments-of-federal-government)

[21] “Diversity, Equity, and Inclusion in Cybersecurity,” *Aspen Institute*, September 2021, page 4. (https://www.aspeninstitute.org/wp-content/uploads/2021/09/Diversity-Equity-and-Inclusion-in-Cybersecurity_9.921.pdf)

[22] “Women in Cybersecurity,” *International Information System Security Certification Consortium*, April 2019. (https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=4C3B33AABFBEAFDDA211856CB274EBDDF9DBEB38)

[23] “Federal Workforce,” *Partnership for Public Service*, 2019. (https://ourpublicservice.org/wp-content/uploads/2019/08/FedFigures_FY18-Workforce.pdf)

[24] U.S. Department of Commerce, National Institute of Standards and Technology, “NICE Community,” October 4, 2021. (https://www.nist.gov/itl/applied-cybersecurity/nice/community)

[25] U.S. Department of Commerce, National Institute of Standards and Technology, “Implementation Plan: NICE Strategic Plan,” November 2020. (https://www.nist.gov/system/files/documents/2021/09/23/Implementation%20Plan_22Sep2021.pdf)

[26] The National Academy of Public Administration identified this same trend, observing that “existing interagency mechanisms primarily facilitate information exchange and may not successfully promote reaching an agreement on strategies and approaches to address present challenges.” See: “A Call to Action: The Federal Government’s Role in Building a Cybersecurity Workforce for the Nation,” *National Academy of Public Administration*, January 2022, page 38. (https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf)

[27] “Cybersecurity Supply/Demand Heat Map,” *CyberSeek*, accessed May 4, 2022. (https://www.cyberseek.org/heatmap.html)

[28] Consolidated Appropriations Act of 2016, Pub. L. 114-113, 129 Stat. 2975, codified as amended at 5 U.S.C. §301. (https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf)

[29] Note that some departments and agencies, including most intelligence community agencies, have pre-existing agency-wide alternative hiring systems.

[30] While this memorandum principally deals with federal activities, note that state, local, tribal, and territorial governments face a compounded version of this challenge. These actors play a critical role in public-sector cybersecurity and face very stark hiring challenges. See, for example, workforce data in: “2020 Deloitte-NASCIO Cybersecurity Study,” *Deloitte and the National Association of Chief Information Officers*, 2020. (https://www.nascio.org/wp-content/uploads/2020/10/2020-Deloitte-NASCIO-Cybersecurity-Study-1.pdf)

[31] U.S. Department of Commerce, National Institute of Standards and Technology, “National Initiative for Cybersecurity Education (NICE),” accessed May 4, 2022. (https://www.nist.gov/itl/applied-cybersecurity/nice)

[32] U.S. Department of Commerce, National Institute of Standards and Technology, “NICE Framework Resource Center,” accessed May 4, 2022. (https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center)

[33] See, for example: “National Initiative for Cybersecurity Education (NICE) Workforce Framework,” *Australian Cyber Security Growth Network*, accessed May 4, 2022. (https://www.austcyber.com/resources/dashboards/NICE-workforce-framework)

[34] The Cybersecurity Competitions to Yield Better Efforts to Research the Latest Exceptionally Advanced Problems, or Cyber LEAP, are a series of challenges authorized by Section 9407 of the FY21 NDAA. One of the challenges focuses on cyber training.

[35] U.S. Congress, “Division A—Agriculture, Rural Development, Food and Drug Administration, and Related Agencies Appropriations Act, 2014,” *Congressional Record*, 113th Congress, Volume 160, Number 9, Book II, January 15, 2014. (https://www.congress.gov/113/crec/2014/01/15/160/9/CREC-2014-01-15-pt2-PgH475-2.pdf)

[36] U.S. Office of Personnel Management, “Interpretive Guidance for Cybersecurity Positions: Attracting, Hiring and Retaining a Federal Cybersecurity Workforce,” October 11, 2018. (https://www.opm.gov/policy-data-oversight/classification-qualifications/reference-materials/interpretive-guidance-for-cybersecurity-positions.pdf)

[37] U.S. Office of Personnel Management, “Hiring Information: Direct Hire Authority,” accessed May 4, 2022. (https://www.opm.gov/policy-data-oversight/hiring-information/direct-hire-authority/#url=Governmentwide-Authority); U.S. Office of Personnel Management, “Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals,” accessed May 4, 2022. (https://www.opm.gov/policy-data-oversight/pay-leave/reference-materials/handbooks/compensation-flexibilities-to-recruit-and-retain-cybersecurity-professionals.pdf)

[38] Consolidated Appropriations Act of 2016, Pub. L. 114-113, 129 Stat. 2975, codified as amended at 5 U.S.C. §301. (https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf)

39. The group draws on representation from the 24 executive branch agencies specified in the Chief Financial Officers Act. See: Chief Financial Officers Act of 1990, Pub. L. 101-576, 104 Stat. 2838, codified as amended at 31 U.S.C. §501. (https://www.congress.gov/101/statute/STATUTE-104/STATUTE-104-Pg2838.pdf)

40. Data provided in email correspondence with NSF, April 1, 2022.

41. U.S. Office of Personnel Management, "CyberCorps: Scholarship for Service," accessed May 4, 2022. (https://www.sfs.opm.gov/default.aspx)

42. According to CyberSeek, there were 38,655 open positions in the public sector as of May 4, 2022. "Cybersecurity Supply/Demand Heat Map," *CyberSeek*, accessed May 4, 2022. (https://www.cyberseek.org/heatmap.html)

43. U.S. National Science Foundation, "FY 2020 NSF Budget Request to Congress," March 2019. (https://nsf.gov/about/budget/fy2020/pdf/14_fy2020.pdf)

44. U.S. National Science Foundation, "National Science Foundation: FY 2021 Budget Request to Congress," February 2020. (https://nsf.gov/about/budget/fy2021/pdf/fy2021budget.pdf)

45. U.S. National Science Foundation, "National Science Foundation: FY 2022 Budget Request to Congress," May 2021. (https://www.nsf.gov/about/budget/fy2022/pdf/fy2022budget.pdf)

46. U.S. Congress, "Division B—Commerce, Justice, Science, and Related Agencies Appropriations Act, 2022," 2022, page 146. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-B.pdf)

47. National Science Foundation, "National Science Foundation: FY 2021 Budget Request to Congress," February 2020. (https://nsf.gov/about/budget/fy2021/pdf/fy2021budget.pdf); U.S. Congress, "Division B—Commerce, Justice, Science, and Related Agencies Appropriations Act, 2021," 2020, page 132. (https://docs.house.gov/billsthisweek/20201221/BILLS-116RCP68-JES-DIVISION-B.pdf)

48. See, for example: Executive Order 13870, "America's Cybersecurity Workforce," May 2, 2019. (https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce); President Joseph Biden, "Remarks by President Biden on Collectively Improving the Nation's Cybersecurity," *Remarks to the Press*, August 25, 2021. (https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/25/remarks-by-president-biden-on-collectively-improving-the-nations-cybersecurity)

49. U.S. Cyberspace Solarium Commission, "Report of the U.S. Cyberspace Solarium Commission," March 2020. (https://www.cybersolarium.org/reports-and-white-papers); U.S. Cyberspace Solarium Commission, "Growing a Stronger Federal Cyber Workforce: CSC White Paper #3," September 2020. (https://www.cybersolarium.org/public-communications/workforce-white-paper)

50. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388, codified as amended at 6 U.S.C. §1719. (https://www.congress.gov/bill/116th-congress/house-bill/6395/text)

51. Data provided by Cyber.org personnel in email exchanges on November 4, 2021, and April 4, 2022.

52. Eric Goldstein, "America Under Cyber Siege: Preventing and Responding to Ransomware Attacks," *Testimony Before the U.S. Senate Committee on the Judiciary*, July 27, 2021. (https://www.judiciary.senate.gov/meetings/america-under-cyber-siege-preventing-and-responding-to-ransomware-attacks)

53. See, for example: U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Budget Overview, Fiscal Year 2022, Congressional Justification," 2021, page 183. (https://www.dhs.gov/sites/default/files/publications/cybersecurity_and_infrastructure_security_agency_0.pdf)

54. U.S. Senate Committee on Appropriations, "Explanatory Statement for the Homeland Security Appropriations Bill, 2022," 2021. (https://www.appropriations.senate.gov/imo/media/doc/DHSRept_FINAL.PDF)

55. U.S. Congress, "Division F—Department of Homeland Security Appropriations Act, 2022," 2022, page 57. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-F.pdf)

56. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Budget Overview, Fiscal Year 2023, Congressional Justification," 2022, page 176. (https://www.dhs.gov/sites/default/files/2022-03/Cybersecurity%20and%20Infrastructure%20Security%20Agency%20%28CISA%29_Remediated.pdf)

57. Data provided by Cyber.org personnel in email exchanges on November 4, 2021, and April 4, 2022.

58. U.S. Department of Commerce, National Institute of Standards and Technology, "Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS)," March 3, 2020. (https://www.nist.gov/itl/applied-cybersecurity/nice/regional-alliances-and-multistakeholder-partnerships-stimulate-ramps)

59. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388, codified as amended at 6 U.S.C. §9401(f). (https://www.congress.gov/bill/116th-congress/house-bill/6395/text)

60. U.S. Congressional Budget Office, "Cost Estimate: S.2775, HACKED Act of 2019," January 31, 2020. (https://www.cbo.gov/system/files/2020-01/s2775.pdf). The HACKED Act does include provisions beyond the regional alliances program. The CBO estimated that these activities would cost an additional $7 million over a five-year period.

61. U.S. Department of Commerce, National Institute of Standards and Technology, "National Institute of Standards and Technology, National Technical Information Service, Fiscal Year 2022 Budget Submission to Congress," 2021. (https://www.commerce.gov/sites/default/files/2021-06/fy2022_nist_congressional_budget_justification.pdf)

62. U.S. Congress, "Division B—Commerce, Justice, Science, and Related Agencies Appropriations Act, 2022," 2022, page 13. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-B.pdf)

63. U.S. Department of Commerce, National Institute of Standards and Technology, "National Institute of Standards and Technology, National Technical Information Service, Fiscal Year 2023 Budget Submission to Congress," 2022, page 37. (https://www.commerce.gov/sites/default/files/2022-03/FY2023-NIST-NTIS-Congressional-Budget-Submission.pdf)

64. National Centers of Academic Excellence in Cybersecurity Community, "The Initiatives Guide 2022," 2022. (https://www.caecommunity.org/sites/default/files/2022-02/NCAE-C_Initiatives_Guide_2022.pdf)

65. "Cybersecurity Education Diversity Initiative (CEDI)," *Fordham Center for Cybersecurity*, accessed May 4, 2022. (https://www.fordham.edu/fcc/cedi)

66. U.S. Department of Defense, Defense Information Systems Agency, "DoD Cyber Scholarship Program (DoD CySP)," accessed May 4, 2022. (https://public.cyber.mil/cw/cdp/dcysp)

67. For a more exhaustive list, see: "A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation," *National Academy of Public Administration*, January 2022, page 74. (https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf)

68. "A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation," *National Academy of Public Administration*, January 2022. (https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf)

69. Ibid.

70. The Career Technical Education CyberNet program "seeks to increase the number of career and technical education (CTE) teachers who can effectively prepare students for cybersecurity education and careers." See: U.S. Department of Education, Office of Career, Technical, and Adult Education, Perkins Collaborative Resource Network, "CTE CyberNet," accessed May 4, 2022. (https://cte.ed.gov/initiatives/cte-cybernet)

71. Note that there may be beneficial changes in future iterations of this program and the FY22 funding appropriated for CISA. See: Natalie Alms, "Lessons of the Cyber Reskilling Academy," *FCW*, September 23, 2021. (https://fcw.com/articles/2021/09/23/lessons-reskilling-academy.aspx); U.S. Congress, "Division F—Department of Homeland Security Appropriations Act, 2022," 2022, page 57. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-F.pdf)

72. U.S. Department of Commerce, National Institute of Standards and Technology, "The Federal Information Systems Security Educators' Association (FISSEA)," 2017. (https://csrc.nist.rip/organizations/fissea/home/index.shtml)

73. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388, codified as amended at 6 U.S.C. §1752. (https://www.congress.gov/bill/116th-congress/house-bill/6395/text)

74. This memorandum focuses predominantly on recommended priorities and changes to enable the NCD to guide overall initiatives of the U.S. government. As such, the memorandum does not focus at length on new initiatives that could be created. For high-impact lines of work that the U.S. government might pursue under the NCD's direction, see the goals of the National Initiative for Cybersecurity Education Strategic plan, several of which are reinforced by the elements and focus areas of the National Academy of Public Administration. See: U.S. Department of Commerce, National Institute of Standards and Technology, "Strategic Plan (2021-2025)," accessed May 4, 2022. (https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan); "A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation," *National Academy of Public Administration*, January 2022, page 20. (https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf)

75. Note that this report is not the first to highlight this gap. See, for example: Shaun Donovan, Beth F. Cobert, and Tony Scott, U.S. Executive Office of the President, Office of Management and Budget, Memorandum for Heads of Executive Departments and Agencies, "Federal Cybersecurity Workforce Strategy," July 12, 2016, page 3. (https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-15.pdf)

76. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388, codified as amended at 6 U.S.C. §1752 (c)(1)(C)(ii). (https://www.congress.gov/bill/116th-congress/house-bill/6395/text)

77. Deriving meaningful insights regarding the outcomes and impacts of programs is, of course, very challenging, even in a data-rich environment. Many factors beyond the programs themselves can cause the federal cyber workforce to grow or shrink, so evaluating the programs' effectiveness would require significant quantitative and qualitative analysis. This memorandum's call for greater data collection should not be taken to imply that these insights will result naturally from collecting more data or that federal decision makers will have perfect visibility into the impact of their programs. Rather, it is indicating a starting point toward data-driven policy.

78. Consolidated Appropriations Act of 2016, Pub. L. 114-113, 129 Stat. 2975, codified as amended at 5 U.S.C. §301. (https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf)

79. See, for example, the letter from the Department of Homeland Security in response to a 2019 GAO report. The letter details the challenge of mapping positions to the prescribed NICE Cyber Workforce Framework while position descriptions still must align to the far more generalized occupational classifications OPM uses for most hiring and personnel management actions. Letter available in: U.S. Government Accountability Office, "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs," March 2019, page 64. (https://www.gao.gov/assets/700/697462.pdf)

80. U.S. Department of Commerce, National Institute of Standards and Technology, "NICE Framework Resource Center," accessed May 4, 2022. (https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center)

81. OPM released guidance in 2018 that does provide some help in aligning the two systems by allowing departments and agencies to consider the NICE Framework designations as criteria for classifying federal cyber work, though this guidance has not substantially changed the contours of the problem. See: U.S. Office of Personnel Management, "Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need," April 2018. (https://chcoc.gov/sites/default/files/Attachment%20to%20Memo%20-%20Guidance%20for%20Identifying%20Addressing%20Reporting%20Cyb..._.pdf)

82. Consolidated Appropriations Act of 2016, Pub. L. 114-113, 129 Stat. 2975, codified as amended at 5 U.S.C. §301. (https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf)

83. U.S. Office of Personnel Management, "Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need," April 2018. (https://chcoc.gov/sites/default/files/Attachment%20to%20Memo%20-%20Guidance%20for%20Identifying%20Addressing%20Reporting%20Cyb..._.pdf)

84. Notably, OPM has endeavored to address this gap by requiring departments and agencies not only to report their work roles of critical need, but also to identify the reasons for their personnel shortages. Departments and agencies are further required to develop an action plan to ameliorate those shortages.

85. U.S. Department of Commerce, National Institute of Standards and Technology, "Updated Workforce Framework for Cybersecurity: NIST SP 800-181 Revision 1," November 16, 2020. (https://csrc.nist.gov/News/2020/updated-workforce-framework-for-cybersecurity)

86. U.S. Department of Commerce, National Institute of Standards and Technology, "Federal Cybersecurity Coding Structure," October 18, 2017. (https://www.nist.gov/file/394236)

87. Beth F. Cobert, "Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions," January 4, 2017. (https://www.chcoc.gov/content/guidance-assigning-new-cybersecurity-codes-positions-information-technology-cybersecurity)

88. U.S. Department of Commerce, National Institute of Standards and Technology, "Strategic Plan: 2022-2026," page 34. (https://www.commerce.gov/sites/default/files/2022-03/DOC-Strategic-Plan-2022%E2%80%932026.pdf)

89. "Cybersecurity Supply/Demand Heat Map," *CyberSeek*, accessed May 4, 2022. (https://www.cyberseek.org/heatmap.html)

90. U.S. Cyberspace Solarium Commission, "Report of the U.S. Cyberspace Solarium Commission," March 2020, page 43. (https://www.cybersolarium.org/reports-and-white-papers)

91. U.S. Cyberspace Solarium Commission, "Growing a Stronger Federal Cyber Workforce: CSC White Paper #3," September 2020, pages 18-19. (https://www.cybersolarium.org/public-communications/workforce-white-paper)

92. "A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation," *National Academy of Public Administration*, January 2022, page 42. (https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf)

93. Including NICE Framework work roles wherever possible.

94. See, in particular: "A Resilient Cybersecurity Profession Charts the Path Forward," *International Information System Security Certification Consortium*, 2021. (https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx); Information Systems Audit and Control Association, Press Release, "New ISACA Study Finds Cybersecurity Workforce Minimally Impacted by Pandemic, but Still Grappling with Persistent Hiring Challenges," May 4, 2021. (https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2021/new-isaca-study-finds-cybersecurity-workforce-minimally-impacted-by-pandemic-but-still-grappling)

95. Irvin Lachow, "Diversity in the Cyber Workforce: Addressing the Data Gap," *The MITRE Corporation*, January 2022. (https://www.mitre.org/publications/technical-papers/diversity-in-the-cyber-workforce-addressing-the-data-gap)

96. America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science Reauthorization Act of 2010, Pub. L. 111-358, codified as amended at 42 U.S.C. 1861, §505. (https://www.congress.gov/bill/111th-congress/house-bill/5116)

97. While some efforts are already working to measure the cybersecurity workforce (for example, CyberSeek), this data is predominantly drawn from open job postings. Accordingly, the data may reflect a bias insofar as many roles may be badly needed but, due to bureaucratic or other factors, may not be reflected in active job postings. Furthermore, data on the composition, demographics, academic and professional background, and other key characteristics of the current workforce are very limited.

98. CyberSeek provides a very important starting point for data collection, but there is ample space for further efforts. CyberSeek does not, in general, provide demographic data on the cyber workforce. Because job postings provide the site's primary source of data, CyberSeek is broadly limited to describing the workforce that employers are seeking. Accordingly, much is still unknown about the current composition of the workforce and the dynamics, such as retention, that drive it.

99. "A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation," *National Academy of Public Administration*, January 2022, page 36. (https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf)

100. Ibid., page 41.

101. Ibid., page 40.

102. U.S. Department of Commerce, National Institute of Standards and Technology, "NICE Community Coordinating Council," accessed May 4, 2022. (https://www.nist.gov/itl/applied-cybersecurity/nice/community/community-coordinating-council). This recommendation draws on the National Academy of Public Administration's cited report and is, in principle, well-founded in seeking to include these important non-federal stakeholders. However, for the purposes of functionality among federal stakeholders, the NCD should avoid steps that would require implementation of the Federal Advisory Committee Act (FACA). That is, functionality as a coordination mechanism among federal stakeholders should be the priority given a choice between triggering FACA and not including non-federal stakeholders.

103. "A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation," *National Academy of Public Administration*, January 2022, page 41. (https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf)

104. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Cyber Career Pathways Tool," accessed May 4, 2022. (https://niccs.cisa.gov/workforce-development/cyber-career-pathways)

105. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388, codified as amended at 6 U.S.C. §1752 (c)(1)(C)(iii). (https://www.congress.gov/bill/116th-congress/house-bill/6395/text)

106. Ellen Nakashima, "Biden's new cyber czar is pushing for collective defense inside government and out," *The Washington Post*, October 28, 2021. (https://www.washingtonpost.com/national-security/inglis-national-cyber-director-plans/2021/10/27/af7da21a-373c-11ec-9bc4-86107e7b0ab1_story.html)

107. These efforts should be coordinated with other White House offices and councils as appropriate, including, for example, the Office of Science and Technology Policy and the National Economic Council.

108. U.S. Department of Commerce, "National Institute of Standards and Technology, National Technical Information Service, Fiscal Year 2022 Budget Submission to Congress," 2021. (https://www.commerce.gov/sites/default/files/2021-06/fy2022_nist_congressional_budget_justification.pdf); U.S. Department of Commerce, "National Institute of Standards and Technology, National Technical Information Service, Fiscal Year 2023 Budget Submission to Congress," 2022, page 37. (https://www.commerce.gov/sites/default/files/2022-03/FY2023-NIST-NTIS-Congressional-Budget-Submission.pdf); U.S. Congressional Budget Office, "Cost Estimate: S.2775, HACKED Act of 2019," January 31, 2020. (https://www.cbo.gov/system/files/2020-01/s2775.pdf)

109. Mark Montgomery, "Critical cybersecurity education program turns 21," *Federal News Network*, January 8, 2021. (https://federalnewsnetwork.com/commentary/2021/01/critical-cybersecurity-education-program-turns-21)

110. For a selection of examples, see: "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce," *Partnership for Public Service and Booz Allen Hamilton*, July 2009, page 19. (https://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In-Security__Strengthening_the_Federal_Cybersecurity_Workforce-2009.07.22.pdf); "Cyber In-Security II: Closing the Federal Talent Gap," *Partnership for Public Service and Booz Allen Hamilton*, April 2015, page 2. (https://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In-Security_II__Closing_the_Federal_Talent_Gap-2015.04.13.pdf)

111. "A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation," *National Academy of Public Administration*, January 2022, page 19. (https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf)

112. Shaun Donovan, Beth F. Cobert, and Tony Scott, U.S. Executive Office of the President, Office of Management and Budget, Memorandum for Heads of Executive Departments and Agencies, "Federal Cybersecurity Workforce Strategy," July 12, 2016, page 3. (https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-15.pdf)

113. "Future of the Federal IT Workforce Update," *CIO Council*, May 2020. (https://www.cio.gov/assets/resources/Future_of_Federal_IT_Workforce_Update_Public_Version.pdf)

114. U.S. Department of Commerce, National Institute of Standards and Technology, "Strategic Plan (2021-2025)," accessed May 4, 2022. (https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan)

115. Ibid.

116. “A Call to Action: The Federal Government’s Role in Building a Cybersecurity Workforce for the Nation,” *National Academy of Public Administration*, January 2022, page 57. (https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf)

117. In fact, this data was already collected pursuant to Executive Order 13800, which charged the secretaries of commerce and homeland security with jointly assessing the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related educational curricula, training, and apprenticeship programs, from primary through higher education.” See: U.S. Executive Order 13800, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” May 11, 2017. (https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce)

118. To encourage the development of a strategy that prioritizes rather than catalogs efforts, the NCD should consider consulting with leaders outside the conventional workforce development conversation. Board and operational leaders, for example, may provide unique insights into these challenges.

119. John Hewitt Jones, “Cyber Talent Management System expected to produce results ‘within months,’ DHS leader says,” *Fedscoop*, November 17, 2021. (https://www.fedscoop.com/cyber-talent-management-system-expected-to-produce-results-within-months-dhs-leader-says)

120. Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113-277, 128 Stat. 2995, codified as amended at 5 U.S.C. §101. (https://www.congress.gov/bill/113th-congress/senate-bill/1691/text)

121. National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, 129 Stat. 726. (https://www.congress.gov/bill/114th-congress/senate-bill/1356/text)

122. U.S. Department of Defense, Defense Information Systems Agency, “DoD Cyber Excepted Service (CES),” accessed May 4, 2022. (https://public.cyber.mil/cw/dod-cyber-excepted-service-ces)

123. U.S. Office of Personnel Management, “Governmentwide Authority,” accessed May 4, 2022. (https://www.opm.gov/policy-data-oversight/hiring-information/direct-hire-authority/#url=Governmentwide-Authority)

124. This is further reinforced, in principle, by OPM’s implementation guidance for a 2019 executive order that calls for departments and agencies to “scale back reliance upon educational qualifications as a substitute for competencies in the Federal hiring process.” See: Kiran A. Ahuka, U.S. Office of Personnel Management, Memorandum for Heads of Executive Departments and Agencies, “Updated Interim Guidance - E.O. 13932; Modernizing and Reforming the Assessment and Hiring of Federal Job Candidates,” December 29, 2021. (https://www.chcoc.gov/content/updated-interim-guidance-eo-13932-modernizing-and-reforming-assessment-and-hiring-federal)

125. Richard Fry, Brian Kennedy, and Cary Funk, “STEM Jobs See Uneven Progress in Increasing Gender, Racial and Ethnic Diversity,” *Pew Research Center*, April 1, 2021. (https://www.pewresearch.org/science/2021/04/01/stem-jobs-see-uneven-progress-in-increasing-gender-racial-and-ethnic-diversity)

126. U.S. Office of Personnel Management, “Interpretive Guidance for Cybersecurity Positions: Attracting, Hiring and Retaining a Federal Cybersecurity Workforce,” October 11, 2018. (https://www.opm.gov/policy-data-oversight/classification-qualifications/reference-materials/interpretive-guidance-for-cybersecurity-positions.pdf)

127. U.S. Office of Personnel Management, “Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals,” accessed May 4, 2022. (https://www.opm.gov/policy-data-oversight/pay-leave/reference-materials/handbooks/compensation-flexibilities-to-recruit-and-retain-cybersecurity-professionals.pdf)

128. U.S. Department of Commerce, National Institute of Standards and Technology, “Federal Cybersecurity Coding Structure,” October 18, 2017. (https://www.nist.gov/file/394236)

129. 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); 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); U.S. Government Accountability Office, “Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements,” February 6, 2018. (https://www.gao.gov/products/gao-18-175)

130. U.S. Office of Personnel Management, “High Risk Area: Strategic Human Capital Management,” accessed May 4, 2022. (https://www.gao.gov/highrisk/strategic-human-capital-management)

131. Consolidated Appropriations Act of 2016, Pub. L. 114-113, 129 Stat. 2977, codified as amended at 5 U.S.C. §301. (https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf). Depending on the timing, this may be a reauthorization rather than an extension. The last deliverable required by FCWAA was due in April 2022.

132. Data was drawn from NSF annual budget requests and appropriations legislation, as noted below. Inflation was calculated using the Bureau of Labor Statistics' CPI Inflation Calculator, using constant January 2012 dollars measured against January of each subsequent fiscal year. Notably, using the same calculation, the overall NSF budget has grown by about $20 million in 2012 dollars, an increase of about 0.3 percent relative to its FY2012 budget. Accordingly, the solution proposed is not to increase SFS by cannibalizing other NSF programs, but rather to increase appropriations for SFS as a central priority among other funding increases for NSF. See: U.S. National Science Foundation, "FY 2014 NSF Budget Request to Congress," April 10, 2013. (https://nsf.gov/about/budget/fy2014/pdf/03_fy2014.pdf); U.S. National Science Foundation, "Education and Human Resources Funding by Division and Program FY 2014 Request to Congress," May 28, 2021. (https://www.nsf.gov/about/budget/fy2022/pdf/fy2022budget.pdf); U.S. National Science Foundation, "Education and Human Resources Funding by Division and Program: FY 2015 Request," March 10, 2014. (https://nsf.gov/about/budget/fy2015/pdf/12_fy2015.pdf); U.S. National Science Foundation, "Education and Human Resources Funding by Division and Program: FY 2016 Request to Congress," February 2, 2015. (https://nsf.gov/about/budget/fy2016/pdf/12_fy2016.pdf); U.S. National Science Foundation, "Education and Human Resources Funding by Division and Program: FY 2017 Request to Congress," February 9, 2016. (https://nsf.gov/about/budget/fy2017/pdf/12_fy2017.pdf); U.S. National Science Foundation, "Education and Human Resources Funding by Division and Program: FY 2018 Request to Congress," May 23, 2017. (https://nsf.gov/about/budget/fy2018/pdf/11_fy2018.pdf); U.S. National Science Foundation, "Education and Human Resources Funding by Division and Program: FY 2019 Request to Congress," February 28, 2018. (https://nsf.gov/about/budget/fy2019/pdf/15_fy2019.pdf); U.S. National Science Foundation, "Education and Human Resources Funding by Division and Program: FY 2020 Request to Congress," March 18, 2019. (https://nsf.gov/about/budget/fy2020/pdf/14_fy2020.pdf); U.S. National Science Foundation, "Education and Human Resources Funding by Division and Program: FY 2021 Request to Congress," February 10, 2020. (https://nsf.gov/about/budget/fy2021/pdf/14_fy2021.pdf); U.S. National Science Foundation, "National Science Foundation: FY 2022 Budget Request to Congress," May 2021, page 48. (https://www.nsf.gov/about/budget/fy2022/pdf/fy2022budget.pdf); U.S. Congress, "Division B—Commerce, Justice, Science, and Related Agencies Appropriations Act, 2021," 2020, page 145. (https://docs.house.gov/billsthisweek/20201221/BILLS-116RCP68-JES-DIVISION-B.pdf); U.S. Bureau of Labor Statistics, "CPI Inflation Calculator," accessed May 4, 2022. (https://www.bls.gov/data/inflation_calculator.htm)

133. America Creating Opportunities for Manufacturing, Pre-Eminence in Technology, and Economic Strength Act of 2022, H.R. 4521, 117th Congress (2022). (https://www.congress.gov/bill/117th-congress/house-bill/4521/text/eh)

134. In 2020, the Commission recommended an increase of 20 percent annually for 10 years, beginning with an increase of $20 million for FY21. See: U.S. Cyberspace Solarium Commission, "Growing a Stronger Federal Cyber Workforce: CSC White Paper #3," September 2020, page 9. (https://www.cybersolarium.org/public-communications/workforce-white-paper)

135. See, for example: AI Scholarship-for-Service Act, S.3901, 116th Congress (2020). (https://www.congress.gov/bill/116th-congress/senate-bill/3901/text?r=4&s=1)

136. U.S. National Science Foundation, "Award Abstract #2146280 CyberCorps Scholarship for Service: Cyber Defense of Intelligence Systems," January 20, 2022. (https://www.nsf.gov/awardsearch/showAward?AWD_ID=2146280&HistoricalAwards=false)

137. U.S. National Science Foundation, "Award Abstract #2142229 CyberCorps Scholarship for Service: Preparing Future Cybersecurity Professionals with Data Science Expertise," January 20, 2022. (https://www.nsf.gov/awardsearch/showAward?AWD_ID=2142229&HistoricalAwards=false)

138. U.S. National Science Foundation, "Award Abstract #2146497 CyberCorps Scholarship for Service: Cybersecurity Workforce Preparation in the Age of Artificial Intelligence," January 20, 2022. (https://www.nsf.gov/awardsearch/showAward?AWD_ID=2146497&HistoricalAwards=false)

139. Institutions may receive $10,000 per student per year for program expenses. See: U.S. National Science Foundation, "CyberCorps(R) Scholarship for Service (SFS)," accessed May 9, 2022, page 1. (https://www.nsf.gov/pubs/2021/nsf21580/nsf21580.pdf)

140. "A Resilient Cybersecurity Profession Charts the Path Forward," *International Information System Security Certification Consortium*, 2021. (https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx); "State of Cybersecurity 2021 Part 1," *Information Systems Audit and Control Association*, May 4, 2021. (https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko4uEAC)

141. See: "Cybersecurity Supply/Demand Heat Map," *CyberSeek*, accessed May 4, 2022. (https://www.cyberseek.org/heatmap.html)

142. See, for example: Cyber Ready Workforce Act, S.3570, 117th Congress (2022). (https://www.congress.gov/bill/117th-congress/senate-bill/3570/text?r=18&s=1)

143. Veterans are often a focus of such efforts. For more information on these programs and on perceptions surrounding veterans upskilling, see: Jason Dempsey, Katherine L. Kuzminski, Nathalie Grogan, and Cody Kennedy, "Transitioning to Tech: Transitioning Service Members and Veteran Perceptions Regarding a Career in the Technology Sector," *Center for a New American Security*, November 9, 2021. (https://www.cnas.org/publications/reports/transitioning-to-tech)

144. U.S. Cyberspace Solarium Commission, "Report of the U.S. Cyberspace Solarium Commission," March 2020, page 35. (https://www.cybersolarium.org/reports-and-white-papers)

145. See: Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113-277, 128 Stat. 3005, codified as amended at 6 U.S.C. §147. (https://www.congress.gov/bill/113th-congress/senate-bill/1691/text); National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, 129 Stat. 1024, codified as amended at 5 U.S.C. §1599f. (https://www.congress.gov/bill/114th-congress/senate-bill/1356/text)

146. U.S. Cyberspace Solarium Commission, "Growing a Stronger Federal Cyber Workforce: CSC White Paper #3," September 2020, page 20. (https://www.cybersolarium.org/public-communications/workforce-white-paper)

147. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388, codified as amended at 6 U.S.C. §1719. (https://www.congress.gov/bill/116th-congress/house-bill/6395/text)

148. U.S. Congress, "Division F – Department of Homeland Security Appropriations Act, 2022," 2022, page 57. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-F.pdf)

149. "A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation," *National Academy of Public Administration*, January 2022, page 53. (https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf)

150. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Budget Overview, Fiscal Year 2023, Congressional Justification," page 174. (https://www.dhs.gov/sites/default/files/2022-03/Cybersecurity%20and%20Infrastructure%20Security%20Agency%20%28CISA%29_Remediated.pdf)

151. Estimate provided for S. 2775, the HACKED Act of 2019, which was incorporated into the FY21 NDAA. Section 9401(f) authorizes the RAMPS program, for which OMB estimates $10 million in grant outlays each year and $2 million in administrative costs. See: U.S. Congressional Budget Office, "Cost Estimate: S.2775, HACKED Act of 2019," January 31, 2020. (https://www.cbo.gov/system/files/2020-01/s2775.pdf)

152. U.S. Congress, "Division B—Commerce, Justice, Science, and Related Agencies Appropriations Act, 2022," 2022, page 13. (https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-B.pdf)

153. U.S. Executive Office of the President, Office of the National Cyber Director, "A Strategic Intent Statement for the Office of the National Cyber Director," October 2021. (https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf)

154. "Microsoft Cybersecurity Scholarship Program," *Last Mile*, accessed May 4, 2022. (https://www.lastmile-ed.org/microsoftcybersecurityscholarship)

155. Brad Smith, "America faces a cybersecurity skills crisis: Microsoft launches national campaign to help community colleges expand the cybersecurity workforce," *Microsoft*, October 28, 2021. (https://blogs.microsoft.com/blog/2021/10/28/america-faces-a-cybersecurity-skills-crisis-microsoft-launches-national-campaign-to-help-community-colleges-expand-the-cybersecurity-workforce)

156. "TEALS Program," *Microsoft*, accessed May 4, 2022. (https://www.microsoft.com/en-us/teals)

157. "Cybersecurity Talent Initiative," *The Cybersecurity Talent Initiative*, accessed May 4, 2022. (https://cybertalentinitiative.org)

158. "IBM Extends HBCU Initiatives Through New Industry Collaborations," *IBM*, May 7, 2021. (https://newsroom.ibm.com/2021-05-07-IBM-Extends-HBCU-Initiatives-Through-New-Industry-Collaborations)

159. U.S. Department of Commerce, National Institute of Standards and Technology, "NICE Cybersecurity Apprenticeship Program Finder," accessed May 4, 2022. (https://www.nist.gov/nice/apprenticeship-finder)

About the Authors

Laura Bate served as a senior director and task force lead for the congressionally mandated Cyberspace Solarium Commission. Previously, she was a policy analyst with the Cybersecurity Initiative at New America, a policy think tank based in Washington, DC. She is a member of the Mid-Atlantic Affiliate of Women in Cybersecurity and serves as an adjunct faculty member at Georgetown University's School of Foreign Service.

RADM (Ret.) Mark Montgomery serves as senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies. Mark also directs CSC 2.0 — a project established to continue the work of the Cyberspace Solarium Commission — having served as the Commission's executive director. Previously, Mark served as policy director for the Senate Armed Services Committee under the leadership of Senator John S. McCain, coordinating policy efforts on national security strategy, capabilities and requirements, and cyber policy. Mark served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017.

The views of the authors do not necessarily reflect the views of CSC 2.0's distinguished advisors, senior advisors, or any affiliated organizations or individuals.

About CSC 2.0

CSC 2.0 is preserving the legacy and continuing the work of the Cyberspace Solarium Commission (CSC). Congress created the CSC in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The commission operated successfully for two and a half years, publishing its flagship report in March 2020 along with subsequent white papers. The CSC issued more than 80 recommendations to reform U.S. government structures and organization, strengthen norms and non-military tools, promote national resilience, reshape the cyber ecosystem, operationalize public-private collaboration, and preserve and employ military instruments of national power.

At the CSC's planned sunset, the commissioners launched the CSC 2.0 project to support continued efforts to implement outstanding CSC recommendations, provide annual assessments of the implementation of CSC recommendations, and conduct research and analysis on several outstanding cybersecurity issues identified during the commission's tenure.

For more information, visit **www.CyberSolarium.org**.

Co-Chairmen

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

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

Distinguished Advisors

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

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

Partners

FDD

McCRARY INSTITUTE
FOR CYBER AND CRITICAL INFRASTRUCTURE SECURITY

CSC 2.0

Preserving and Continuing the Cyberspace Solarium Commission