A Report by a Panel of the

NATIONAL ACADEMY OF PUBLIC ADMINISTRATION

for the Cybersecurity and Infrastructure Security Agency,
US Department of Homeland Security

A Call to Action

The Federal Government's Role in Building a Cybersecurity Workforce for the Nation

NATIONAL ACADEMY OF
PUBLIC ADMINISTRATION®

January 2022

January 2022

A Report by a Panel of the

NATIONAL ACADEMY OF PUBLIC ADMINISTRATION

for the Cybersecurity and Infrastructure Security Agency,
US Department of Homeland Security

A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation

PANEL OF ACADEMY FELLOWS

Daniel Chenok, *co-chair*

Karen S. Evans, *co-chair*

Dr. Marilu Goodyear

Dr. Costis Toregas

Daniel Weitzner

NATIONAL ACADEMY OF PUBLIC ADMINISTRATION®

Officers of the Academy

David Wennergren,* *Chair of the Board*

William Baity,* *Vice Chair*

David Mader,* *Treasurer*

Jane Fountain,* *Secretary*

Teresa W. Gerton,* *President and Chief Executive Officer*

Study Team

Brenna Isman, *Director of Academy Studies*

Sarah (Sally) Jaggar,* *Project Director*

Maria Rapuano, *Senior Advisor*

Jonathan Tucker, *Senior Research Analyst*

Adam Darr, *Senior Research Analyst*

Allen Harris, *Senior Research Associate*

Elise Johnson, *Senior Research Associate*

Sarah Jacobo, *Intern*

* Academy Fellow

The views expressed in this report are those of the Panel. They do not necessarily reflect the views of the Academy as an institution.

National Academy of Public Administration

1600 K Street, NW
Suite 400
Washington, DC 20006
www.NAPAwash.org

January 2022
Printed in the United States of America
Academy Project Number: 3824

About the Academy

The National Academy of Public Administration is an independent, nonprofit, and nonpartisan organization established in 1967 and chartered by Congress in 1984. It provides expert advice to government leaders in building more effective, efficient, accountable, and transparent organizations. To carry out this mission, the Academy draws on the knowledge and experience of its over 950 Fellows—including former cabinet officers, Members of Congress, governors, mayors, and state legislators, as well as prominent scholars, career public administrators, and nonprofit and business executives. The Academy helps public institutions address their most critical governance and management challenges through in-depth studies and analyses, advisory services and technical assistance, congressional testimony, forums and conferences, and online stakeholder engagement. Learn more about the Academy and its work at www.NAPAwash.org.

Foreword

Cybersecurity is a significant concern for governments, businesses, universities, service providers, and citizens throughout the country. Ransomware attacks and other cyber intrusions are featured in the news almost daily, and there is a growing demand for cybersecurity workers who can protect the electronic systems that enable so many aspects of our lives and our economy. In recognition of these vulnerabilities, the Academy identified as one of its twelve Grand Challenges in Public Administration the need to *Ensure Data Security and Privacy Rights of Individuals*. Yet only recently has the federal government begun to bring together key federal and nonfederal actors to address cybersecurity workforce problems.

As part of the FY 2021 Consolidated Appropriations Act, Congress directed the Department of Homeland Security to contract with the National Academy of Public Administration (or a similar organization) to review the Cybersecurity and Infrastructure Security Agency (CISA) programs (primarily housed within the Cybersecurity Defense Education and Training [CDET] branch) to build a national cybersecurity workforce. The task was to assess the excellence, scalability, and diversity of select CISA/CDET workforce-development programs and to consider alternative models for building a cyber workforce. Our study Panel of Academy Fellows also looked at additional efforts across the government aimed at ensuring the nation's cybersecurity workforce needs are being met. The Academy's Study Team staff performed the research and analysis to inform Panel member analysis and recommendations.

I deeply appreciate our Panel members, who provided valuable guidance and introductions to federal and nonfederal leaders in the cybersecurity workforce development field. The views expressed in this report are those of the Panel. In addition, I would like to acknowledge the time and contributions as subject matter experts of Academy Fellows Franklin Reeder, Director Emeritus and Founding Chair, Center for Internet Security, and Ronald Sanders, Staff Director, The Florida Center for Cybersecurity at the University of South Florida. Both went above and beyond to provide information, context, contacts, and other guidance to the Study Team and Panel.

Last, but far from least, I appreciate the constructive engagement with CISA leaders and experts—including those in CDET—along with current and former federal officials and numerous private sector leaders in related federal, academic, and private sector fields who contributed to the development of this report.

The Panel's report presents findings and recommendations that support the development of an effective cybersecurity workforce for the government and for the nation. The report acknowledges that this can be done only through strong, ongoing national coordination and leadership reaching across federal agencies and the larger economy. I hope these recommendations help build a more robust and resilient cybersecurity workforce to better support the nation's long-term security posture and capabilities.

Teresa W. Gerton
President and Chief Executive Officer
National Academy of Public Administration

A Note from the Panel Co-Chairs

This past year we lost a cybersecurity icon, Alan Paller. As the founder of the SANS Institute, a cooperative for information security thought leadership, Alan was a pioneer in the cybersecurity industry and championed the need for greater education and knowledge for practitioners.

During the development of this study, the Academy team had the opportunity to interview Alan, and many of his views of future workforce needs have been incorporated into the study's analysis and recommendations. Alan's expansive vision and clear articulation of the need for improvements in the cybersecurity field drove success in ways too numerous to specify. He always focused on the workforce that would be needed to execute and maintain the cybersecurity posture of our nation. The impact of his loss on the future development of the cybersecurity workforce is immeasurable.

Alan influenced so many throughout his consequential life and work. We, as Panel Co-chairs, are among those who consider him a great mentor. If the government and the nation achieve a fraction of what Alan believed possible, his memory will indeed be honored. On behalf of the Academy Panel, we dedicate our efforts to his memory.

Daniel Chenok

Karen S. Evans

Table of Contents

List of Tables

List of Figures

Acronyms and Abbreviations

Acronym or Abbreviation	Definition
Academy	National Academy of Public Administration
CAE	Centers of Academic Excellence
CDET	Cybersecurity Defense Education and Training
CETAP	Cybersecurity Education and Training Assistance Program
CISA	Cybersecurity and Infrastructure Security Agency
CTMS	Cybersecurity Talent Management System
DHS	Department of Homeland Security
DoD	Department of Defense
FFRDC	Federally Funded Research and Development Centers
HBCU	Historically Black Colleges and Universities
HSSEDI	Homeland Security Systems Engineering and Development Institute
ICS	Industrial Control Systems
INL	Idaho National Laboratory
K-12	Kindergarten through twelfth grade
NCD	National Cyber Director
NCDU	National Cyber Defense University
NDAA	National Defense Authorization Act
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSF	National Science Foundation
NTTP	Non-Traditional Training Providers
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OPM	Office of Personnel Management
PISCES	Public Infrastructure Security Cyber Education Systems

PNNL	Pacific Northwest National Laboratory
SFS	Scholarship for Service
SLTT	State, local, tribal, and territorial

Executive Summary

Cybersecurity poses one of the most important and urgent challenges of the 21st century. Secure technology and data present key channels for economic growth, citizen engagement, and national security. In contrast, insecure technology and data create vulnerabilities that enable threats and breaches that can disrupt economies, foment citizen distrust in public institutions, and weaken national security. Recent cyberattacks such as SolarWinds, which affected the US Government and organizations around the world in 2020;[1] the Colonial Pipeline ransomware attack in May 2021;[2] and the breach of the Microsoft Exchange Server software by China's main intelligence service, the Ministry of State Security,[3] in March 2021 highlight the vulnerability of the nation's critical infrastructure and computer systems that underpin the American economy and society. The latest vulnerability, "log4j," could result in significant global economic impacts.[4]

The nation must take many actions to meet the cybersecurity challenge. These include technical solutions, like designing software and systems to be more resistant to cyberattacks, applying artificial intelligence capabilities to detect and protect our assets, and educating the general workforce and citizenry about basic cyber hygiene. However, achieving successful security outcomes depends foremost on the workforce that develops and delivers secure applications in government and industry. A professional cybersecurity workforce is critical to an effective national response that seizes this historical moment to address the challenges of cybersecurity.

In recent years, estimates are that half a million cybersecurity positions across the public and private sectors remain unfilled, and the gap is only expected to grow.[5] Within that total number, though, specific information about roles, responsibilities, and competencies that can guide investments is limited. Moreover, public and private demands evolve constantly with rapid changes in technology and practice.

Developing an effective cyber workforce requires a large and integrated multisector effort to clearly identify issues, validate possible solutions, scale efforts, manage costs, and consistently evaluate impact. The total effort also requires flexibility as circumstances change in a dynamic environment. The federal government does not generally operate in a manner consistent with these operational considerations due to its size, complexity, and antiquated human resource

1. David E. Sanger, Nicole Perlroth, Eric Schmitt, "Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit," *The New York Times,* December 14, 2020, updated September 9, 2021, https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.
2. Dustin Volz, "Colonial Pipeline Chief Says Recovery From Ransomware Hack Not Complete," *The Wall Street Journal,* June 8, 2021, https://www.wsj.com/articles/colonial-pipeline-chief-to-testify-in-senate-panel-on-ransomware-hack-11623144602.
3. Eric Tucker, "Microsoft Exchange hack caused by China, US and allies say," *AP News*, July 19, 2021, https://apnews.com/article/microsoft-exchange-hack-biden-china-d533f5361cbc3374fdea58d3fb059f35.
4. CISA Director Jen Easterly called log4j "the most serious vulnerability I have seen in my decades-long career." Tatum Hunter and Gerrit De Vynck, "The 'most serious' security breach ever is unfolding right now. Here's what you need to know.," *The Washington Post*, December 20, 2021, https://www.washingtonpost.com/technology/2021/12/20/log4j-hack-vulnerability-java/.
5. CyberSeek, a National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) program carried out in partnership with Burning Glass and CompTIA, is a commonly cited source of workforce gap data. https://www.cyberseek.org/index.html.

processes. As a result, addressing the cyber workforce challenge will require extraordinary measures.

In this context, the FY 2021 Consolidated Appropriations Act directed the Department of Homeland Security (DHS) to engage the National Academy of Public Administration (Academy) to review the Cybersecurity and Infrastructure Security Agency's (CISA) strategies and programs related to building a national cybersecurity workforce. The Panel of Academy Fellows assembled to guide and oversee this review determined that an effective assessment of CISA's cybersecurity workforce strategy and programs would entail looking more broadly at federal government efforts to help develop the nation's cybersecurity workforce.

The Panel finds that CISA and other agencies have made progress on individual programs. However, there is no government-wide strategy for developing a national cybersecurity workforce to set priorities and focus attention and resources. Absent such a strategy, congressional and agency officials have independently addressed various challenges related to meeting the cybersecurity workforce development needs of the federal government and the nation more broadly. This lack of coordination has created the potential for unnecessary duplication and lost opportunities for leverage and integration across agencies. Moreover, lack of clarity about federal agency roles and responsibilities has hindered the federal government's ability to tap the capabilities and resources in the private sector, academia, and other levels of government.

The recent establishment of the Office of the National Cyber Director (ONCD) in the White House presents an important opportunity to create a government-wide strategy for developing the national cybersecurity workforce. Congress authorized the ONCD and gave it the primary responsibility to advise the President on cybersecurity strategy.[6]

The Panel's report first recommends that the ONCD lead the development of a government-wide strategy for developing the national cybersecurity workforce, in consultation with CISA, the Office of Management and Budget (OMB), and leaders of relevant federal agencies. Moreover, the Panel recommends that the strategy should include four key elements:

1. Encouraging more people to choose a career in the cybersecurity field through outreach and education
2. Enabling education and training to build needed competencies and alternative pathways to cybersecurity careers
3. Overcoming barriers to recruiting talent and matching people to jobs
4. Assessing performance and promoting innovation in workforce development practice

Under each of these elements, the Panel recommends focus areas and actions to achieve results. These recommended focus areas emphasize outreach to underrepresented communities and the establishment of multiple pathways for individuals to pursue cybersecurity careers.

Second, the Panel's report focuses on the ONCD's ability to develop and carry out a national strategy that will depend on close collaboration with leaders in relevant federal agencies and partnership with industry, academia, and state, local, tribal, and territorial (SLTT) governments.

6. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No 116-283, tit. XVII, 134 Stat. 4144 (2021), Section 1752.

However, collaboration and persuasion alone will not ensure the cross-agency coordination needed to achieve strategic priorities and outcomes. The National Cyber Director will need to establish a high-level governance structure, emanating from his office, that aligns participating federal agencies and provides the authorities commensurate to the task of developing and carrying out the detailed workforce development strategy described above. These authorities should include budget and performance assessment authorities to determine how well programs perform and how best to scale or adjust investments, which may well depend upon the collection of granular data.

Finally, the report presents the results of the Panel's review of CISA's cybersecurity workforce development programs. CISA's cybersecurity workforce development responsibilities as defined in law include "increasing the pipeline of future cybersecurity professionals" across the nation as well as "building awareness and competency in cybersecurity across the civilian Federal Government workforce."[7] Within CISA, the Cybersecurity Defense Education and Training (CDET) branch currently has primary responsibility for implementing this charge.

As Congress requested, the Panel reviewed CISA's programs and strategy in terms of three objectives set out by Congress—excellence, diversity, and scalability.[8] The Panel finds CISA has generally performed well in meeting these objectives in planning, designing, and executing its programs, given constraints of authorities, resources, and the short period of time many of these programs have been in place. Success will depend on two factors. First, it will depend on clarifying and supporting CISA's role and responsibilities in national workforce development, which should follow from the government-wide strategy for developing the national workforce. Second, the Panel concludes that fully realizing the potential of CISA's workforce development programs will depend on Congress providing the authorities to enable CISA to partner effectively with educational and training institutions and the staff needed to manage programs at scale.

7. Cybersecurity and Infrastructure Security Agency, 6 U.S.C. § 652.
8. Consolidated Appropriations Act of 2021, HR 133, 116th Cong., 2nd sess., *Congressional Record* 166, no. 218—Book IV, daily ed. (December 21, 2020): H 8477.

List of Findings and Recommendations

Chapter 3: Government-Wide Strategy for Developing the National Cybersecurity Workforce

Finding 3.1: The federal government lacks a comprehensive, integrated government-wide strategy for developing the national cybersecurity workforce.

Recommendation 3.1: The National Cyber Director, in consultation with the Cybersecurity and Infrastructure Security Agency (CISA) Director and other relevant leaders, should lead the creation of a government-wide strategy to develop the national cybersecurity workforce. The strategy should reflect the following guiding principles and priorities:

- Addressing both federal government and national workforce development needs
- Partnering with industry, academia, and nonprofits to achieve goals and priorities
- Reaching out to and engaging underrepresented populations and communities
- Considering the needs of state, local, tribal, and territorial (SLTT) governments and leveraging and supporting their workforce development initiatives
- Identifying areas where the federal government can serve as the model for implementing innovative and cost-effective approaches

This government-wide strategy for developing the national workforce should include the following four elements:

Element 1 Encouraging more people to choose a career in the cybersecurity field through outreach and education

Element 2 Enabling education and training to build needed competencies and alternative pathways to cybersecurity careers

Element 3 Overcoming barriers to recruiting talent and matching people to jobs

Element 4 Assessing performance and promoting innovation in workforce development practice

Chapter 4: Governance Framework for Cybersecurity Workforce Development

Finding 4.1: Although active collaboration between leaders of the Office of the National Cyber Director (ONCD) and CISA has led to great strides in coordinating initiatives and resources for meeting the nation's larger cybersecurity challenges, federal agencies are not clear about their developmental, implementation, and operational responsibilities for workforce development and how these fit together to accomplish the larger workforce development objectives of the nation.

Recommendation 4.1: The ONCD should develop and implement an appropriate operating model and governance structure to integrate actions by the CISA, the National Security Agency (NSA), the National Institute of Standards and Technology (NIST), the Department of Defense

(DoD), and other relevant federal agencies and organizations involved in building the cybersecurity workforce for the nation. This includes coordinating with and specifying roles and responsibilities between and among agencies.

Recommendation 4.2: Congress should ensure the ONCD has budget and performance assessment authority to lead and coordinate the programs that will develop the needed workforce, including authorities to drive agency implementation of these programs.

Recommendation 4.3: The ONCD should establish and run a leadership working group or council for cybersecurity workforce development with responsibility for both government-wide and external cybersecurity workforce development programs. The ONCD should also charge a designated senior official as the leader of this working group. The ONCD should specify the authorities and responsibilities of the group and its leader and identify the major federal member organizations. Private sector, SLTT governments, and academic representatives could also be included as working group members, as appropriate, based on objectives.

Recommendation 4.4: The ONCD should 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. One way of accomplishing this would be to establish a Bureau of Cybersecurity Statistics or a similar organization.

Chapter 5: A Review of CISA Programs and Strategies

Finding 5.1: The planning and design of most of CISA's cybersecurity workforce development programs—as implemented by the Cybersecurity Defense Education and Training (CDET) branch—meet diversity, excellence, and scalability objectives identified by Congress.

Finding 5.2: CISA's workforce development programs succeed because of CDET's ability to identify and partner with organizations with a proven track record in cybersecurity and workforce development.

Finding 5.3: Although CISA is not considered an education agency, CISA has the authority and responsibility under law to create programs focused on elementary and secondary education. There are several benefits of the Cybersecurity Education and Training Assistance Program's (CETAP) placement in CISA, as currently administered by CDET.

Recommendation 5.1: As a key approach to workforce pipeline building, the Office of Management and Budget (OMB), Department of Homeland Security (DHS), and CISA should sustain funding for CETAP in the President's budget request to better integrate and update the grant in accordance with future planned K-12 workforce activities.

Recommendation 5.2: Congress should provide CISA with additional grant-making authority to effectively partner with colleges, universities, and community colleges. The additional authority should allow CISA to issue grants that can last up to five years in duration. CDET is the entity responsible for these initiatives within CISA.

Recommendation 5.3: Congress should periodically review and adjust CISA's staffing, resources, and authorities as CISA's cybersecurity workforce development program changes.

Chapter 1: Introduction

Why Do Cybersecurity and the Cyber Workforce Matter to the Nation?

Cybersecurity is among the most important and urgent challenges facing our nation. Recent cyberattacks—such as SolarWinds, which affected the US government and organizations around the world in 2020;[9] the Colonial Pipeline ransomware attack in May 2021;[10] the breach of the Microsoft Exchange Server software by China's main intelligence service, the Ministry of State Security in March 2021; [11] and the log4j software bug discovered in December 2021[12]—underscore the vulnerability of the nation's critical infrastructure and computer systems. Cybersecurity safeguards government systems, networks, and data along with private sector critical infrastructure, such as electric grids, health care networks, and supply chains. Cybersecurity touches every aspect of the government, economy, and lives of the entirety of the American public.

Against this backdrop, the United States faces a critical cybersecurity workforce shortage. Estimates have hovered around five hundred thousand unfilled positions in recent years.[13] Hundreds of thousands of additional workers with the necessary knowledge and skills are required to effectively prevent attacks and respond when they occur. Further, this workforce must be prepared to meet the nation's needs as they change over time.

The Status Quo Does Not Address the Cyber Need

Developing a national cybersecurity workforce is a complex and daunting task. Beyond the sheer number of workers needed to fill empty positions, experts debate what makes a good cybersecurity worker. Do workers need a background in soft skills, like teamwork and problem solving, combined with foundational knowledge and STEM education? Or do high school graduates with hands-on cyber training bring the needed skills and experience? The answer, in part, depends on what job roles government and industry need to fill. But there is also continuing debate about that; industry has not often communicated its needs in a manner consistent enough to frame national action.

---

9. Sanger, Perlroth, Schmitt, "Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit," *The New York Times*, December 14, 2020, Updated September 9, 2021, https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.
10. Dustin Volz, "Colonial Pipeline Chief Says Recovery From Ransomware Hack Not Complete." *The Wall Street Journal*, June 8, 2021, https://www.wsj.com/articles/colonial-pipeline-chief-to-testify-in-senate-panel-on-ransomware-hack-11623144602.
11. Eric Tucker, "Microsoft Exchange hack caused by China, US and allies say." *AP News*, July 19, 2021, https://apnews.com/article/microsoft-exchange-hack-biden-china-d533f5361cbc3374fdea58d3fb059f35.
12. CISA Director Easterly called log4j "the most serious vulnerability I have seen in my decades-long career." Tatum Hunter and Gerrit De Vynck, "The 'most serious' security breach ever is unfolding right now. Here's what you need to know.," *The Washington Post*, December 20, 2021, https://www.washingtonpost.com/technology/2021/12/20/log4j-hack-vulnerability-java/.
13. CyberSeek, a National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) program carried out in partnership with Burning Glass and CompTIA, is a commonly cited source of workforce gap data. https://www.cyberseek.org/index.html.

Given the number of vacant cybersecurity positions, no single strategy or source of workers will ever solve the problem—this calls for multiple approaches that draw from a variety of talent sources. Most cybersecurity workers are white males,[14] meaning large segments of the talent pool—including females, people of color, and people with disabilities—are left untapped. While most agree on the need to expand and diversify the cybersecurity talent pipeline, experts disagree on the best way to do that. Is it targeting kindergarten through twelfth grade (K-12) students with outreach and education, or does upskilling and reskilling adults already in the workforce produce better outcomes?

To further complicate matters, technology, the cyber threat, and the nature and sophistication of those who carry out the threat are in a constant state of flux. This dynamic environment requires government officials and industry to focus on the needs of today and anticipate the needs of five, ten, and fifteen years from now. As attackers innovate and the nature of attacks changes, the workforce's ability to use cybersecurity tools and tactics adapt. New and updated software and systems are released at a rapid pace, requiring new skills to protect them. Work roles themselves will change over time. A significant portion of workers needed today is entry-level. Still, much of what they do is already or will be automated, necessitating more cybersecurity experts to monitor those processes and develop responses to new and evolving vulnerabilities and threats. The education and training that produced today's cybersecurity workforce will not be sufficient to meet tomorrow's needs.

Study Mandate and Focus

As part of the FY 2021 Consolidated Appropriations Act, Congress directed the Department of Homeland Security (DHS) to contract with the National Academy of Public Administration (the Academy) or a similar organization to review the Cybersecurity and Infrastructure Security Agency's (CISA) programs to build a national cybersecurity workforce. Congress specified that this review should determine "whether the partnership models under development by CISA are positioned to be effective and scalable to address current and anticipated needs for a highly capable cybersecurity workforce; whether other existing partnership models, including those used by other agencies and private industry, could usefully augment CISA's strategy; and the extent to which CISA's strategy has made progress on workforce development objectives, including excellence, scale, and diversity."[15]

Recognizing that assessing the effectiveness of CISA's workforce development strategy and programs would require an understanding of the broader federal government approach—and CISA's role within it—the Academy developed the following research questions:

1. What is the current state of CISA and other federal cybersecurity workforce programs, and what are their responsibilities and challenges?

---

14. Jason Reed and Jonathan Acosta-Rubio, *Innovation Through Inclusion: The Multicultural Cybersecurity Workforce: An (ISC)² Global Information Security Workforce Study*, Frost & Sullivan, 2018. This 2018 white paper estimated that 24 percent of the cyber workforce identified as female, 9 percent as Black, and 4 percent as Hispanic.
15. Consolidated Appropriations Act of 2021, HR 133, 116th Cong., 2nd sess., *Congressional Record* 166, no. 218—Book IV, daily ed. (December 21, 2020): H 8477.

2. What can the federal government do to create a sufficient workforce with the necessary knowledge and skills to meet the nation's short- and longer-term cybersecurity needs?
3. Within the larger context, where and how could—or should—CISA lead or participate in meeting the nation's cybersecurity workforce needs? How well are current initiatives working, and how effective and scalable are the partnership models CISA is currently using to meet its objectives?
4. What governance arrangements will result in clear leadership priorities being articulated and then implemented through transparent coordination across the federal government, other governments, educators, and the private sector to meet the nation's cybersecurity workforce needs most effectively and efficiently?

Study Methodology

To answer its charge, the Academy convened an expert Panel of five Fellows with broad cybersecurity knowledge and backgrounds in federal, state, and local government; academia; nonprofit organizations; and industry. The Panel oversaw and provided guidance to a Study Team that followed a structured methodology to collect and analyze data. (See Appendix A for a list of Panel members and Study Team members, with brief bios.)

The Study Team conducted extensive research and analysis of CISA documents and information, including budget and staffing data, strategy documents, and program descriptions. CISA also self-assessed its workforce development programs against the three criteria established by Congress (scalability, diversity, and excellence[16]) using a table developed by the Study Team (see Appendix B). To understand the environment in which CISA operates, the Study Team reviewed documents and information on cybersecurity workforce development, existing data on workforce needs, other federal agency workforce development program documents, congressional hearings, pertinent legislation, published reports, media coverage, and public statements of subject matter experts and federal leaders.

In addition, the Study Team conducted interviews with approximately ninety key stakeholders and experts, including congressional staff; current and former CISA officials, managers, and contractors; officials of other federal agencies; and experts and practitioners in academia, industry, and state and local governments. (See Appendix C for a list of interviewees.)

The Study Team used these data to document and assess the current state of CISA's programs and capabilities, document the current state of other federal cybersecurity workforce programs, and identify workforce development challenges and opportunities facing the federal government and the nation.

16. Consolidated Appropriations Act of 2021.

Report Contents

Five additional chapters and seven appendices follow this introductory chapter. Chapters 3, 4, and 5 contain findings and recommendations.

- Chapter 2 provides background on the cybersecurity workforce and the evolution of the federal response to workforce needs.
- Chapter 3 outlines the elements of a government-wide strategy for developing the national cybersecurity workforce.
- Chapter 4 presents a governance framework for developing, leading, and coordinating a comprehensive, integrated workforce development strategy for the nation.
- Chapter 5 focuses on reviewing CISA's cybersecurity workforce development programs and partnerships.
- Chapter 6 concludes the report with a summary of key takeaways.

The appendices provide information about the Academy Panel and Study Team, a list of individuals interviewed for this study, and additional information on CISA and other federal cybersecurity programs to augment the report chapters.

Chapter 2: Background and Landscape

Background

This report focuses on the development of a professional cybersecurity workforce, an important—but not the only—part of an effective national response to the challenge of cybersecurity. The federal government is also responsible for protecting its data and systems, securing critical infrastructure, and managing risks. Technology developments, such as systems and software more resistant to cyberattacks to begin with and artificial intelligence, are also part of the solution. Finally, while this report focuses on education and training related to the cybersecurity workforce, outreach to and training of the public and the general workforce to create "good cyber citizens" is also a critical component of cybersecurity.

Nevertheless, developing the cybersecurity workforce is attracting a significant amount of attention and resources, and for a good reason. Estimates of the significant and increasing national cybersecurity workforce "gap" range in the hundreds of thousands. CyberSeek estimates the current US workforce gap at over 450,000 and breaks the gap down into several job categories (Figure 1).[17] An example from the federal government of the growing workforce need is a Bureau of Labor Statistics projection that the Information Security Analyst job—which encompasses many, but not all, cybersecurity jobs for the federal government—will grow by 33 percent between 2020 and 2030.[18] Figure 1 also illustrates that the need goes beyond highly technical positions. The nation's cybersecurity workforce needs reflect a diversity of work roles,[19] including technical, managerial, policy, and other supporting staff roles, many carried out by professionals who might not have "cybersecurity" in their job titles (e.g., software engineers). These roles demand competencies that depend on different mixes of knowledge and skills. Technical roles have an important knowledge component, such as understanding the principles of computer networks, architecture, and programming. Many essential work roles require both technical skills and "soft" skills, such as oral and written communication.

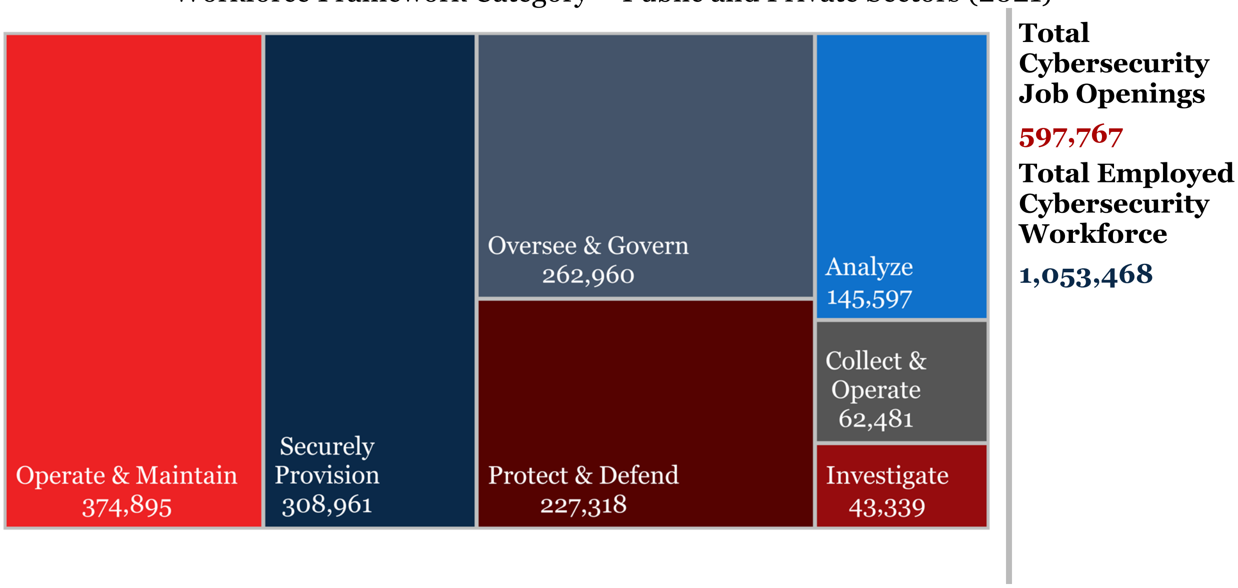
The worldwide cybersecurity workforce gap is estimated at 2.7 million,[20] making it even more difficult for government and private sector entities in the United States to compete for cyber talent. The staggering size of the current workforce gap, combined with the continual growth and evolution of cybersecurity positions, underscores the need for urgent action.

---

17. "Cybersecurity Supply/Demand Heat Map," National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE), https://www.cyberseek.org/heatmap.html. This analysis is of open positions. The gap is likely larger because there is a need for cyber workers that is greater than current employer demand.
18. "Information Security Analysts: Job Outlook," US Bureau of Labor Statistics, accessed December 21, 2021, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6.
19. NIST, *Workforce Framework for Cybersecurity (NICE Framework) – SP 800-181 Rev. 1*, November 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.
20. (ISC)², *Cybersecurity Professionals Stand Up to a Pandemic: (ISC)² Cybersecurity Workforce Study*, 2020, p. 19-22, https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.as.

However, data on the size and composition of the workforce shortage are inadequate. Several estimates of the national need for cybersecurity professionals exist but quantifying the number of open and filled jobs in the cybersecurity workforce has proven exceptionally challenging. For example, different cybersecurity jobs have overlapping skills, meaning a single cybersecurity job classification would likely underestimate the full scope of the need. In addition, the workforce gap constantly evolves in real time due to the changing needs of businesses and governments, new threats, advances in technology, and unique circumstances, like COVID-19. Further, it is difficult to compare available data because organizations that collect and analyze workforce data rely on different methodologies and sources, some more reliable than others.[21]

Figure 1. Job Openings by National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework Category – Public and Private Sectors (2021)



Source: CyberSeek (2021), sponsored by NICE within the National Institute of Standards and Technology (NIST).[22]

Currently, no federal statistical agency rigorously tracks and quantifies the cybersecurity workforce, as done for other workforce sectors (e.g., manufacturing and farm labor). The formal US Bureau of Labor Statistics characterization of the cybersecurity workforce helps but does not encompass the broad range of different specialties and disciplines required to enable adequate staffing of enterprises for a complete and effective cybersecurity response. The Cyberspace Solarium Commission recommended the creation of a Bureau of Cyber Statistics in the Department of Homeland Security (DHS), and legislation creating the Bureau has been

21. For example, (ISC)², a common source of cyber workforce gap data, reports that, despite using measures to increase the credibility of its estimates, a potential limitation is that the estimation relies on survey respondents. (ISC)², *Cybersecurity Professionals Stand Up to a Pandemic: (ISC)² Cybersecurity Workforce Study*, 19-22.
22. CyberSeek notes that there can be overlap among the NICE categories as they are not mutually exclusive. A job within one category may also perform functions of another category. Therefore, the number of job openings by *NICE Framework* category depicted in Figure 1 add up to more than the total number of job openings. The data contained in this figure represent the number of online job listings for cybersecurity-related positions between October 2020 and September 2021.

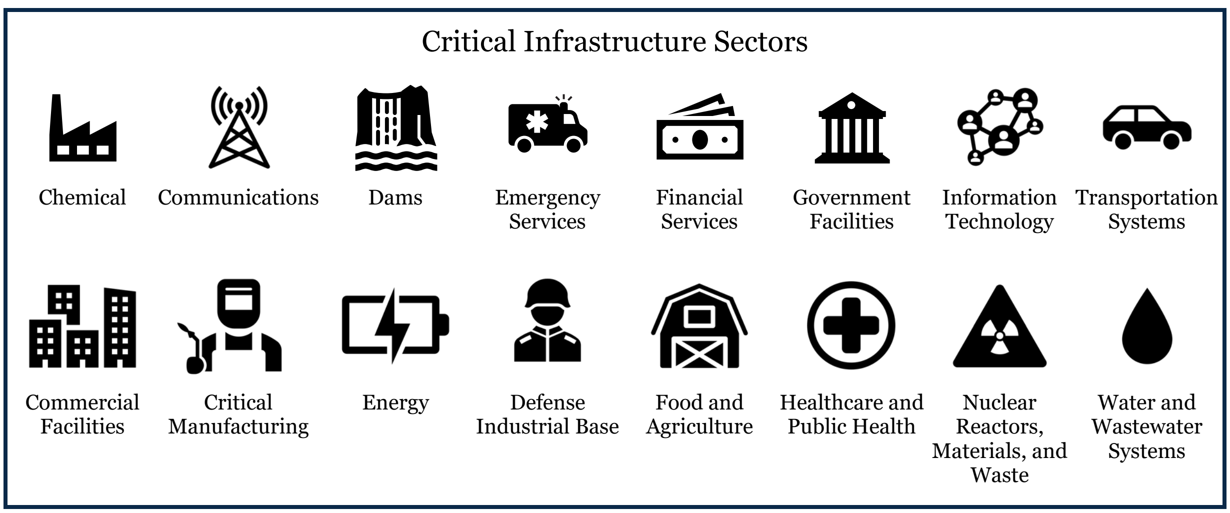
introduced in Congress.[23] While the recommended purpose of the Bureau of Cyber Statistics is to collect information on cyberattacks, if tasked with collecting and analyzing workforce data, it could provide more reliable information for policy makers to use for planning and evaluating programs.

History and Evolution of the Federal Response

The federal government has planned for, mitigated, and responded to cybersecurity intrusions for several decades, with activity ramping up in response to the Computer Security Act of 1987.[24] One focus of these efforts has been developing a pipeline of cybersecurity talent available and sufficiently trained to meet the cybersecurity needs of the federal government and the country.

From the beginning, federal efforts focused on developing both the federal and national cybersecurity workforce. Given the need in both the public and private sectors, and the difficulty the government has in competing with industry to attract talent, the federal government could not address its own needs by vying for scarce talent—it had to focus on expanding the pipeline of available talent. In addition, the federal civilian agencies contract out for a majority of their cyber services, making them heavily reliant on the quality of the private sector workforce. Experts argue that the vulnerability of critical infrastructure, the vast majority of which is owned by the private sector, constitutes the most significant risk to the nation's security (see Figure 2 for a listing of the sixteen critical infrastructure sectors). This risk necessitates an increased focus on cyber skills in industries that often place greater emphasis on physical infrastructure.

Figure 2. Critical Infrastructure Sectors[25]



23. *Cyberspace Solarium Commission Final Report*. March 2020, https://www.solarium.gov/report.
US Congress, Senate, *Defense of the United States Infrastructure Act of* 2021, S. 2491, 117th Cong., 1st sess., introduced in Senate July 27, 2021.
24. *Computer Security Act of 1987*, Pub. L. No. 100-235, 101 Stat. 1724 (1988).
25. "Critical Infrastructure Sectors," CISA, last updated October 21, 2020, https://www.cisa.gov/critical-infrastructure-sectors.

The interdependence between the federal government and the private sector on the cybersecurity workforce does not end there. Federal government initiatives to develop its own workforce have helped develop the national workforce. Workers trained by the federal government have skills and security clearances sought by the private sector. While the attraction of higher pay can encourage employees to leave the federal government, overall skill enhancement across the government cyber workforce contributes to enhancing the skills of the whole workforce. There are other opportunities for federal workforce development to advance national workforce development needs. For example, materials and resources produced by the federal government, such as competitions and cyber ranges,[26] can be made publicly available. And federal training programs can demonstrate what works to the private sector.

The federal government is only one part of the overall solution. Developing cybersecurity talent depends on the commitment of not only industry but also educators; state, local, tribal, and territorial (SLTT) governments; and nonprofit organizations.[27] This range of public and private sector actors are already involved in different aspects of cybersecurity workforce development—curriculum development, training, certification, apprenticeships, and research—and need to be engaged in developing and implementing solutions. Cybersecurity requires a whole-of-nation effort, and the federal government's success will depend on its ability to partner effectively with a myriad of nongovernmental actors.

Summary of Players and Programs

Congress asked the Academy to review the Cybersecurity and Infrastructure Security Agency's (CISA) workforce development programs.[28] However, as described in Chapter 1, CISA's strategy, programs, and role must be understood in the context of a broader set of federal agency programs to promote the development of the national cybersecurity workforce.

Timeline of Major Federal Events in Cybersecurity (See Appendix D)

1999
- NSA Launched CAE Program

2000
- NSF SFS Program Created

2001
- DoD Cybersecurity Scholarship Program Created

2010
- NIST Establishes NICE

2012
- NICE Framework Published
- CETAP Grant Created (K-12 Cyber Education)

2017
- Executive Order 13800: Strengthening Cybersecurity
- Executive Order 13801: Cyber Apprenticeships

2018
- President's National Cyber Strategy released
- CISA created (predecessor NPPD)

2019
- Executive Order 13870: Cybersecurity Workforce
- NSA CAE Program adds 2-Year Colleges

2020
- Cyberspace Solarium Commission Report Released
- Department of Education CyberNet created

2021
- White House National Cyber Director Appointed
- Executive Order 14028: Improving the Nation's Cybersecurity
- White House Summit on whole-of-nation effort to improve cybersecurity

26. NIST defines cyber ranges as follows: "interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment." "Cyber Ranges," NIST, https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf.
27. President's National Security Telecommunications Advisory Committee (NSTAC), *Report to the President on a Cybersecurity Moonshot*, November 14, 2018, https://www.cisa.gov/sites/default/files/publications/NSTAC_CyberMoonshotReport_508c.pdf.
28. Consolidated Appropriations Act of 2021.

The DHS has been involved in workforce development—to varying degrees—since its inception in 2002. CISA, formed in 2018 as a result of the Cybersecurity and Infrastructure Security Agency Act,[29] has responsibility within the DHS for cybersecurity workforce development. In 2019, CISA consolidated external cybersecurity education and training programs under the newly formed Cybersecurity Defense Education and Training (CDET) branch.

Several other federal agencies, including the Department of Defense (DoD), National Security Agency (NSA), Department of Education, National Institute of Standards and Technology's (NIST) NICE program, National Science Foundation (NSF), and Office of Personnel Management (OPM), have a role in cybersecurity workforce development. These agencies execute both long-standing and relatively new programs and initiatives with a range of purposes aimed at different audiences. The programs encompass outreach, education, and training at the K-12 level; education and training at the post-secondary level; and cross-cutting activities, such as setting standards.

In the K-12 area, a major long-standing effort includes the Cybersecurity Education and Training Assistance Program (CETAP), a DHS program since 2012 and currently run by CDET. CETAP, through its cooperative agreement with a nonprofit organization (CYBER.ORG), undertakes a variety of K-12 initiatives, primarily to support educators by providing resources, such as curricula, training, and professional development. More recently, CETAP developed education standards for state adoption. Other CETAP activities, such as pilot projects for blind and visually impaired people and matching historically black colleges and universities (HBCU) with feeder high schools, aim to diversify the cybersecurity talent pipeline. (See Chapter 5 for more information on the CETAP program.) The NSA and NSF have funded GenCyber camps for K-12 students and educators since 2014.

At the post-secondary level, major efforts include the NSA's National Centers of Academic Excellence (CAE) program, which the NSA established in 1999 as a partnership with the DHS,[30] and the National Science Foundation's CyberCorps: Scholarship for Service (SFS) Program. The CAE program promotes common standards in cybersecurity education; both universities and community colleges participate. The SFS program has awarded grants to CAE universities to provide scholarships for students in cybersecurity education programs since 2000.[31] Similar to the SFS, the DoD's Cyber Scholarship Program provides scholarships to civilians, military officers, and enlisted personnel pursuing degrees in cybersecurity; unlike the SFS, the DoD has input into the process for selecting scholarship recipients.

NIST presides over a collaborative public-private standard-setting effort as part of its NICE Program. The *Workforce Framework for Cybersecurity (NICE Framework)*,[32] first issued in 2012 and most recently updated in 2020, identifies the skills, standards, and capabilities suitable for different cybersecurity jobs. These standards also provide a common nomenclature to which

---

29. Cybersecurity and Infrastructure Security Agency, 6 U.S.C. § 652.
30. The CAE has been administered almost entirely by the NSA, as DHS has focused its limited funding and resources on other priorities.
31. CISA, "CyberCorps: Scholarship for Service," National Initiative for Cybersecurity Careers and Studies (NICCS), accessed December 21, 2021, https://niccs.cisa.gov/formal-education/cybercorps-scholarship-service-sfs.
32. *NICE Framework.*

the federal government and private sector can adhere. Federal agencies and their contractors must use the *NICE Framework* to categorize positions. NICE also convenes an Interagency Coordinating Council, a Community Coordinating Council, and public-private communities of interest on topics such as K-12 education and apprenticeships.

In recent years, these and other federal agencies have launched additional programs. Examples of newer entrants include the Department of Education's CyberNet program, which provides support for the professional development of K-12 cybersecurity educators, and the Department of Labor's Registered Apprenticeship Program, which has recently prioritized the development of apprenticeship programs in cybersecurity.[33] These newer programs reflect the federal government's current approach, which emphasizes bringing more people into the cyber workforce pipeline through K-12 education and outreach, reskilling the existing workforce, and hands-on and experiential learning. (A more exhaustive list of federal government programs and additional details are provided in three Appendices. Appendix D provides a timeline of major federal cybersecurity developments and initiatives. Appendix E identifies and describes federal programs and activities and groups them as they relate to the challenges of meeting the nation's cybersecurity workforce needs. Appendix F provides more detailed summaries of programs, initiatives, and activities).

As discussed earlier, several nonfederal actors have essential roles in cybersecurity workforce development, including industry, nonprofit organizations, and SLTT governments. Industry is a significant player and falls into the five categories listed below in terms of its needs and roles:

- Training providers and certification entities
- Employers/customers of education and training program graduates
- Companies (typically large ones) that are delivery partners by providing training to their employees, for example, through apprenticeship programs
- Technology companies that might offer innovative tools and approaches to training and delivery
- Contractors that provide cybersecurity services to the federal government

In addition to industry, institutes of higher education, including two- and four-year colleges and universities, play an important role in providing education and training, with many providing both degrees and certifications. Some academic institutions also conduct research related to cybersecurity workforce development, develop and provide access to cyber curriculum, partner with governments and businesses to tailor curricula to meet current employer needs (including experiential, scenario-based education), and partner with local governments too small to hire cybersecurity talent.[34] Community colleges and other higher education organizations participate in apprenticeship programs with industry partners.

Nonprofit organizations, including professional associations, also play a critical role by conducting research; providing education, training, and certifications; and developing and

---

33. The White House, *Executive Order 13801: Expanding Apprenticeships in America*, 82 FR 28229 (June 20, 2017), https://www.federalregister.gov/documents/2017/06/20/2017-13012/expanding-apprenticeships-in-america.
34. See, for example, "MIT Cybersecurity Clinic," MIT Department of Urban Studies and Planning, accessed December 21, 2017, https://urbancyberdefense.mit.edu/CybersecurityClinic.

implementing K-12 programs. Nonprofit organizations with ties to underrepresented communities are particularly well suited to reaching diverse populations, including adult learners. Some nonprofits, like Girls Who Code, target specific demographics, and others provide services (e.g., career services to adult learners) in specific underserved communities.

Due to limited resources, many SLTT governments play a limited role in developing the national cybersecurity workforce. However, some states fund important post-secondary and K-12 programs.

Opportunities and Challenges

Several recent developments provide opportunities to make significant progress on workforce development. In 2021, the Senate confirmed the nation's first White House National Cyber Director (NCD);[35] this position can provide leadership, strategy, and coordination on cybersecurity workforce development across federal agencies. The new CISA Director works closely with the NCD, addressing similar visions and priorities. In addition, previous federal efforts and studies can be built upon, such as the Obama Administration's Comprehensive National Cybersecurity Initiative,[36] the *NSTAC Report to the President on a Cybersecurity Moonshot*, and the *Cyberspace Solarium Commission Final Report*. These efforts addressed cybersecurity broadly but included workforce development components that can assist the federal government in identifying priorities and developing solutions.

Congress also provides leadership on cybersecurity workforce development. With the increased frequency and intensity of cyberattacks, Congress has proposed legislation that would institute new approaches, like a cyber rotation program and a "cyber reserve,"[37] funding new programs, increasing the funding and scope of existing programs, and expanding agency responsibilities.

Recent commitments from the private sector to strengthen and expand workforce development are promising. Recognizing that the federal government is only part of the solution, in August 2021, President Biden convened a White House summit with private sector and education leaders "to discuss the whole-of-nation effort needed to address cybersecurity threats."[38] As a result of the summit, for example, Google committed to train one hundred thousand individuals in technical fields such as IT support and data analytics. Nonprofit organizations and academic

35. US Congress, Senate, *Chris Inglis – Executive Office of the President,* PN455, 117th Cong., confirmed on June 17, 2021, https://www.congress.gov/nomination/117th-congress/455.
36. The Obama Administration, *The Comprehensive National Cybersecurity Initiative*, accessed December 21, 2021, https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf.
37. US Congress, House, *Federal Rotational Cyber Workforce Program Act of 2021*, HR 3599, 117th Cong., 1st sess., introduced in House on May 5, 2021.
US Congress, Senate, *Civilian Cyber Security Reserve Act,* S 1324, 117th Cong., 1st sess., introduced in Senate on April 22, 2021.
38. White House, "FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity," August 25, 2021.
The meeting resulted in a series of commitments from educators and private sector companies to expand the pipeline of available talent. Participants who made commitments include Google, IBM, Microsoft, Code.org, Girls Who Code, the University of Texas System, and Whatcom Community College.

institutions that participated in the summit also made commitments to train underserved populations, develop new credentials, reskill and upskill workers, train educators, and more.[39]

Although these developments are promising, more must be done to realize the full potential of the commitments made and resources dedicated to developing the nation's cybersecurity workforce. Most importantly, the federal government needs a coherent, integrated strategy for developing the national workforce and an associated governance framework. New programs are created and existing programs are expanded without a clear sense of what the priorities are, what refinements are needed based on lessons learned, where there are instances of duplication or gaps between agency programs, and where the federal government can add the most value relative to the private sector. Furthermore, without a governance structure or workforce development strategy, the strong leadership and interagency coordination in place now depends on the goodwill among leaders and might not be sustained into the future.

39. White House, "FACT SHEET."

Chapter 3: Government-Wide Strategy for Developing the National Cybersecurity Workforce

The Cyberspace Solarium Commission,[40] the US Government Accountability Office,[41] and others have previously noted that there is no government-wide strategy for developing the national cybersecurity workforce. This chapter explains the need for a strategy and describes the elements that such a strategy should include. This strategy is strongly linked to the governance framework discussed in Chapter 4; neither can succeed without the other.

Finding 3.1: *The federal government lacks a comprehensive, integrated government-wide strategy for developing the national cybersecurity workforce.*

The White House, various federal agencies, and Congress are working to build a national cybersecurity workforce. Congress is passing new legislation and dedicating additional resources to cybersecurity readiness. Federal agencies are implementing new programs and approaches. However, no comprehensive, integrated government-wide strategy sets priorities and focuses attention and resources.[42] As a result, congressional and agency officials act independently to address various challenges related to meeting the cybersecurity workforce development needs of the federal government and the nation more broadly. Without an overarching strategy, these independent initiatives have the potential to be duplicative. In addition, it is unclear whether these initiatives are addressing the federal government's highest priorities and in the most effective and efficient ways.

The absence of a federal government-wide strategy for developing the national workforce reflects the fact that, until recently, there has been no formal federal government-wide leadership. That has changed with the recent appointment and confirmation of the National Cyber Director (NCD) and the Director of Cybersecurity and Infrastructure Security Agency (CISA). The newly confirmed NCD has taken a first step toward developing a strategy by issuing *A Strategic Intent Statement for the Office of the National Cyber Director*.[43]

These new leaders will face daunting challenges in developing and implementing a strategy. Beyond inadequate data on cybersecurity workforce development needs, there is a lack of agreement on the most effective ways to meet those needs. Nevertheless, federal leaders must move forward in developing a strategy. The government cannot achieve its workforce development goals if it has not articulated them.

---

40. *Cyberspace Solarium Commission: Executive Summary*; March 2020, p. 3, 9 (Key Recommendation 1.5: Diversify and Strengthen the Federal Cyberspace Workforce)
41. US Government Accountability Office, GAO-20-629, C*ybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, https://www.gao.gov/products/gao-20-629.
42. The Cybersecurity Enhancement Act of 2014 requires NICE to develop a workforce development strategic plan every five years. While the NICE strategic plan is a good start—and is developed with input from the private sector and other federal agencies—this plan is not the same as a government-wide plan that articulates the administration's priorities. Further, it appears that other federal agencies view it as NICE's, rather than a government-wide, plan.
43. Office of the National Cyber Director, *A Strategic Intent Statement for the Office of the National Cyber Director*, 2021, https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf.

Recommendation 3.1: The National Cyber Director, in consultation with the CISA director and other relevant leaders, should lead the creation of a government-wide strategy to develop the national cybersecurity workforce. The strategy should reflect the following guiding principles and priorities:

- ***Addressing both federal government and national workforce development needs***
- ***Partnering with industry, academia, and nonprofits to achieve goals and priorities***
- ***Reaching out to and engaging underrepresented populations and communities***
- ***Considering the needs of state, local, tribal, and territorial (SLTT) governments and leveraging and supporting their workforce development initiatives***
- ***Identifying areas where the federal government can serve as the model for implementing innovative and cost-effective approaches***

The government-wide strategy for developing the national workforce should include the following four elements: [44]

1. Encouraging more people to choose a career in the cybersecurity field through outreach and education
2. Enabling education and training to build needed competencies and alternative pathways to cybersecurity careers
3. Overcoming barriers to recruiting talent and matching people to jobs
4. Assessing performance and promoting innovation in workforce development practice

In-depth research into the opportunities and challenges of the strategy elements was outside the scope of this study. However, data collected through interviews and document reviews suggest areas of focus that could be fruitful for the federal government to pursue within each element. Figure 3 presents recommended focus areas for each strategy element. These recommended areas of focus are not intended to be comprehensive; they are intended to supplement the recommendations made by the Cyberspace Solarium Commission and others.

---

44. These elements largely align with the challenges to building a national workforce identified in Appendix E. Element 3 encompasses two challenges from Appendix E: "barriers to matching people/competencies with jobs" and "barriers to the federal government recruiting and retaining talent *vis-à-vis* the private sector." The fourth strategy element was inspired by the NICE workforce development strategy and Panel discussions about the lack of agreement on or evidence of what approaches work/work best. These elements do not reflect the challenge facing small government and private organizations that lack the resources to hire or even contract for cybersecurity services because it is not a workforce development challenge per se.

Figure 3. Four Elements of a National Workforce Development Strategy

Element 1

Encouraging more people to choose a career in the cybersecurity field through outreach and education

Recommended Focus Areas

- Conducting outreach to underrepresented populations and communities
- Enabling K-12 educators to take advantage of cybersecurity curricula
- Ensuring schools, particularly in underserved communities, have the necessary technology infrastructure in place to support teacher development and student participation in cybersecurity education and training, including competitions
- Exploring options for targeting the existing noncybersecurity workforce and adult learners for recruitment into the cybersecurity field and helping them acquire the necessary credentials

Element 2

Enabling education and training to build needed competencies and alternative pathways to pursuing cybersecurity careers

Recommended Focus Areas

- Promoting the development of educational and training programs at institutions willing and able to provide high-quality, experience-based curricula and activities
- Helping to ensure relevant scenario-based exercises and low-cost, adaptable platforms for experiential learning are accessible to educational and training institutions
- Supporting the adoption of apprenticeship programs by the public and private sectors

Element 3

Overcoming barriers to recruiting talent and matching people to jobs

Recommended Focus Areas

- Expanding the Cybersecurity Talent Management System (CTMS) to provide flexibilities that will help the federal government compete with the private sector and attract and retain top talent
- Making the most of hiring flexibilities within the federal personnel systemin in the near term
- Making it easier for federal agencies to tap top private sector talent to meet immediate cybersecurity needs
- Increasing employer confidence in certifications and encouraging a more flexible approach to cybersecurity position qualifications

Element 4

Assessing performance and promoting innovation in workforce development practice

Recommended Focus Areas

- Evaluating the performance of federal programs and private sector approaches to workforce development
- Cultivating innovative approaches to workforce development

It is important to emphasize that the recommended focus areas identified under each of the four proposed elements of a national workforce development strategy encompass actions with the potential for impact over different timeframes. For instance, the potential impact of outreach and education efforts targeting kindergarten through twelfth grade (K-12) students is generally longer-term, depending on the age group targeted. By contrast, reskilling adults in noncybersecurity technical positions can potentially make an impact in the short term.

Figure 4 below presents a legend with icons indicating different timeframes (short-, medium-, and long-term) within which policy makers can generally expect actions under each recommended focus area to achieve impact. The assignment of timeframes to each recommended focus area does not presume to anticipate the particular political and administrative challenges that may occur.

Figure *4*. Legend of Time to Impact

The timer icons below indicate the expected time before the actions under each recommended focus area result in impact.

Short Term (less than two years)

Medium Term (between two to four years)

Long Term (greater than four years)

Element 1: Encouraging More People to Choose a Career in the Cybersecurity Field through Outreach and Education

Element 1 focuses on expanding and diversifying the cybersecurity talent pipeline by encouraging more people to pursue a cybersecurity career, particularly in underrepresented populations and communities. This goal is primarily accomplished through outreach to K-12 students and adults already in the workforce in noncybersecurity roles. The specific strategies and objectives for each audience are very different. Outreach to K-12 students represents a long-term strategy with outcomes realized several years later, while reskilling adults already in the workforce can fill positions more quickly.

Recommended Focus Area: Conducting outreach to underrepresented populations and communities

Actions to achieve progress in this area might include

- Developing messaging and leveraging existing mechanisms (e.g., school counselors) to reach diverse students in underserved communities with information on cybersecurity careers and available pathways; and
- Partnering with community-based programs with successful track records in providing education, training, career services, and other related services to diverse populations and underserved communities.

Addressing the sizeable current workforce gap will require a dramatic increase in the number of people choosing to pursue a career in cybersecurity. Closing this gap will entail efforts to help encourage and enable individuals from all parts of the population (e.g., people of color, people with disabilities, those who are neurodiverse, women, and members of rural and low-income communities) to enter the cybersecurity talent pipeline. The gap cannot be filled solely by recruiting more white males, who already constitute most of the current cybersecurity workforce.[45] Nor can the gap be filled by relying only on graduates of four-year institutions.[46] (See Element 2.) Bringing individuals from more diverse backgrounds into the field would not only expand the talent pipeline but would allow organizations to benefit from different talents and perspectives, ultimately improving the quality and effectiveness of the cybersecurity workforce overall.[47]

K-12 Outreach and Education

Several federal agencies pursue outreach and education strategies that target K-12 students based on social science research indicating that success depends on reaching students earlier rather than later.[48] However, it is unclear when the most effective time is to reach students, and agencies are targeting students of different age groups and in different ways, such as raising awareness about cybersecurity careers; attracting students to STEM and cybersecurity tracks through

45. Reed and Acosta-Rubio, *Innovation Through Inclusion: The Multicultural Cybersecurity Workforce: An (ISC)² Global Information Security Workforce Study*. This 2018 white paper estimated that 24 percent of the cyber workforce identified as female, 9 percent as Black, and 4 percent as Hispanic.
46. "Digest of Education Statistics," National Center for Education Statistics, accessed December 6, 2021, https://nces.ed.gov/programs/digest/d17/tables/dt17_322.30.asp?referer=raceindicators. In 2015-2016, the last school year for which data are available, there were sixty-four thousand graduates of four-year institutions who earned degrees in computer science, of which cybersecurity is a subset.
47. McKinsey & Company, *Diversity wins: How inclusion matters*, p. 13, May 2020.
David Rock and Heidi Grant, "Why Diverse Teams Are Smarter," *Harvard Business Review*, November 2016. Numerous studies have shown that diverse organizations outperform nondiverse ones, largely driven by their innovation and heterogeneity in ideas.
48. Journal of The Colloquium for Information Systems, Security Education, Volume 7, No. 1, Summer, 2020, https://cisse.info/journal/index.php/cisse/article/view/114.

competitions, camps, and gaming apps; developing curricula and standards; training teachers; and encouraging middle and high school students to earn certifications.

Outcomes of K-12 strategies can take many years to achieve, depending on the age and grade of targeted students. The long-term nature of K-12 strategies, combined with the difficulty of collecting information on K-12 students due to privacy concerns,[49] makes it difficult to determine how effective these programs are. (See Element 4 for a discussion of potential focus areas for program performance assessment.)

Recommended Focus Area: Enabling K-12 educators to take advantage of cybersecurity curricula

Actions to achieve progress in this area might include

- Increasing the number of K-12 educators with the necessary level of expertise to teach cybersecurity effectively through a mix of scalable strategies, including the use of train-the-trainers approaches to expand the reach of training and supplementing the expertise of local teachers with the virtual delivery of content by top cybersecurity teaching talent (similar to the Khan Academy[50]);
- Providing funding to states for teacher training and access to virtual teaching options; and
- Assisting states and school systems with adopting cybersecurity education standards.

The shortage of K-12 educators with expertise in cybersecurity presents a key challenge in providing K-12 education in cybersecurity. Developing curricula alone will not help reach K-12 students if educators do not have the knowledge and skills to teach the curriculum effectively. At least two scalable strategies can help address this shortfall. One is a "train-the-trainers" approach, training a relatively small group of teachers who can then train a much larger group of teachers. Another, modeled by the work of groups like the Khan Academy, involves identifying top teaching talent in a field and sponsoring the development of online courses by these teachers. These strategies, by themselves, will not be enough to increase access to K-12 education unless cybersecurity is included in state education standards, [51] as teachers face considerable pressure to teach to standards and tests.

49. The Family Educational Rights and Privacy Act (FERPA), 20 USC § 1232g, 34 CFR Part 99. https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
50. "About Khan Academy," Khan Academy, accessed January 12, 2021, https://www.khanacademy.org/about. Khan Academy is a nonprofit organization which provides free virtual education content.
51. CISA has developed model state standards that can be standalone or incorporated into other related (e.g., computer science) standards. See chapter 5 for more information on CISA's effort in K-12 education, including its Cybersecurity Education and Training Assistance Program.

Recommended Focus Area: Ensuring schools, particularly in underserved communities, have the necessary technology infrastructure in place to support teacher development and student participation in cybersecurity education and training, including competitions

Actions to achieve progress in this area might include providing devices and high-speed internet access to schools in low-income, rural, and other underserved communities.[52]

A recent survey of K-12 educators found that K-12 student access to cybersecurity education varies widely. Students are much less likely to learn about cybersecurity if they attend public versus private schools; live in communities with no cybersecurity companies; or live in small, rural, and/or high-poverty school districts.[53] These survey results indicate that the availability of K-12 cyber-related education depends on school and community resources.

Outreach to and Reskilling of the Existing Noncybersecurity Workforce

Some experts are starting to shift attention and resources to post-secondary students and adult learners to fill cybersecurity jobs and achieve greater diversity more quickly—and successfully—than is possible with K-12 outreach and education.

Recommended Focus Area: Exploring options for targeting the existing noncybersecurity workforce and adult learners for recruitment into the cybersecurity field and helping them acquire the necessary credentials

Actions to achieve progress in this area might include

- Leveraging existing nonprofit networks for adult learners, such as the Council for Adult and Experiential Learning, The Graduate! Network, and private sector noncredit providers, to raise awareness of cybersecurity career opportunities and provide additional support, such as mentoring, career services, and scholarships;[54] and
- Conducting outreach to community college students and providing resources to community colleges to enable them to provide cybersecurity career services.

Specific strategies include conducting outreach to and educating community college and university students and reskilling adults already in the workforce through programs such as apprenticeships and noncredit programs. Providing support to adult learners and leveraging

52. "Internet Access and Education: Key considerations for policy makers," Internet Society, November 20, 2017, https://www.internetsociety.org/resources/doc/2017/internet-access-and-education/.
US Department of Education, Office of Educational Technology, *Building Technology Infrastructure for Learning*, June 2017, https://tech.ed.gov/infrastructure/.
53. EdWeek Research Center, *The State of Cybersecurity Education in K-12 Schools: Results of a National Survey*, accessed June 14, 2021, p. 4, https://cyber.org/news/state-cybersecurity-education-k-12-schools.
54. Goldie Blumenstyk, "What Adult Students Need Now," The Chronicle of Higher Education, *The Edge newsletter*, November 17, 2021, https://www.chronicle.com/newsletter/the-edge/2021-11-17.

organizations and networks that work to reskill adults already in the workforce could help bring this approach to the scale needed to significantly impact the workforce gap.

Focusing on community colleges to expand the talent pipeline by reaching diverse populations and reskilling adults shows particular promise. A majority of community college students are women, people of color, lower-income individuals, and adults already in the workforce. Twenty percent of community college students have disabilities.[55] A focus on encouraging community college students to enter the cybersecurity field can expand and diversify the cyber workforce in the medium term.

Element 2: Enabling the Education and Training to Build Needed Competencies and Alternative Pathways to Cybersecurity Careers

Element 2 focuses on the education and training needed to build the cybersecurity workforce in the medium and short term, emphasizing experience-based learning and alternative pathways to pursuing careers in cybersecurity, such as two-year degree programs and apprenticeships.

There is little agreement on the particular competencies (mix of knowledge and skills) needed in the nation's cybersecurity workforce. This disagreement partly reflects the diversity of work roles, including technical, managerial, policy, and other supporting staff roles. These roles depend on different mixes of knowledge and skills. However, there is an emerging consensus on the following:

- Greater emphasis on experience-based training is needed to build the practical skills sought by employers.
- While four-year college and university programs play an essential role in providing generalizable knowledge and skills (e.g., analytic thinking, writing), they are often less suited to providing more specific knowledge and hands-on experience that is especially important to prepare students for more technical and operational work roles.
- The tendency of government and private sector employers to require four-year degrees for most cybersecurity positions has hindered the nation's ability to fully tap available talent by constraining access to disadvantaged groups and those with needed skills but less formal education.

Based on the Study Team's research, the Panel sees opportunities for the federal government to enable the development of experience-based training and alternative pathways to cybersecurity careers in three ways: (1) enabling alternatives to traditional four-year degree programs, (2) promoting experiential learning by means of relevant scenario-based exercises and low-cost, adaptable platforms and (3) promoting the adoption of apprenticeships.

55. "Fast Facts," American Association of Community Colleges, accessed December 2, 2021, https://www.aacc.nche.edu/research-trends/fast-facts/.

Enabling Alternatives to Traditional Four-Year Degree Programs

The major federal cybersecurity workforce development programs primarily focus on four-year degree programs. More recent efforts to enable alternatives and complements to four-year degree programs must be understood in this context.

The National Security Agency (NSA), National Science Foundation (NSF), and Department of Defense (DoD) pioneered federal efforts to promote cybersecurity education. The NSA's National Centers of Academic Excellence (CAE) program, which preceded the National Institute of Standards and Technology National Initiative for Cybersecurity Education (NIST/NICE), aims to align post-secondary educational curricula with a common set of standards to ensure a certain level of quality. The NSF CyberCorps: Scholarship for Service (SFS) program awards funding to colleges and universities with cybersecurity programs for scholarships to students on the condition that students receiving funds promise to serve a set term of service in the federal government. The DoD supports its own scholarship program, the Cyber Scholarship Program, providing scholarships to civilians, military officers, and enlisted personnel pursuing degrees in cybersecurity on the condition that students receiving a scholarship serve a fixed term in the military. The NSF and DoD programs are focused on supporting students through completing a four-year degree, a requirement for most cybersecurity positions in the federal government.

Recommended Focus Area: Promoting the development of educational and training programs at institutions willing and able to provide high-quality, experience-based curricula and activities

Actions to achieve progress in this area might include

- Supporting the NSA CAE program's ongoing efforts to cultivate and certify community colleges to provide more experience-based programs;
- Expanding support for the NSF's SFS program to include students seeking degrees from two-year programs as a pathway to initial employment (not just as a step toward completing a four-year degree) and adjusting program performance metrics accordingly;[56]
- Considering elements of the DoD Cyber Scholarship Program that might be applicable to the NSF SFS program, including agency input into the selection of candidates for scholarships; and
- Supporting competitive grants to institutions willing and able to provide experience-based programs, such as the Cyber Defense Education and Training (CDET) Non-Traditional Training Providers grant program.

Interviews indicate that four-year colleges and universities often are less responsive to developing programs focused on meeting near-term employer needs. This partly reflects the reluctance of universities and colleges to engage in what is viewed as training versus education. By contrast,

56. Note, the successful implementation of this approach is dependent on changing the federal government's four-year degree requirement. See Element 3.

community colleges have a long history of providing experiential education tailored to employers' more immediate, practical needs.

Recognizing this history, the CAE program expanded its certification program to encompass two-year institutions and is working with community colleges in states that authorize community colleges to provide more technical four-year degrees. The NSF's SFS program remains focused on supporting students seeking a traditional four-year degree, although it tries to enable a more diverse workforce to obtain such a degree by including two-year degree programs as subawardees of four-year institutions. Under the SFS program, students in two-year programs are only eligible for scholarships if they complete a four-year degree program. The program's performance metrics reflect this focus on four-year degrees (e.g., number of supported students completing a four-year degree).

Leaving aside the challenge of expanding the focus of these programs to include alternatives to four-year degree programs, there is another challenge to be addressed—matching graduates with employers. The DoD's Cyber Scholarship Program offers possible lessons learned in this regard. The DoD program is similar to the SFS program but differs in important respects. Notably, the DoD has input into the selection of candidates for scholarships. Interviews suggest that agency input into the selection of candidates of the DoD program contributes to greater success, such as fulfilling service commitments and higher retention rates.

Most recently, CISA has focused on identifying and supporting education and training programs that can provide more experience-based programs and recruit effectively from a more diverse population. For example, CISA's Non-Traditional Training Providers (NTTP) program has just made its first set of competitive awards. The NTTP provides training is focused on historically underrepresented communities in cybersecurity. (See Chapter 5 for more information on the NTTP program.)

Experiential Learning

A key theme in the Study Team's research was the need for more emphasis on experiential learning to build practical skills and validate for employers that applicants possess such skills. There are a variety of approaches to providing experiential learning, but the main consideration is the quality and relevance of the scenarios. Cyber ranges are an important, but not the only, means to enable hands-on experience with various scenarios in simulated environments.[57]

Recommended Focus Area: Helping to ensure relevant scenario-based exercises and low-cost, adaptable platforms for experiential learning are accessible to education and training institutions

57. NIST defines cyber ranges as "interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing. A cyber range may include actual hardware and software or may be a combination of actual and virtual components. Ranges may be interoperable with other cyber range environments. The Internet level piece of the range environment includes not only simulated traffic, but also replicates network services such as webpages, browsers, and email as needed by the customer." "Cyber Ranges," NIST, https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf.

Actions to achieve progress in this area might include

- Identifying and resolving issues related to the collection of information on actual attacks, such as how to anonymize information and avoid compromising national security and proprietary interests;
- Rapidly developing scenario-based exercises;
- Providing funding to enable the development and dissemination of scenarios for use in education and training; and
- Providing funding to support access for education and training institutions to cloud-based platforms as a service.

Some interviewees told the Study Team that the greatest challenge is generating and making available high-quality scenarios relevant to current threats. Currently, incentives are not aligned with meeting this need. Private trainers do not have an incentive to share content, and the federal government sees itself constrained by legal and other barriers to collecting information about actual attacks for use in the development of training scenarios. Even if the federal government were to satisfy concerns related to collecting information about cyberattacks and their use in training scenarios, the government lacks the capacity and resources to systematically translate attack information into training scenarios and make them available to the public.

Organizations are attempting to develop cyber ranges that are more adaptable and less costly, understanding the need to enable improved scenario-based education relevant to evolving challenges. One example is the cyber range maintained by the Virginia Polytechnic Institute and State University, which provides affordable access to a cyber range platform adaptable to various needs and scenario-based exercises developed by faculty at schools participating in the program. A key ingredient is access to a cloud-based platform as a service, which offers scalability and adaptability. However, up-front costs can be prohibitive for many institutions.

Apprenticeships

Even with improved access to relevant scenario-based exercises and inexpensive, adaptable platforms, there are limits to the ability of education and training institutions to provide the practical skills needed by employers. The most direct way to provide workers with the practical skills employers seek is on-the-job experience. Of course, training new employees requires a significant investment with uncertain returns. Interviewees indicated that both public and private sector employers have been hesitant to make such investments. While the military services maintain major education and training programs for their officer corps and enlisted personnel, civilian federal government agencies have generally preferred to hire experienced personnel or contract for the service rather than hire entry-level talent and develop them in-house. In the case of the private sector, leading technology companies like Google, Microsoft, and Apple invest heavily in such training and made major commitments to training at the recent White House cybersecurity summit. Still, interviews indicate a reluctance by many private sector employers to invest in training employees, partly reflecting the concern that these investments will not be recouped in the context of high levels of employee turnover in cybersecurity and other IT jobs. This reluctance to invest in the training of entry-level hires has contributed to a zero-sum game of employers competing for the same limited pool of talent rather than growing the talent pool.

Apprenticeships are one of a few options (others include internships and cooperative education programs) for enabling potential new employees to get some on-the-job experience at organizations and for organizations to assess whether these persons are a good fit.[58] However, apprenticeships offer a more structured approach involving not only on-the-job experience but also mentoring and formal instruction, including relevant general knowledge and company-specific information. This structure is certainly the case with the Department of Labor's Registered Apprenticeships program. Moreover, registration under this program requires that apprentices be paid at a certain level. Paying participants is important to promoting diversity in the cybersecurity workforce. Internship stipends or salaries are often quite small or nonexistent, limiting access to talented individuals from disadvantaged groups.

Recommended Focus Area: Supporting the adoption of apprenticeship programs by the public and private sectors

Actions to achieve progress in this area might include

- Promoting awareness of the positive return on investment resulting from the screening processes provided by such programs and the higher retention rates for apprentices;
- Providing time-limited incentives to the private sector (e.g., temporary tax credits) to promote adoption and realization of the benefits of apprenticeships.
- Providing public agencies with funding to support apprenticeships in advance of employment decisions to enable their adoption; and
- Examining the military's approach to on-the-job training for possible lessons applicable to managing the challenge of mentoring related to taking the time of operational staff

There is some evidence that apprenticeship programs might offer at least a partial remedy to the current zero-sum situation. Pioneering efforts by leading actors, like IBM, and related research suggest that investments made in potential employees through apprenticeship programs can yield positive returns if properly administered.[59] These returns follow from cost savings related to higher retention rates for employees hired through apprenticeship programs and the avoided costs of recruiting and hiring more experienced employees who are less likely to stay as long.[60]

58. Robert Lerman, Lauren Eyster, Kate Chambers, "The Benefits and Challenges of Registered Apprenticeship: The Sponsors' Perspective," Urban Institute, Center on Labor, Human Services and Population, March 2009. In a 2009 survey of employer sponsors of DOL's Registered Apprenticeship Program, the most frequently cited benefit of apprenticeship, identified as very important by over 80 percent of sponsors, was that it helped meet their demand for skilled workers. The second most frequently cited benefit (noted by 72 percent of sponsors) was apprenticeship's role in reliably showing which workers have the skills needed.

59. Zachery Eanes, "IBM Apprenticeship Program Pays While Candidates Prep for Tech Jobs," Governing, February 14, 2020, https://www.governing.com/work/ibm-apprenticeship-program-pays-while-candidates-prep-for-tech-jobs.html.

60. "Advancing Tech Apprenticeships," Consumer Technology Association, https://shop.cta.tech/products/advancing-tech-apprenticeships-a-guide-to-how-apprenticeship-is-a-

While there is a strong case for adopting apprenticeship programs, investments are necessary to make employers aware of the benefits and facilitate adoption. Also, employers will likely need an incentive, at least initially, to participate in apprenticeship programs and realize the resulting benefits. In the case of federal government employers, additional resources may be required to enable agencies to pay participants in apprenticeship programs before hiring them as employees.

Even if agencies come to appreciate the value of apprenticeships, it is not clear how to fund them. Attention will be needed to determine and build support for the appropriate funding mechanisms.

A critical element of apprenticeships—mentoring—has limited scalability. It is necessarily a one-to-one or one-to-few process. Moreover, it entails taking experienced operational personnel offline to undertake mentoring duties. There are lessons learned from the military on how to manage this challenge. For one, training can be systematized, with those trained then training those who come after them successively enabling higher-level and more specialized training.

Element 3: Overcoming Barriers to Recruiting Talent and Matching People to Jobs

As already discussed under Element 2, it is important to develop multiple pathways to careers in cybersecurity to help bring more—and more diverse—talent into the field. However, these efforts will have limited impact if the federal government and private sector employers continue to require four-year degrees and excessive experience levels. The four-year degree requirement for most positions has been a barrier to hiring by the federal government and private sector. Also, the requirement for one year of experience in a relevant position has hindered internal cybersecurity reskilling efforts, such as the Federal Reskilling Academy.[61]

Two major federal government efforts are underway to eliminate or work around the four-year degree requirement and other barriers to federal and private sector employment. One is the Cybersecurity Talent Management System (CTMS) program authorized by Congress to pilot test more flexible approaches to addressing the challenges of recruiting and retaining cybersecurity talent at DHS. The other is the Interagency Federal Cyber Career Pathways initiative, an informal coordination effort by human capital management officials working at three major federal agency employers of cybersecurity workers.

In addition to facilitating the ability of the federal government to recruit talent generally to staff agencies, the federal government must be able to recruit top talent from the private sector in a more targeted, near-term way to address immediate and critical challenges. This talent may not stay in the government but can help position solutions to various challenges that career staff work

---

future-of-work-solution-to-create-certainty-in-uncertain-times. See section on return on investment (p.10), which notes higher retention rates for apprenticeship hires.

61. The Federal Cybersecurity Reskilling Academy pilot program was launched in 2019 by the Chief Information Officer Council in conjunction with the OMB, OPM, and the Department of Education. The program aimed to equip current federal employees with cyber skills that would allow them to fill open cyber-related positions. The program could not place its graduates because they did not meet the one-year experience requirement for federal positions. This initiative was transferred to CISA and is under evaluation to determine how this challenge can be addressed.

to implement over the longer term. Also, it is important to tap into private sector talent as a surge capacity in the wake of major cyberattacks.

The success of efforts to eliminate or work around the four-year degree requirement in the federal government and the private sector ultimately will depend on developing an alternative basis for assessing applicants' capabilities. This challenge is addressed in part under Element 2, which discusses ways to help ensure that job candidates have the competencies needed by employers, such as incorporating experiential learning (e.g., cyber range testing) into educational curricula and apprenticeship and related programs that enable employers to assess the fit of potential employees in the context of structured on-the-job experience and related education and training.

Another factor critical to enabling alternative pathways to cybersecurity careers is strengthening the credibility of certifications. Employers must have confidence that certifications are reliable indicators that applicants have the knowledge and skills needed to perform on the job.

Recommended Focus Area: Expanding the Cybersecurity Talent Management System (CTMS) to provide flexibilities that will help the federal government compete with the private sector and attract and retain top talent

Actions to achieve progress in this area might include

- Expanding the authorities of the CTMS program to cover all appropriate cybersecurity work roles; and
- Quickly evaluating the Department of Homeland Security (DHS) pilot and, if successful, expanding the program to other agencies.

In recognition of the four-year degree requirement and other barriers to the federal government's ability to recruit and retain cybersecurity personnel, the DHS was authorized to undertake a major human capital pilot program. After years of delays, the DHS launched the pilot in November 2021. When in place, the CTMS will offer new ways to describe work, identify and encourage applicants, consider time/professional experience, evaluate applicants and employees, and manage career progression. It also will allow the DHS to hire cybersecurity professionals under the excepted service. However, the congressional authorization of the CTMS pilot limits hiring to a total of 150 positions. The CTMS pilot will reach this limit by filling vacancies as they occur in existing positions. Also, the CTMS will take several years to implement fully; even assuming success, it is unclear if and when the federal government might adopt this new system more broadly.

Recommended Focus Area: Making the most of hiring flexibilities within the federal personnel system in the near term

Actions to achieve progress in this area might include facilitating coordination among mission agencies and mission support agencies, such as the Office of Personnel Management (OPM) and NIST/NICE, needed to develop and implement more systematic approaches to exploiting hiring flexibilities within the federal personnel system.

As already noted, the implementation of the CTMS pilot will take some time, and it is not clear if and when the authorities under this pilot will be extended to the rest of the federal government. In the near-term, federal agencies will need to make the most of hiring flexibilities to work as well as possible within the existing federal personnel system. Moreover, this should be done in a consistent way across agencies. An example of such an effort is the Interagency Federal Cyber Career Pathways working group chaired by human capital management officials at DoD, CISA, and Veterans Affairs. This grassroots effort, launched by human capital management officials in 2019, aims to implement Executive Order 13870, *America's Cybersecurity Workforce*.[62] Since its formation, this group has sought to merge disparate federal cyber workforce efforts, develop and promote cyber workforce guidance and best practices, and standardize implementation of the *NICE Framework* by creating Cyber Career Pathways for *NICE Framework* work roles.

The success of any such effort will depend on effective coordination between mission agencies, the OPM, and NIST/NICE. In the case of the Pathways initiative, representatives of these mission agencies, the OPM, and NIST/NICE participate in joint deliberations, but effective coordination has been hindered by diverse agency responsibilities and sometimes conflicting priorities. Divergences across agency priorities are difficult to resolve in the absence of overarching leadership.

Recommended Focus Area: Making it easier for federal agencies to tap top private sector talent to meet immediate cybersecurity needs

Actions to achieve progress in this area might include

- Exploring models, such as the US Digital Service, to bring private sector talent into the government for fixed terms to be deployed to help agency staff solve critical problems; and
- Exploring options for developing a "cyber reserve" that would enable the federal government to quickly tap private sector cybersecurity experts in the wake of major cyberattacks.

As discussed in Chapter 2, it can be difficult for the federal government to compete with the private sector for the limited supply of top cybersecurity talent. In addition, there are situations where the federal government needs to quickly scale up its cybersecurity workforce, such as in response to cyberattacks. One approach, which has been introduced in legislation, is to create a "Civilian Cyber Security Reserve" at the DHS and DoD. The reserves would consist of former federal employees or military personnel with cybersecurity expertise. These individuals would be required to respond to a call to activation.[63]

Another option to fill critical federal workforce gaps strategically in the immediate term with top talent might be an approach modeled on the US Digital Service. The US Digital Service deploys teams of experts to federal agencies to help with short-term priorities, such as implementing new

62. The White House, *Executive Order No. 13870: America's Cybersecurity Workforce*, 84 FR 20523 (May 2, 2019), https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce.
63. US Congress, *Civilian Cyber Security Reserve Act*, S. 1324, 117th Congress (2021).

programs or responding to crises.[64] Terms of employment are limited to a maximum of four years to help ensure teams are benefitting from fresh perspectives and cutting-edge skills and expertise.

Recommended Focus Area: Increasing employer confidence in certifications and encouraging a more flexible approach to cybersecurity position qualifications

Actions to achieve progress in this area might include

- Working with employers and the certification community to reach an agreement on work roles and related competencies, with attention to differences between needs of the federal government and private industry and between DoD and the civilian federal government;
- Basing certification to the extent feasible on experiential testing of knowledge and skills;
- Driving adoption of common standards across the federal government by establishing minimum qualifications for specific work roles, including by indicating what training certifications the person doing the work should have;[65] and
- Driving adoption of standards by the private sector through Office of Management of Budget (OMB) federal acquisition regulations incorporating requirements for work-related competencies in federal requests for proposals.

As discussed above, enabling alternative pathways into the cybersecurity workforce ultimately will depend on the willingness of employers to take a more flexible approach to qualification in recruitment. Currently, both government and private sector employers rely heavily on four-year degrees and, often excessive, experience requirements to help ensure they hire workers who can do the job with minimal on-the-job training. This reliance reflects a lack of confidence in certifications, including four-year degrees, as indicators of ability, the lack of reliable alternative screening processes, and often poor knowledge of work roles and related competencies (mix of knowledge and skills) needed.

An important first step in increasing employer confidence in certifications is to reach an agreement on the work roles and related competencies that certifications aim to validate. Employers are not always clear on the work roles that advertised positions intend to fill or the competencies required to perform the roles. Moreover, the definition and relative importance of work roles vary considerably between the government and the private sector.[66] Recognizing this,

---

64. US Digital Service, accessed December 21, 2021, https://www.usds.gov/.
65. Department of Defense, 8570 Information Assurance Workforce Improvement Program, November 10, 2015. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf. The DoD's 8570 program provides a precedent. DoD's 8570 program defines minimum training and certification requirements for cybersecurity-related positions in DoD using the NICE Framework.
66. HSSEDI, *Technical Options and Recommendations for Strengthening the Cyber Ecosystem*, August 2020 (this report is not for distribution). CDET contracted with MITRE's Homeland Security Systems Engineering and Development Institute (HSSEDI) to identify and prioritize the cybersecurity skill sets on which education and training efforts should focus. HSSEDI's work started with an assessment of current and future employer demand for cybersecurity skills. HSSEDI found that *NICE Framework* concepts do not adequately capture employer needs. NICE "tasks" are too granular and "work roles" too general. Given this constraint, HSSEDI developed an intermediate-level approach to analysis organized around cybersecurity "functions" determined to better reflect the actual skills sought by employers.

NIST has been working with industry to adapt the *NICE Framework* to better reflect the competencies related to work roles in industry and developing electronic tools to facilitate the integration of standards into human capital processes.

Work roles also vary considerably across the federal government, most notably between the DoD and the civilian federal government. This variance partly reflects the heavy reliance of the civilian federal government, in general, on contractors for operational services in contrast with the DoD, which tends to maintain more of its cybersecurity operations in-house.

Once agreement is reached on work roles and related competencies, these competencies should inform the development of common standards for educational curricula, experiential testing, and related certifications that can validate competencies. Essential to these efforts will be the development of relevant scenario-based exercises and low-cost, adaptable platforms discussed under Element 2.

Agreement on work roles and related competencies will never be complete. Consensus in such a complex and rapidly evolving field will be elusive. Still, the adoption of common standards is essential to guide educational and certification efforts that can inspire the confidence of employers and enable multiple pathways to cybersecurity careers. The Study Team's research suggests that the DoD's adoption of the 8570 standard catalyzed efforts in the certification community. Given the importance of contracting for the provision of cybersecurity services in the civilian federal government, the adoption of common standards by the private sector might be catalyzed through Office of Management of Budget (OMB) federal acquisition regulations that incorporate requirements for work-related competencies in federal requests for proposals.

Element 4: Assessing Performance and Promoting Innovation in Workforce Development Practice

The diversity of workforce development approaches pursued by federal agencies offers an opportunity to learn more about what might work best, which will help guide both federal government and private sector decisions regarding resource allocation and program scaling. The federal government also has a vital role in cultivating innovative approaches to cyber workforce development in partnership with academia, industry, and nonprofits to identify and implement them as appropriate.

Recommended Focus Area: Evaluating the performance of federal programs and private sector approaches to workforce development

Actions to achieve progress in this area might include

- Evaluating existing programs and initiatives against a set of metrics to guide decisions regarding the allocation of resources and program scaling; and
- Identifying priority areas for evaluation, such as K-12 outreach and education, experiential learning, and apprenticeships to determine which approaches are most effective.

Currently, the federal agencies undertaking workforce development programs are responsible for their assessment. The federal government needs the capacity to systematically evaluate different workforce development approaches to inform investment decisions and scale up promising approaches as part of a larger strategy. If tasked with collecting and analyzing cybersecurity workforce data, the proposed Bureau of Cyber Statistics could contribute to this capacity.

Based on importance and evaluation challenges, three possible priorities for assessment are K-12 education and outreach approaches, experiential learning programs, and the costs and benefits of apprenticeships. For example, as previously noted, federal agencies pursue multiple approaches to identify and engage talent to bring more people into the cybersecurity field, which may include targeting the existing noncybersecurity workforce and students. It is unclear which approaches to K-12 engagement are the most effective or how investments targeting adults in the existing workforce might be weighed against investments in K-12. Moreover, evaluating K-12 programs is complicated because the payoff is long-term and current privacy laws constrain collecting personally identifiable information on students.[67]

Recommended Focus Area: Cultivating innovative approaches to workforce development

Actions to achieve progress in this area might include

- Developing, implementing, and evaluating pilot projects;
- Awarding competitive grants for developing and evaluating innovative approaches to cyber workforce development; and
- Identifying and publicizing best practices implemented by federal agencies, SLTT governments, the private sector, and other countries.

The federal government can contribute to the development and adoption of innovative workforce development approaches by providing funding and publicizing successes. Potential areas to explore involve using technology to enhance training delivery and developing assessment tools to identify individuals with strong cybersecurity skills and aptitude. CISA might utilize public-private entities, notably the Information Sharing and Analysis Centers and the Joint Cyber Defense Collaborative, to gather input from the private sector on workforce trends, education and training best practices, and alternative workforce development approaches.[68] Two potential mechanisms for fostering innovation are federal pilot projects and competitive grants to the private sector to test different approaches to cyber workforce development and learn which work best to expand and diversify the cybersecurity talent pipeline.

---

67. The Family Educational Rights and Privacy Act (FERPA), 20 USC § 1232g, 34 CFR Part 99.
68. "Information Sharing and Awareness," CISA, accessed December 6, 2021, https://www.cisa.gov/information-sharing-and-awareness. The CISA Information Sharing and Analysis Centers are "sector-specific…non-profit, member-driven organizations formed by critical infrastructure owners and operators to share information between government and industry.
"Joint Cyber Defense Collaborative," CISA, accessed December 6, 2021, https://www.cisa.gov/jcdc.The recently formed CISA Joint Cyber Defense Collaborative "will bring together public and private sector entities to unify deliberate and crisis action planning while coordinating the integrated execution of these plans."

Chapter 4: Governance Framework for Cybersecurity Workforce Development

As described earlier, multiple agencies across the federal government implement workforce development programs, and Congress is considering legislation to fund new programs and approaches.[69] While current federal workforce development programs focus on varying aspects of cybersecurity workforce development, there has been no high-level, centralized leadership; coherent, integrated government-wide strategy; or effective interagency coordination and collaboration. As a result, 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. In addition, there has been no effective way to collaborate on common objectives across agencies to optimize efforts and outcomes

A governance framework can create a structure and processes for decision making—including planning, priority setting, and assigning roles and responsibilities—and accountability. The framework helps to ensure structures and processes will be institutionalized and will survive changes in leadership.

In its March 2020 report, the Cyberspace Solarium Commission called for the creation of a national cyber director (NCD) and a corresponding Office of the National Cyber Director (ONCD).[70] The Commission cited four areas of concern that the new position and office would address: producing and updating a national cyber strategy and then monitoring its implementation, having a qualified advisor to the President on cybersecurity matters, empowering a recognized leader with the statutory authority to manage interagency coordination and collaboration, and designating a spokesperson who could speak authoritatively to internal and external stakeholders about cybersecurity issues.[71]

Congress quickly acted on the Solarium Commission's recommendation, including the establishment of the ONCD in the National Defense Authorization Act (NDAA) for FY 2021. The first NCD was confirmed in June 2021. The creation of the ONCD presents an opportunity to establish an effective governance framework, with the NCD providing the necessary leadership.

---

69. For example, Senator Gary Peters (D-Mich.) introduced the Federal Rotational Cyber Workforce Program Act of 2021 on December 15, 2021. The bill calls for the creation of a rotational cyber workforce development program across several government agencies. *Federal Rotational Cyber Workforce Program Act of 2021*, S.1097.
70. *Cyberspace Solarium Commission Final Report*, p. 3.
71. Robert Chesney, "The NDAA's National Cyber Director: Justifications, Authorities and Lingering Questions," December 7, 2021, www.lawfareblog.com/ndaas-national-cyber-director-justifications-authorities-and-lingering-questions.

Essential Components of a Governance Framework for Cybersecurity Workforce Development

There are three essential and interrelated components for an effective governance framework for cybersecurity workforce development: leadership, strategy, and coordination. In combination, these three components will help ensure multiple federal agencies pull together in the same direction and expend their resources effectively and efficiently.

Leadership

Sustained leadership by and within the executive branch will be required to successfully develop and execute an overall strategy like that discussed in Chapter 3. Such leadership has been lacking in federal cybersecurity workforce development efforts until recently. The new NCD has the potential to play a cross-agency leadership role, similar to that played by the Director of National Intelligence following 9/11. The NCD should bring the relevant agencies together to develop a government-wide strategy for developing the national cybersecurity workforce.

Leadership is also needed to ensure necessary coordination and collaboration are happening across agencies, roles and responsibilities are clear, and agencies are held accountable for operationalizing the strategy. Based on program results, leadership should make decisions about which programs to scale. Leadership is also responsible for communicating the strategy and progress on achieving strategic goals to Congress and other external stakeholders and advocating for adequate resources to effectively implement the strategy.

Strategy

As noted in Chapter 3, disparate (and sometimes competing) national workforce development programs carried out by different agencies do not create a coherent government-wide strategy. The lack of a government-wide strategy for developing the national cybersecurity workforce has been noted previously by the Cyberspace Solarium Commission,[72] the US Government Accountability Office,[73] and others. By setting forth the vision and priorities for the federal government in developing the national cybersecurity workforce, the creation of a government-wide strategy will accomplish several governance goals, including enabling the establishment of clear roles and responsibilities, facilitating effective engagement with external stakeholders, and highlighting areas where improved coordination and collaboration are needed. Clarifying roles and responsibilities will promote transparency between the agencies, making it easier to identify areas where coordination and collaboration are needed and which agencies need to be involved. The strategy also provides the goals and objectives against which leadership can measure progress and hold agencies accountable.

Having a clear strategy in place will facilitate the federal government's effective engagement of external stakeholders. Congress will be able to steer resources at the appropriate scale to programs necessary to achieving the strategy. The private sector and state, local, tribal, and

72. *Cyberspace Solarium Commission: Executive Summary*; March 2020, p. 3, 9 (Key Recommendation 1.5: Diversify and Strengthen the Federal Cyberspace Workforce)
73. US Government Accountability Office, GAO-20-629, C*ybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*.

territorial (SLTT) governments will understand which agencies are responsible for programs affecting them, enabling them to engage more effectively with the federal government.

Coordination

In the past—and currently—coordination between federal agencies has been mostly informal and voluntary. The effectiveness of coordination has been uneven and often has depended on the initiative of individuals at the programs and agencies involved.[74] Examples of current coordination mechanisms include the National Institute of Standards and Technology National Institute for Cybersecurity Education (NIST/NICE) Interagency Coordinating Council, which convenes federal agency representatives working on national workforce development, and Community Coordinating Council (comprised of industry, academic, and nonprofit participants, in addition to government officials); and the National Centers of Academic Excellence (CAE) program, led by the National Security Agency (NSA) in partnership with the Department of Homeland Security (DHS).

However, existing interagency mechanisms primarily facilitate information exchange and may not successfully promote reaching an agreement on strategies and approaches to address present challenges. Further, there are indications that even information-sharing has been sporadic and ineffective at times. Representatives of several agencies interviewed by the Study Team expressed concern about not having insight into other agencies' activities. They provided examples of finding out about other agency initiatives (in some cases duplicating their own efforts) after those initiatives were well underway or complete. With multiple agencies carrying out programs in the same mission space, a lack of coordination is particularly problematic. An example of multiple agencies working in a similar space is that at least four agencies—the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Education, NIST, and the NSA—are implementing K-12 programs. Such efforts pursued independently may lead to duplication, confusion (among both agencies and external stakeholders), and lost opportunities to leverage the work of other agencies.

Office of the National Cyber Director

The ONCD is well-positioned to lead the federal workforce development governance structure. The NCD and the supporting office can provide the authoritative leadership necessary to deliver strategic direction and prompt collaboration and coordination among federal agencies to achieve long-term workforce objectives. However, the ONCD must have sufficient authority and resources to accomplish this important function. Congress specified the ONCD's authorities and much about its operational framework, including its size and characteristics, as listed in Figure 5.[75]

---

74. US Government Accountability Office, GAO-21-288, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, March, 2021, https://www.gao.gov/products/gao-21-288.
GAO-20-629, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, September 22, 2020.
75. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No 116-283, (2021).

Figure 55. Office of National Cyber Director: Key Characteristics Related to Workforce Development

Office of the National Cyber Director (ONCD)

Duties

- Advise the President on cybersecurity policy and strategy.
- Lead the implementation and coordination of national cyber policy and strategy.
  - Monitor and assess the effectiveness of implementation.
  - Make recommendations to changes in organization, personnel, and resources.
  - Review annual budget proposals to advise how consistent they are with cyber policy and strategy.
- Offer advice and consultation to the National Security Council, Homeland Security Council, and relevant federal departments and agencies on the development and coordination of national cyber policy and strategy.
- Coordinate and consult with private sector leaders on cybersecurity issues with the Director of CISA, Director of National Intelligence, and other federal departments and agencies.

Structure

- Employ a maximum of seventy-five individuals.

The ONCD is in the Executive Office of the President. Such offices are typically responsible for policy development and oversight. They influence agencies' work by developing strategies and overseeing agency budgets in coordination with the Office of Management and Budget. Offices in the Executive Office of the President rely on the expertise and resources of federal agencies to assist in policy formulation and operational program execution. Examples of this include the National Security Council staff (with the Departments of Defense and State and the Intelligence Community), the Office of National Drug Control Policy (with the Department of Health and Human Services), and the Office of the US Trade Representative (with the Department of Commerce). With the ONCD as the new center of gravity in cybersecurity, CISA should be resourced to assist the ONCD with operationalizing the ONCD's strategy, policies, and programs—including workforce programs as a key part of the ONCD's overall priorities.

In fall 2021, the ONCD issued *A Strategic Intent Statement for the Office of the National Cyber Director* (*Strategic Intent Statement*). In recent hearings, congressional leaders have asked the NCD about his overall objectives and authorities and how his office would interact with other agencies, including CISA, the FBI, and federal chief information security officer and chief information officer positions in the cybersecurity field.[76] The *Strategic Intent Statement* partially responds to these questions by describing how the NCD intends to interact with other key

76. National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems, Hearing Before the Committee on Homeland Security & Governmental Affairs, 117 Cong. (2021), https://www.hsgac.senate.gov/hearings/national-cybersecurity-strategy-protection-of-federal-and-critical-infrastructure-systems.

governmental cybersecurity-related positions to develop policy and address challenges. This document explicitly underscores the coordinative and leadership roles of the NCD while carefully drawing lines around the authorities and responsibilities of other key players in the field.[77] The NCD highlights that his office will work "in partnership with the National Security Council, the OMB, other White House offices, CISA and its partner Sector Risk Management Agencies, government stakeholders at every level, and the private sector."[78]

In so doing, the NCD notes that the ONCD will "realize its outcomes" through seven lines of effort, including one on workforce development. In addition, the ONCD will hold itself accountable for achieving four outcomes, all necessary precursors to successful national cybersecurity workforce development: (1) ensuring federal coherence, (2) improving public-private collaboration, (3) aligning resources to aspirations, and (4) increasing present and future resilience.

The first of the ONCD's stated outcomes—federal coherence—has been hindered by the lack of an overall strategy that clearly lays out goals and the roles and responsibilities of federal agencies in contributing to the achievement of those goals. This, in turn, has challenged agencies' ability to effectively collaborate and coordinate with each other.

Finding 4.1: Although active collaboration between leaders of the ONCD and CISA has led to great strides in coordinating initiatives and resources for meeting the nation's larger cybersecurity challenges, federal agencies are not clear about their developmental, implementation, and operational responsibilities for workforce development and how these fit together to accomplish the larger workforce development objectives of the nation. As discussed in the earlier section of this chapter, Essential Components of a Governance Framework, agencies sometimes have been implementing congressional direction and undertaking initiatives independent of each other for lack of an overall governance framework. Coordination and collaboration have depended largely on the initiative of individuals.

Recommendation 4.1: The ONCD should develop and implement an appropriate operating model and governance structure to integrate actions by CISA, the NSA, NIST, the DoD, and other relevant federal agencies and organizations involved in building the cybersecurity workforce for the nation. This includes coordinating with and specifying roles and responsibilities between and among agencies.

Successful Operation of the ONCD: What Is Needed to Meet Cybersecurity Workforce Development Goals

Key federal agencies have developed expertise and have notable accomplishments and leadership roles in workforce development. The ONCD can help achieve additional, larger objectives without disrupting or minimizing existing programs, initiatives, and activities. Hence, the approach should build on and go beyond current programs, particularly in coordinating with the private sector to better meet the nation's cyber workforce needs.

---

77. Including agencies associated with various sectors of the economy (see Figure 2 in Chapter 2).
78. *Strategic Intent Statemen*t, p. 8.

In sum, as the ONCD moves forward on workforce development, the NCD should specify important objectives that

- Avoid duplication or deletion of efforts and functions already established unless there is a reason to do so;
- Build upon important, successful relationships that have been established and clarify those relationships when helpful or needed;
- Avoid creating a bureaucracy that slows down innovation, hampers outreach, or damages successful programs already in place;
- Encourage innovation;
- Facilitate and expect ongoing communication between and among agencies;
- Mobilize and collaborate with other parts of the government, as appropriate, to support and expand on current efforts;
- Collaborate with the private and educational sectors to coordinate strategic issues and leverage best practices; and
- Identify and address unproductive duplication and gaps between agency programs.

The NCD will need resources to develop a comprehensive workforce strategy, and the role of and resources for the ONCD are only now being identified. For the time being, existing organizations will support the Director and the office. However, as new functions are required or if existing structures do not meet the ONCD's needs, then the NCD should consider requesting additional authorities or funding streams to enable the ONCD to meet its objectives. Optimally, the office will have authorities that allow it to operate flexibly to meet changing needs and goals.

Recommendation 4.2: Congress should ensure the ONCD has budget and performance assessment authority to lead and coordinate the programs that will develop the needed workforce, including authorities to drive agency implementation of these programs.

Because the responsibilities of the NCD are significant and the resources of the ONCD are limited, the NCD should establish an interagency body to assure communication, coordination, and collaboration among and across the multiple federal agencies and programs that already perform major roles in cybersecurity workforce development. Thus, a "leadership working group" or "council for cybersecurity workforce development" should be established and formalized under the auspices of and reporting to the NCD to address this significant and ongoing challenge.

Recommendation 4.3: The ONCD should establish and run a leadership working group or council for cybersecurity workforce development with responsibility for both government-wide and external cybersecurity workforce development programs. The ONCD should also charge a designated senior official as the leader of this working group. The ONCD should specify the authorities and responsibilities of the group and its leader and identify the major federal member organizations. Private sector, SLTT governments, and academic representatives could also be included as working group members, as appropriate, based on objectives.

Data to Quantify and Monitor Needs, Guide Plans, and Assess Progress

Effective design and management of cybersecurity workforce development must be "data-informed." If the NCD and agency program leaders are to make real-time adjustments to workforce development programs that reflect constantly shifting market demand, they require data sets that describe and document the quantity and types of skills the cybersecurity workforce needs. Reliable data is needed to document the successes and failures of existing workforce development programs. Further, the data necessary to make decisions on the value of new initiatives has been hard to come by, and assessment of results across programs has been difficult or impossible.

The federal statistical community currently includes thirteen bureaus throughout the executive branch. They collect, analyze, and disseminate data on specific topics where program operators and the public need meaningful, timely, reliable, and independent information. A well-established set of principles guides the bureaus.[79]

Recommendation 4.4: The ONCD should 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. One way of accomplishing this would be to establish a Bureau of Cybersecurity Statistics or a similar organization.

The *Cyberspace Solarium Commission Final Report* recommended that "Congress should establish a Bureau of Cyber Statistics to be charged with collecting and providing statistical data on cybersecurity and the cyber ecosystem to inform policy making and government programs."[80] That recommendation and proposed legislation to create such a bureau are focused primarily on collecting information from firms and organizations on the nature and frequency of cybersecurity incidents and threats;[81] however, it could be tasked with capturing data on cybersecurity workforce composition and needs, as well.

Establishing a Bureau of Cyber Statistics (or a Bureau of Cyber Data, which would not necessarily follow the full set of requirements for federal statistical agencies) could provide valuable information about cyber incidents, the cyber workforce, and other relevant data needed to design, plan, and evaluate cybersecurity workforce programs. Further, such data could enable the evaluation of programs' results as they are reported to ensure appropriate expenditures of federal funds. Such a bureau could provide or facilitate analysis of federal programs for excellence, scalability, and diversity, and support outreach across agencies for all federal cybersecurity workforce development activities.

---

79. National Academy of Sciences, *Principles and Practices for a Federal Statistical Agency: Seventh Edition,* March 2021, https://www.nationalacademies.org/our-work/7th-edition-of-principles-and-practices-for-a-federal-statistical-agency.
80. *The Cyberspace Solarium Commission Final Report*, p. 78.
81. *The Cyberspace Solarium Commission Final Report*.
US Congress, Senate, *Defense of the United States Infrastructure Act of* 2021, S. 2491.

Chapter 5: A Review of CISA Programs and Strategies

Congress's interest in the effectiveness of the Cybersecurity and Infrastructure Security Agency (CISA) workforce development programs and the partnerships it utilizes to execute them prompted the request for this study. CISA has a unique role in workforce development, given its technical expertise and knowledge of the workforce needs of state, local, tribal, and territorial (SLTT) governments and industry. Understanding how—and how well—CISA carries out its workforce development programs and the challenges it faces is necessary to best design and resource CISA for the role it should play within the government-wide strategy for developing the national cybersecurity workforce in the future.

CISA's History and Mission

CISA's predecessor, the National Protection and Programs Directorate, was established in 2007. In 2018, the Cybersecurity and Infrastructure Security Agency Act reorganized the National Protection and Programs Directorate and named it CISA. CISA's mission is to lead the effort to protect and enhance the resilience of the nation's cyber and critical infrastructure. Within that broad mission, in recognition that cybersecurity depends largely on a sufficiently sized and skilled workforce, one of CISA's goals is to reduce cyber-related risk in the nation by addressing the cybersecurity workforce gap. This goal includes creating a "cybersecurity talent pipeline" for the nation and the government by enhancing the education, training, recruitment, retention, and diversification of a world-class cyber workforce.[82] To meet this goal, CISA

- Supports efforts to increase the supply of national cybersecurity talent through traditional and nontraditional cyber education programs aligned with the *NICE Framework*;
- Continuously develops and promotes cybersecurity training programs dedicated to advancing the cybersecurity skills of the existing federal; state, local, tribal, and territorial (SLTT); and private critical infrastructure workforce; and
- Works to expand and accelerate cybersecurity personnel recruitment, training, and retention efforts.[83]

CISA's Director believes "addressing the cyber workforce shortage requires us to proactively seek out, find, and foster prospective talent from nontraditional places."[84] In written testimony before the House Homeland Security Committee, the Director noted the importance of collaboration and partnerships to CISA's workforce development goals.[85] CISA is building

82. Department of Homeland Security, *Statement of Work (SOW) for Cybersecurity Workforce Study*, May 3, 2021.
83. US Congress, Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-287, tit. VI, 132 Stat. 4168, https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf.
84. "CISA Awards $2 Million to Bring Cybersecurity Training to Rural Communities and Diverse Populations," CISA, October 2021, https://www.cisa.gov/news/2021/10/20/cisa-awards-2-million-bring-cybersecurity-training-rural-communities-and-diverse.
85. Jen Easterly, Written Testimony for a Hearing on Evolving the US Approach to Cybersecurity: Raising the Bar Today to Meet the Threats of Tomorrow, November 3, 2021, https://homeland.house.gov/imo/media/doc/easterly_testimony_full_110321.pdf.

"relationships, trust, and connectivity with state and local officials, private sector, and our interagency partners."[86]

Cybersecurity Defense Education and Training (CDET) is the branch within CISA primarily responsible for carrying out these activities.

CDET's Role in Workforce Development

CDET was formed in 2019 when CISA consolidated its externally focused cybersecurity education and training programs. At the time, CDET was a branch within CISA's Cybersecurity Division (see Figure 6).[87] In March 2021, CISA underwent another reorganization, and CDET was repositioned under Capacity Building, still within the Cybersecurity Division (see Figure 7). Capacity Building is CISA's central hub for building partnerships, including with federal, SLTT, private, and other critical infrastructure organizations. During the 2021 reorganization, several of CDET's personnel were reassigned to CISA's Office of the Chief Learning Officer and its Office of Strategy, Policy, and Plans.

CDET Budget, Size, and Structure

Total Budget: $52,087,000 in FY 21

Budget for CDET Programs: $46,437,000 in FY 21

Salaries and Benefits: $5,650,000 in FY 21

Staff Size: 19 staff with 3 vacancies

Structure: CDET branch manager oversees the front office and the two branches

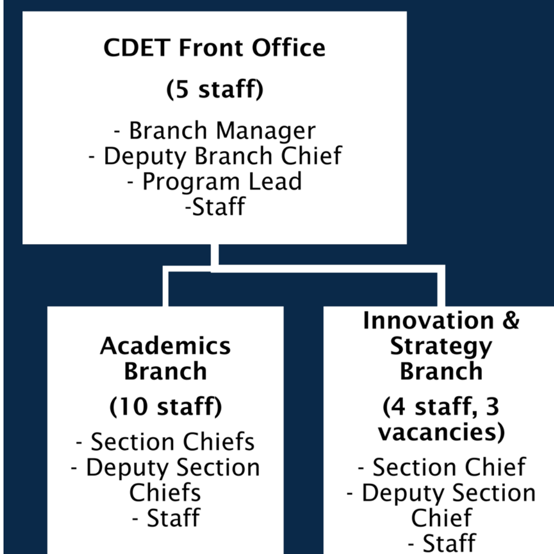
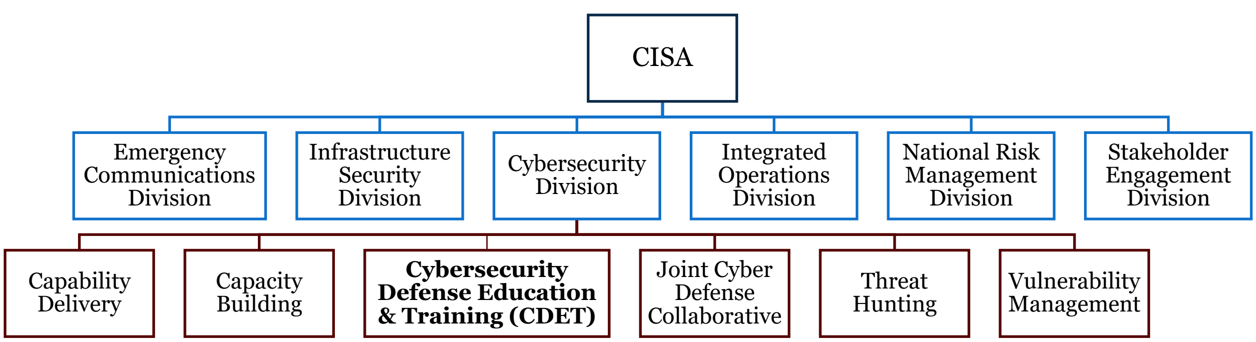


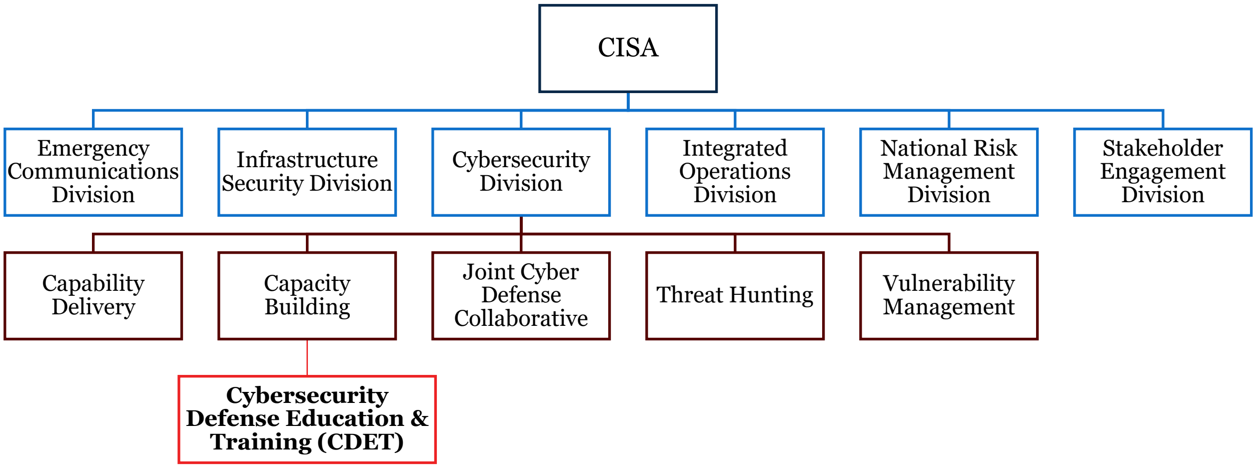
Figure 66. CISA Organization Chart (2019)



Source: CDET

86. Easterly, Written Testimony.
87. "Cybersecurity Division Mission and Values," CISA, accessed Dec 21, 2021, https://www.cisa.gov/cybersecurity-division.

Figure 77. CISA Organization Chart (2021)[88]



Source: CDET

Within the current organizational structure, CDET's responsibilities include strengthening training, education, and other activities of the Cybersecurity Division and CISA stakeholders (e.g., SLTT governments and private owner-operators of critical infrastructure assets). CDET's role also includes creating a national workforce development program. CDET accomplishes both missions by implementing five workforce development programs:[89]

- Cybersecurity Education and Training Assistance Program (CETAP): CETAP is a kindergarten through twelfth grade (K-12) grant program that has been awarded to the same grantee (CYBER.ORG) since the program's inception in 2012. The grant aims to build the cyber workforce by providing cybersecurity education and career awareness support to educators and students across the United States and its territories. CYBER.ORG meets that goal by delivering cybersecurity curricula for grades K-12, professional development for educators, and technology to classrooms to help reduce the cyber workforce gap and promote cyber literacy.
- Non-Traditional Training Provider Grant (NTTP): The NTTP is a new grant program (2021) to expand the cybersecurity talent pipeline. CISA awarded two separate grants for building three-year pilot projects in underserved communities. The grantees are building job placement programs that include cybersecurity certifications and apprenticeships. There is $2 million in total funding available for the first thirty-six months of performance.[90]

88. This organization chart shows the placement of CDET following a reorganization; the CDET source is dated August 2021. For illustrative purposes, CDET is the only subunit displayed at that level.
89. CETAP, the NTTP, PISCES, ICS Training, and the President's Cup Competition are CDET's more prominent workforce development programs. CDET has five programs that are recent additions to their portfolio and therefore are not covered in this report. Those programs are Federal Cyber Defense Skilling, Professors in Practice, Continuous Diagnostic Mitigation Training, Federal Virtual Training, and the Incident Response Series.
90. Notice of Funding Opportunity, Cybersecurity Workforce Development and Training Pilot for Underserved Communities, https://www.grantsolutions.gov/gs/preaward/previewPublicAnnouncement.do?id=94010.

- Public Infrastructure Security Cyber Education Systems (PISCES): PISCES is a nonprofit organization created by the Pacific Northwest National Laboratory (PNNL) that pairs post-secondary cybersecurity students with small local governments with no in-house cybersecurity expertise. Cybersecurity students receive local governments' metadata and search for vulnerabilities and compromises. PISCES is currently operating with partners in Washington State and Alabama.
- Industrial Control Systems (ICS) Training: ICS Training is a highly technical training program targeting the critical infrastructure community. The Idaho National Laboratory (INL) conducts the training. On-site training includes classroom and hands-on mock-ups of critical infrastructure dashboards and systems, enabling participants to see how their cyber actions impact critical infrastructure. The INL has expanded its virtual course offerings by transitioning some of its on-site training, including the critical infrastructure dashboards and systems, to the remote environment.
- President's Cup Cybersecurity Competition: This annual cybersecurity competition is open to federal employees and uniformed services personnel from the US government's executive departments and agencies. The competition was created by Executive Order 13870 on May 9, 2019.[91] The Software Engineering Institute develops the challenges and activities and presents participants with problems in both offensive and defensive cybersecurity disciplines. Challenges align with the *NICE Framework* work roles.

These five CISA programs emphasize experience-based education, training, and skill development and provide opportunities to develop the competencies required in cybersecurity positions. Through the various paths for delivering cybersecurity education, training, and skill development, the programs reach a broad audience that includes populations and communities that are underserved and underrepresented in the cybersecurity workforce.

Review of CISA's Cybersecurity Workforce Development Programs

Congress asked the Panel to assess "the extent to which CISA's strategy has made progress on workforce development objectives, including excellence, scale, and diversity." [92] The Study Team developed the following definitions for the three workforce development objectives:

- **Diversity:**[93] expanding participation in the cybersecurity workforce by underrepresented groups, such as people of color, women, people with disabilities, people who are neurodivergent, and rural communities

91. The White House, *Executive Order 13870, America's Cybersecurity Workforce*.
92. Consolidated Appropriations Act of 2021, HR 133, 116th Cong., 2nd sess., Congressional Record 166, no. 218—Book IV, daily ed. (December 21, 2020): H 8477. Congress did not define diversity, excellence, or scalability in the legislation. These definitions were developed by the Panel and vetted by stakeholders.
93. The definition of diversity contains examples rather than a complete list of the variety of demographics and backgrounds that need to be represented in the cyber security workforce. Other examples include age, socio-economic difference, disability, thinking style, education, career experience, and geography.

- **Excellence**: enabling education/training that provides the competencies (mix of knowledge and skills) required to meet the needs of employers and to allow employees to advance in their careers
- **Scalability**: enabling rapid and cost-effective expansion; encompasses economies of scale such as developing education and training that meets multiple goals (e.g., training covering numerous areas of knowledge, skills, and abilities)

CDET's programs—except for CETAP—are relatively new, making it challenging to evaluate program results. Instead, the Panel reviewed the planning, design, and execution of CISA's workforce development programs against the three study review objectives: diversity, excellence, and scalability. Even though CETAP is an older program, it is also difficult to evaluate results because K-12 outcomes take place over the long term, and current privacy law constrains collecting personally identifiable information on students. The Panel briefly reviews the effectiveness of CETAP based on available data at the end of this section.

Finding 5.1: The planning and design of most of CISA's cybersecurity workforce development programs—as implemented by CDET—meet diversity, excellence, and scalability objectives identified by Congress.

As described in more detail below, each program employs different approaches to cybersecurity workforce development and targets different audiences. Three of CISA's workforce development programs (CETAP, NTTP, and PISCES) consider diversity, excellence, and scalability in the design and execution. Two of CISA's programs (ICS Training and President's Cup) focus on excellence and scalability rather than diversity because both programs are highly technical and targeted to specific audiences. CISA has no control over the composition of these audiences and their diversity.

Objectives Checklist

	Diversity	Excellence	Scalability
CETAP	✓	✓	✓
ICS Training		✓	✓
NTTP	✓	✓	✓
PISCES	✓	✓	✓
President's Cup		✓	✓

Diversity

Three of the five CDET programs aim to expand the cybersecurity pipeline by targeting a diverse set of communities with different levels of cybersecurity experience (see Table 1). Collectively, these programs direct their efforts to multiple facets of the population, including, but not limited to, race, ethnicity, gender, age, socio-economic status, disability, thinking style, educational background, career experience, and geography.

Table 1. Application of the Diversity Workforce Objective to CISA Programs

	Diversity
CETAP	Several of CETAP's initiatives target underserved communities. The grantee, CYBER.ORG, addresses the inequities in cybersecurity "deserts"—rural and low-income communities where access to cybersecurity resources, professional development, curriculum, and education are disproportionately absent. In addition, CYBER.ORG's programming includes pilot projects targeting students at historically black colleges and universities (HBCU) and blind and visually impaired students. All of these communities are traditionally underrepresented or underserved in the cybersecurity field.
ICS Training	*Currently not applicable. ICS Training does not target diversity by design. However, ICS training can now reach a broader audience (both domestically and internationally) because it has transitioned more courses to the virtual environment.*
NTTP	The NTTP cooperative agreement, through its two award recipients, NPower and CyberWarrior, reaches a highly diverse population across several different segments: rural, underemployed, and unemployed.
PISCES	Through hands-on experience with local government organizations, the PISCES organization provides students at rural HBCUs and minority-serving institutions with real-world experience and on-the-job training, preparing them for careers in cybersecurity.
President's Cup	*Currently not applicable. However, with additional authorities and funding, the President's Cup competition could target nonfederal cybersecurity professionals and expand its reach to support and develop opportunities for underrepresented communities.*

Excellence

CISA strives to ensure excellence by carefully choosing partner organizations to implement programs (see Table 2). Three of the five workforce development programs (ICS Training, PISCES, and President's Cup) partner with federally funded research and development centers (FFRDC), which are widely recognized for employing world-class talent. In this case, CISA's FFRDC partners are experts in cybersecurity (PNNL and Software Engineering Institute) and critical infrastructure control systems (INL). CETAP's nonprofit partner, CYBER.ORG, had a proven track record in delivering K-12 education programs in Louisiana before being awarded the CETAP grant. The NTTP's nonprofit partners, NPower and CyberWarrior, were chosen because both organizations have experience creating cybersecurity pathways that begin with training and move to apprenticeships and job placement.

Finding 5.2: CISA's workforce development programs succeed because of CDET's ability to identify and partner with organizations with a proven track record in cybersecurity and workforce development.

Table 2. Application of the Excellence Workforce Objective to CISA Programs

	Excellence
CETAP	CETAP's partner, CYBER.ORG, has delivered K-12 cybersecurity education to students for more than a decade. CYBER.ORG's process to develop its curriculum and standards incorporates industry and educator input, resulting in the curriculum and standards being relevant to both industry and students.
ICS Training	The ICS Training is delivered in partnership with the INL, a Department of Energy national laboratory and an FFRDC with expertise in industrial control systems. This training, which includes a wide variety of course topics, is designed to help course participants develop cybersecurity skills that apply to their work environment. The training is recognized globally for its relevance. It is designed for critical infrastructure owners, operators, engineers, and managers.
NTTP	The NTTP cooperative agreement incorporates the workforce development objective of excellence through its purposeful selection of two organizations with already established training programs and partnerships and the quality of the training and certifications program participants can receive. The availability of apprenticeships and hands-on learning to program participants provides opportunities to develop necessary competencies for cybersecurity careers.
PISCES	CISA's PISCES partner, the PNNL, is an FFRDC specializing in computing and analytics, including cybersecurity. The PISCES program demonstrates excellence by providing university and community college students with real-world experience analyzing metadata on cybersecurity events that occur to local government organizations. This experience offers students opportunities to develop the competencies required of a cybersecurity analyst and other cybersecurity positions. The local governments benefit from no-cost cybersecurity event monitoring.
President's Cup	CISA's partner for the President's Cup Competition, the Software Engineering Institute, is an FFRDC at Carnegie Mellon University. The Software Engineering Institute is a leader in cybersecurity and has expertise in scenario-based cybersecurity training. The President's Cup challenges, both individual and team-based, center around the tasks and work roles of the *NICE Framework*. This pairing ensures that the competition incorporates competencies used by cybersecurity professionals in the federal government. The President's Cup further demonstrates a connection to excellence by providing a venue for the federal government's highly skilled cybersecurity talent to test their ability to resolve challenges based on real-world scenarios.

Scalability

Scalability is a cross-cutting feature of all five programs and is a consideration in each program's planning for the future (see Table 3). However, CISA, program officials, and partners frequently cite CDET's small staff size and a lack of predictable funding as factors limiting their ability to scale programs.

Table 3. Application of the Scalability Workforce Objective to CISA Programs

	Scalability
CETAP	The current CETAP grantee, CYBER.ORG, has a highly scalable program. CYBER.ORG developed a standard K-12 cybersecurity curriculum and provides it to educators online, contributing to CYBER.ORG's ability to scale. Another scalable approach CYBER.ORG uses is to "train the trainers." This approach means that by developing a more comprehensive network of training facilitators, the curriculum programming can reach more educators, who, in turn, reach more students. A challenge, however, is that this approach requires SLTT governments to apply the standards that enable the adoption of the curriculum in school districts. Additionally, a Cyberspace Solarium Commission white paper highlighted the CETAP grant program as an example of a scalable solution to the national cybersecurity education deficit.[94]
ICS Training	While the INL's advanced training classes must be held in person and are difficult to scale due to facility constraints and trainer availability, the INL offers a range of virtual courses. During the first year of the pandemic, the INL successfully transitioned additional in-person courses to online, which involved recreating the physical critical infrastructure ranges in the virtual environment. The virtual courses have no limit on the number of participating students. This virtual format poses a greater opportunity for scalability than in-person training.
NTTP	Scalability was factored into the design of the NTTP grant solicitation by providing additional points to potential grantees capable of reaching multiple CISA regions. The pilot programs implemented by the two grantees cover eight of ten CISA regions across the United States. However, the unpredictability in the funding of this grant, like that of several other CDET programs, limits the program's ability to scale. Thus, this program cannot plan on its expansion beyond the first three years of operation.
PISCES	PISCES has demonstrated the potential to deliberately scale this program through its current partnerships and the expressed interest of the institutes of higher education (both HBCUs and other minority-serving institutions) wanting to enroll in the program. PISCES has the potential to scale up its partnerships with states, localities, and higher education institutions, but funding constraints and varying state data laws have currently prevented more partnerships across the country. Despite these constraints, CISA intends to gradually scale up the program to avoid compromising its effectiveness.
President's Cup	The President's Cup program shares the competition challenges publicly through open-source code. With additional resources, CISA could scale up the program by translating this content into training curricula for education and training programs, which would further expand its reach.

94. Cyberspace Solarium Commission, *Growing a Stronger Federal Cyber Workforce*, 2020, p. 20, https://www.solarium.gov/public-communications/workforce-white-paper.

Review of CISA's CETAP Grant

This section offers an assessment of CDET's CETAP grant program. The DHS has been funding cybersecurity-related K-12 programs and education through its CETAP grant since 2012—before CISA and CDET were established. Reaching students early to encourage interest in cybersecurity careers and facilitate entry into jobs, apprenticeships, and other training programs, and two-year and four-year post-secondary programs is essential to expanding the pipeline. Strategies include raising awareness about cybersecurity careers; attracting students to STEM and cybersecurity tracks through competitions, camps, and gaming apps; supporting curriculum development and educator training; and encouraging middle and high school students to earn certifications. K-12 education and training can help increase workforce diversity by encouraging students in underrepresented populations and communities to explore cybersecurity careers.

CYBER.ORG, CETAP's only grantee, is CDET's longest-standing partnership for cybersecurity education and training. CYBER.ORG is an established organization in the cybersecurity education space that delivers cybersecurity curricula, educator training, and pipeline programs for underserved communities. CYBER.ORG has also developed K-12 cybersecurity education standards and works with state and local education boards on implementing K-12 curricula in schools. These standards aim to provide K-12 students with a fundamental level of cybersecurity knowledge and skills in preparation for cybersecurity careers. Next year, CYBER.ORG will reportedly launch a virtual cybersecurity competition and expects to host over ten thousand students from many states.

To address diversity, CYBER.ORG works on equitable access for cybersecurity education in high schools across the country. The organization also operates Project ACCESS, a pilot program for increasing blind and visually impaired high school students' access to cybersecurity education.

The Cyberspace Solarium Commission's white paper, *Growing a Stronger Federal Cyber Workforce,* stated that the CETAP grant is a foundational cybersecurity education program and an example of a scalable solution to the national cybersecurity education deficit. The Commission recognized the work of the CETAP grantee, CYBER.ORG, and recommended authorizing the CETAP grant in law and expanding it "to facilitate expansion of the professional development and other resources needed for supporting K-12 cybersecurity education." [95]

As noted above, CETAP is DHS's oldest workforce development program. Theoretically, it should be possible to evaluate the program's outcomes. However, evaluating K-12 programs is challenging because the outcomes of current investments may not be realized for several years. In addition, privacy laws constrain the collection of K-12 student data to track students as they progress through and after graduating from their programs.[96] Despite these challenges, CETAP has collected some data to evaluate the program against set metrics and is working to develop new and improved metrics.

CYBER.ORG collects nonevaluative metrics to help inform its programming, such as the number of educators enrolled in CYBER.ORG by state and the number of educators who have completed CYBER.ORG training by state. To try to measure the effectiveness of its training, CYBER.ORG

---

95. Cyberspace Solarium Commission*, Growing a Stronger Federal Cyber Workforce*, p. 20.
96. The Family Educational Rights and Privacy Act (FERPA), 20 USC § 1232g, 34 CFR Part 99.

surveys educators. One key survey question is, "I know how to help students get started with a cyber career." According to CYBER.ORG, 58 percent of educators agreed with this statement before taking CYBER.ORG training, and 90 percent agreed after taking the training.[97]

To pilot a more robust evaluation of CYBER.ORG's effectiveness, CYBER.ORG partnered with Louisiana Tech University to assess the impact of CYBER.ORG's curriculum on the number of students seeking cyber-related degrees after high school. The pilot study found "high schools that had teachers enrolled in CYBER.ORG curricula on average sent 4x more students into cyber-related college or university degree programs than those that did not" between 2014 and 2018.[98]

In its quest to further improve its performance metrics, CYBER.ORG is building a similar assessment into its recently launched Project REACH, a pilot program creating a cybersecurity talent feeder program between high schools and HBCUs. According to CYBER.ORG, it will work with participating universities to study the rate at which high school students in the program enroll in post-secondary cybersecurity degree programs.

Finding 5.3: Although CISA is not considered an education agency, it has the authority and responsibility under law to create programs focused on elementary and secondary education. There are several benefits of the Cybersecurity Education and Training Assistance Program's (CETAP) placement in CISA, as currently administered by CDET.

Since CETAP's creation, some have questioned its placement. Some external stakeholders point out that CISA is not really an education agency, and it does not have a culture of good communication and collaboration with other agencies. In addition, some industry actors and other external stakeholders have some distrust of DHS because they view it as a regulatory agency.

In general, any decision to move a grant program from one agency to another requires significant study and analysis to ensure the benefits of such a move would outweigh the disruptive effects associated with organizational change. With that in mind, the Panel and some interviewees believe there are several reasons why it is appropriate for CETAP to remain in CISA. Among other things, the law establishing CISA includes "increasing the pipeline of future cybersecurity professionals through programs focused on elementary and secondary education" as one of CISA's responsibilities.[99] The CETAP grant program strongly aligns with CISA's statutory responsibility.

CISA also has capabilities and relationships other agencies do not have that benefit and inform CETAP's K-12 programs. For example, CISA operational cybersecurity experts provide input into CETAP initiatives, such as curriculum standards, which contributes to the initiatives' quality and

---

97. Kevin Nolten, *Statement for the Record of Kevin Nolten Before the US House of Representatives on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection & Innovation,* July 2021: 5, https://homeland.house.gov/imo/media/doc/2021-07-29-CIPI-HRG-Testimony-Nolten.pdf.
98. "Our Impact," CYBER.ORG, https://cyber.org/about-us/our-impact. Also see, *2014-2018 Louisiana Tech University Enrollment in Cyber Engineering, Computer Science, & Computer Information Systems,* https://cyber.org/sites/default/files/2020-06/Louisiana%20Study.pdf.
99. Cybersecurity and Infrastructure Security Agency, 6 USC § 652.

gives them credibility.[100] CISA's relationships with and understanding of industry and SLTT governments need to inform CETAP's K-12 programs as well as facilitate the program's ability to partner with state and local boards of education and the private sector.

A recent example of CETAP's success is a partnership with North Dakota, which decided to implement the CYBER.ORG curriculum across the state. North Dakota provides a grant to a third-party contractor who will partner with schools to teach the CYBER.ORG curriculum to over one thousand teachers in many school districts. North Dakota's adoption of the CYBER.ORG curriculum is a promising example of what CETAP could help accomplish.

As mentioned earlier, the Cyberspace Solarium Commission recommended authorizing the CETAP grant in law. Congress followed through with the recommendation and funds the CETAP grant as a congressionally directed appropriation. Adding the CETAP grant to the President's budget would allow the Office of Management and Budget (OMB) and CISA to evaluate the impact of the grant against other K-12 education and training programs and would provide an opportunity to signal the long-term plans for the CETAP grant.

Recommendation 5.1: As a key approach to workforce pipeline building, the OMB, DHS, and CISA should sustain funding for CETAP in the President's budget request to better integrate and update the grant in accordance with future planned K-12 workforce activities.

Challenges Facing CISA's Workforce Development Program

Despite the challenges facing CISA's workforce development programs detailed below, CDET has accomplished much in the three years since its establishment, as shown in the discussions of CDET's programs earlier in this chapter. Implementing a workforce development program in a field as dynamic as cybersecurity is no small feat, and CDET did so with strategic consideration of diversity, excellence, and scalability. The leadership teams at CISA and CDET are passionate about contributing to cybersecurity workforce development in a way that complements other federal agencies. They recognize the unique position of CISA as an asset. Rather than building new workforce development programs or duplicating the work of other federal agencies, CISA and CDET are exploring ways to invest in strategies that fill a unique void in cybersecurity.

The success of CISA's cybersecurity workforce development program is particularly notable because of recent leadership turnover at CISA, CDET's relatively small staff size, and CDET's limited authority to partner with post-secondary institutions. Each of these challenges is explained in more detail below. CDET has done an admirable job navigating these challenges while implementing a cybersecurity workforce development program.

Changing Leadership Priorities

CDET's mission focus has been in flux since its inception because of changes in leadership priorities at CISA. In response to congressional interest in a national cybersecurity education

100. CYBER.ORG, *K12 Cybersecurity Learning Standards, Version 1.0*, 2021, https://cyber.org/sites/default/files/2021-10/K-12%20Cybersecurity%20Learning%20Standards_1.0.pdf.

program, a CISA task force focused on creating a vision for national workforce development. The task force spent 120 days interviewing important stakeholders in government, academia, and the private sector. Their work culminated in a final report with national cybersecurity workforce development recommendations.

The final report and recommendations outlined programs emphasizing skills development and validation that would serve as an alternative and complement to four-year degree programs, thereby providing pathways to cybersecurity positions that are both more accessible and recognized by employers. Programs would include "academies" that provided entry-level knowledge and skills and "institutes" that provided more advanced, specialized knowledge and skills in areas such as penetration testing, industrial control systems, and incident response. Curricula would align with the *NICE Framework*, providing common standards against which to categorize and measure competency levels and include tests to demonstrate proficiency of skills through means such as cyber ranges.

In 2020, new leadership at CISA reprioritized workforce development to a narrower focus on the federal workforce and CISA stakeholders, such as SLTT governments and private owner-operators of critical infrastructure assets. At the same time, the OMB prioritized federal workforce development, while Congress provided CDET with funding and authorities to focus on national workforce development. Unclear mission focus has been a feature of CDET since its creation. Changing priorities led to disruptions and reorganizations and caused key staff at senior and nonsenior levels to leave the organization, limiting CISA's effectiveness. As a result, other agencies report challenges identifying the right CDET point of contact for questions about organizational priorities and workforce development programs. Without clear and consistent direction, CDET has been unable to pursue new initiatives, such as those recommended by the task force.

Small Staff Size

A small group of twenty-two staff members in CDET manages CISA's cybersecurity workforce development programs. As identified by Congress and discussed previously, scalability is a feature of CISA's workforce development programs. Scaling up will require partnering with additional grantees and additional staff to oversee the work of grantees. CDET staff are reaching the limit of what they can reasonably manage with their current set of grantees. As CISA's workforce development program scales up, additional staff capacity will likely be necessary.

Additionally, the five workforce development programs reviewed in this report are CDET's most prominent workforce development programs; however, they are not the only ones CDET is responsible for managing. As mentioned earlier, five new programs were recently added to CDET's portfolio.[101] Congress also entrusted CISA with new responsibility through the K-12 Cybersecurity Act of 2021; the Act requires CISA "to develop an online training toolkit for school officials."[102] These trends may continue or accelerate as a result of the new government-wide strategy.

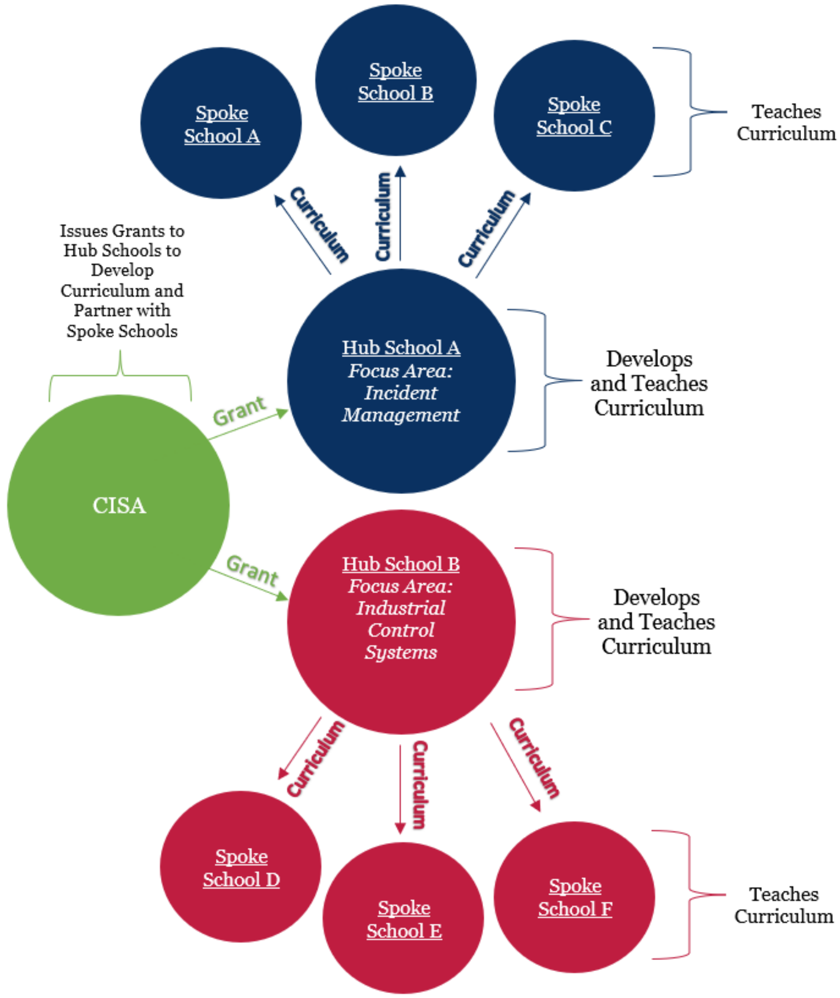
---

101. Those programs are Federal Cyber Defense Skilling, Professors in Practice, Continuous Diagnostic Mitigation Training, Federal Virtual Training, and the Incident Response Series.
102. K-12 Cybersecurity Act of 2021, Pub. L. No. 117-45, (2021).

Limited Authority to Partner with Post-Secondary Institutions

Given CISA's reliance on grantees to implement its programs and the need to scale programs considerably to address the incredibly large and growing workforce gap, CISA is planning to increasingly rely on the hub and spoke model for program delivery.[103] Under this model, CISA would issue grants to four-year universities, each of which would serve as a "hub" for several "spoke" schools (see Figure 8). Spoke schools would be a mix of geographically dispersed four- and two-year schools, including HBCUs and minority-serving institutions. Using this model, the hub schools develop cybersecurity curriculum in specific concentration areas, and the spoke schools teach cybersecurity curriculum. Each hub and its spoke schools would specialize in a single cybersecurity discipline, such as incident response, vulnerability management, or industrial control systems.

Figure 88. Hub-and-Spoke Partnership Model



To inform the approach, CDET is studying the hub-and-spoke model through a contract with the DHS Critical Infrastructure Resilience Institute. Under the contract, the University of Illinois Urbana-Champaign is leading the development of a comprehensive plan for implementing the hub-and-spoke partnership model. The other schools involved in the research are Auburn University, Purdue University, and the University of Tulsa.

CDET's PISCES program has implemented the hub-and-spoke partnership model to a limited degree and is exploring using the model to facilitate the program's expansion into additional states. The model enables PISCES to tap broader, more diverse talent pools by building relationships with HBCUs and community colleges. Rather than approaching individual universities and colleges in other states to expand its operations beyond Washington, PISCES is

103. The hub-and-spoke model is specific to post-secondary education.

working through state governments to identify state colleges and universities that might serve as hubs to build out the program and then extend it to other institutions. PISCES successfully expanded to Alabama in FY 2021 using this approach. In FY 2022, PISCES hopes to add two additional states.

Expanding the hub-and-spoke model to more "hub" schools will require partnerships with more schools, which—given its current authorities—will be challenging for CISA. Grants are a fundamental part of higher education funding. Schools typically require grants with multiple years of funding to develop and implement a new curriculum. Interviewees generally stated that universities and colleges require grants with multi-year funding (at least five years in duration) to commit to developing or implementing a new curriculum in their schools. Without additional grant-making authority, it is nearly impossible for CDET to expand its network of schools; therefore, scaling CISA's workforce programs nationally will require additional grant-making authority.

Recommendation 5.2: Congress should provide CISA with additional grant-making authority to effectively partner with colleges, universities, and community colleges. The additional authority should allow CISA to issue grants that can last up to five years in duration. CDET is the entity responsible for these initiatives within CISA.

CISA's National Workforce Development Role Moving Forward

As noted earlier, CISA's cybersecurity workforce development responsibility is codified in law. CISA is responsible for "increasing the pipeline of future cybersecurity professionals through programs focused on elementary and secondary education, postsecondary education, and workforce development; and building awareness and competency in cybersecurity across the civilian Federal Government workforce."[104] Despite CISA's statutorily defined national workforce development mission, different views about CISA's precise role have emerged within the executive branch and between the executive branch and Congress.

Needed now is an all-in effort to increase the size of the cybersecurity workforce pipeline, and CISA appears well-positioned to take on an expanded role as part of this effort. As the federal government's lead cybersecurity response agency, CISA also has a unique working relationship with SLTT governments, private industry, and critical infrastructure owner-operators.[105] As a result, CISA understands the country's cybersecurity shortcomings, as well as employer needs across multiple sectors. By leveraging its connections with essential stakeholders, CISA could help inform the government-wide strategy for developing the national workforce (see Chapter 3) by providing expert perspectives and knowledge on behalf of partner agencies. In addition, matching CISA's technical and policy cybersecurity expertise with programs designed to expand the talent pipeline has proven successful.

104. Cybersecurity and Infrastructure Security Agency, 6 US Code § 652.
105. As noted in Chapter 3, CISA's Information Sharing and Analysis Centers and the recently formed Joint Cyber Defense Collaborative are two forums CISA could use to cultivate innovative approaches to workforce development.

For CISA to maximize its effectiveness in cybersecurity workforce development, three conditions need to be met. First, CISA could benefit from a clear understanding of its role in cybersecurity workforce development in relation to other federal agencies. Consistent with Chapters 3 and 4 of this report, putting in place a governance structure and government-wide strategy that clarifies CISA's contribution to cybersecurity workforce development will enable the agency to plan accordingly and to justify requests for changes to its budget, staff size, and authorities. Understanding its role vis-à-vis other federal agencies will also enable CISA to coordinate and collaborate across the government and with other stakeholders more effectively.

A second condition required to maximize CISA's effectiveness is sustained leadership attention on cybersecurity workforce development. The new CISA Director has already made great strides on the issue, publicly and frequently emphasizing the importance of developing a national cybersecurity workforce development program and saying that "addressing the cyber workforce shortage requires us to proactively seek out, find, and foster prospective talent from nontraditional places."[106] However, as discussed, the branch currently responsible for CISA's national workforce development programs—CDET—has experienced changing priorities and leadership turnover. These changes have created challenges, such as uncertainty, which have impeded CDET's ability to plan and implement national workforce development programs. Sustained leadership direction includes defining roles and responsibilities within CISA and empowering the entity tasked with leading CISA's national workforce development program.

A third and final condition involves adequate staff capacity for program execution. As Congress recognizes, scalability is an essential feature of CISA's five workforce development programs. Reaching additional segments of the population with education and training resources will help expand the size of the cybersecurity workforce pipeline. As CISA's workforce development programs scale up, additional staff capacity will likely be necessary to support program execution. In addition, Congress has entrusted CISA with the responsibility for new workforce development programs; for example, the K-12 Cybersecurity Act of 2021 requires CISA "to develop an online training toolkit designed for school officials."[107] That trend may continue or accelerate as a result of the new government-wide strategy.

Recommendation 5.3: Congress should periodically review and adjust CISA's staffing, resources, and authorities as CISA's cybersecurity workforce development program changes.

106. "CISA Awards $2 Million to Bring Cybersecurity Training to Rural Communities and Diverse Populations," CISA.
107. K-12 Cybersecurity Act of 2021, Pub. L. No. 117-45, (2021).

Chapter 6: Conclusion

Cybersecurity attacks are becoming more frequent and sophisticated, requiring a responsive and competent cybersecurity workforce. Building the future cybersecurity workforce will require multiple approaches that draw upon individuals from all segments of society. Federal efforts to build a cybersecurity workforce must recognize that doing so will require a whole-of-nation approach where the federal government coordinates and collaborates with industry; educators; state, local, tribal, and territorial (SLTT) governments; and nonprofit organizations.

To effectively partner with this broad range of actors, the federal government will need to outline its goals and objectives in a government-wide strategy for developing a national cybersecurity workforce. At a minimum, the strategy should include four elements: (1) encourage more people to choose a career in the cybersecurity field through outreach and education, (2) enable education and training to build needed competencies and alternative pathways to cybersecurity careers, (3) overcome barriers to recruiting talent and matching people to jobs, and (4) assess performance and promote innovation in workforce development practices.

The Office of the National Cyber Director (ONCD) in the Executive Office of the President should lead the creation of a government-wide strategy. The ONCD is well-positioned to coordinate and lead the growing number of federal cybersecurity workforce development programs carried out by several federal agencies. To effectively lead the development of such a strategy, it will be important for the ONCD to have budget and performance assessment authority to ensure that the federal government's response is efficient and effective.

CISA appears ready to take on an expanded role as a part of the national effort. CISA has a unique role in workforce development because of its technical expertise and understanding of the workforce needs of SLTT governments and the critical infrastructure industry. Despite changing leadership priorities, a small staff, and limited grant-making authority to partner with additional organizations, CDET has successfully incorporated diversity and excellence in its programs, which are also designed to be scalable with additional resources and grant-making authority. As the newest federal agency with cybersecurity workforce development responsibilities, the ONCD, in partnership with CISA, might find different ways to leverage CISA's workforce development programs to increase the pipeline of future cybersecurity professionals and build awareness and competency in cybersecurity within the federal government. Any expansion of CISA's role will require additional staff, resources, and authorities.

The approach presented in this report represents a call to action for the federal government. Coordinating various federal agencies' cybersecurity workforce development programs into a coherent strategy should help operationalize workforce development resources across the government to minimize duplication of effort and focus the government's limited resources and staff on areas where it will add the greatest value for the nation as a whole. The strategy's success depends on strong and ongoing coordination between the executive branch and Congress.

Appendices

Appendix A: Panel and Study Team Member Biographies

Panel of Academy Fellows

Daniel Chenok:* (Panel Co-chair): Executive Director, IBM Center for The Business of Government. Former Vice President and Partner, Technology Strategy, Public Sector, IBM Global Business Services; Senior Fellow, IBM Center for the Business of Government; Government Team Lead, Technology, Innovation and Government Reform Policy Committee; E-Government/IT and OIRA Lead, Office of Management and Budget Agency Review Team; President-Elect Obama's Transition Team.

Karen Evans:* (Panel Co-chair): Managing Director, Cyber Readiness Institute; Former Chief Information Officer, US Department of Homeland Security; National Director, US Cyber Challenge and Partner, KE&T Partners, LLC; Administrator, Office Electronic Government & IT, Office of Management and Budget, Executive Office of the President; Chief Information Officer, US Department of Energy.

Dr. Marilu Goodyear:* Former Associate Vice Chancellor, University of Kansas; Former Director, School of Public Affairs and Public Administration, University of Kansas, Lawrence; Vice Provost for Information Services and Chief Information Officer, Department of Public Administration, University of Kansas, Lawrence.

Dr. Costis Toregas:* Director, Cyber Security Policy and Research Institute, George Washington University; County Council IT Advisor, Montgomery County MD; Board Member and Treasurer, Ecocity Builders; Board Member and Treasurer, Women in Cybersecurity; Board Member and Finance Director, National Cyber League.

Daniel Weitzner:* Founding Director, Internet Policy Research Initiative, MIT. Former US Deputy Chief Technology Officer for Internet Policy, Office of Science and Technology Policy, White House; Associate Administrator for Policy, National Telecommunications and Information Administration, US Department of Commerce.

Study Team Members

Brenna Isman, Director of Academy Studies, Ms. Isman oversees Academy studies, providing strategic leadership, project oversight, and subject matter expertise to the project study teams. Ms. Isman holds an MBA from American University and a BS in Human Resource Management from the University of Delaware.

* Academy Fellow

Sarah (Sally) Jaggar,* Project Director. Ms. Jaggar is a Project Director and Fellow. Her areas of expertise are strategic planning, program and organizational management and evaluation, and human capital. Formerly, she worked at the Partnership for Public Service. At the US Government Accountability Office, she was Managing Director for Mission Support in the Human Capital Office and Managing Director for Health Financing and Public Health Issues. She holds an MA from American University and a BA from Duke University.

Maria Rapuano, Senior Advisor. Ms. Rapuano has served as a Deputy Project Director and as a Senior Advisor for several Academy projects. Her areas of expertise include public policy, strategic planning, organizational design, and change management. She holds an MA in International Affairs from American University and a BA in Government from the College of William and Mary.

Jonathan Tucker, Senior Research Analyst. Mr. Tucker has served as a Project Director and as a Senior Research Analyst for several Academy projects. His areas of expertise include strategic planning, organizational design, change management, and science and technology/innovation policy. Mr. Tucker holds a PhD in Public Policy from George Mason University, an MS in Science and Technology Studies from Rensselaer Polytechnic Institute, and a BA from New College of Florida.

Adam Darr, Senior Research Analyst. Mr. Darr's areas of emphasis are governance, organizational change, human capital, project and acquisition management, customer service best practices, and strategic planning. Mr. Darr is pursuing a Master's in Public Administration at The George Washington University and holds a BA in Political Science and Homeland Security/Emergency Management from Virginia Commonwealth University.

Allen Harris, Senior Research Associate. Mr. Harris has experience assisting agencies with infrastructure design and construction assessment, strategic plan development, and best practice benchmarking. He graduated from the University of St Andrews, Scotland, in 2018, earning an MA, Honors in International Relations and Modern History.

Elise Johnson, Senior Research Associate. Ms. Johnson's focus areas include organizational transformation and change management, human capital, governance, and strategic planning. Before joining the Academy, Ms. Johnson earned a BA in Public Policy and a BA in Government and Politics from the University of Maryland, College Park.

Sarah Jacobo, Intern. Ms. Jacobo is pursuing an MA in Public Policy at the University of Maryland, College Park. She holds a BA in Public Policy and a BA in Government and Politics from the University of Maryland, College Park.

* Academy Fellow

Appendix B: CDET Self-Assessment Table to Assess Programs' Progress on Workforce Development Objectives

<table>
<tr><td colspan="4">Program Name:</td></tr>
<tr><td colspan="4">Background</td></tr>
<tr><td>Budget</td><td colspan="3"></td></tr>
<tr><td>Contract Type</td><td colspan="3"></td></tr>
<tr><td>Contract With</td><td colspan="3"></td></tr>
<tr><td colspan="4">Diversity, Scalability, and Excellence</td></tr>
<tr><td>How is this program intended to meet the three objectives?</td><td>Diversity:</td><td>Scalability:</td><td>Excellence:</td></tr>
<tr><td>What factors constrain CISA's ability to address these objectives more fully (e.g., lack of grant-making authority, lack of people to manage contracts, etc.)?</td><td>Diversity:</td><td>Scalability:</td><td>Excellence:</td></tr>
<tr><td>How is program performance measured against the objectives?</td><td>Diversity:</td><td>Scalability:</td><td>Excellence:</td></tr>
<tr><td colspan="4">Additional detail or comments
(Please provide any documentation of how the three objectives inform planning, development, and/or evaluation of programs in answer to the above questions.)</td></tr>
</table>

Appendix C: List of Interviewees

(Titles and positions are accurate as of the time of the Academy's initial contact)

Department of Homeland Security

Cybersecurity and Infrastructure Security Agency

- **Easterly, Jen**, Director
- **Todt, Kiersten**, Chief of Staff
- **Abernathy, Charles**, Office of the Executive Assistant Director, Cybersecurity Division
- **Bailey, Angela,*** Chief Human Capital Officer
- **Bastien, Greg**, Section Chief, CDET
- **Benson, Toni**, Deputy Associate Director, CDET
- **Caposell, Megan,** Associate Chief, Workforce Planning and Strategy
- **Chen, Johnson**, Program Lead, Hunt and Incident Response Team
- **Cusak, Austin**, Management and Program Analyst, Alliance Building Section, CDET
- **Driggers, Rick**, National Security Cyber Lead, Accenture Federal Services LLC; Former Deputy Assistant Secretary for Cybersecurity and Communications
- **Duffy, Michael**, Associate Director of Capacity Building (Acting), Cybersecurity Division
- **Goldstein, Eric**, Executive Assistant Director for Cybersecurity
- **Harmon, Will**, Deputy Branch Chief, Academics, CDET
- **Hartman, Matt**, Deputy Executive Assistant Director for Cybersecurity
- **Hayes, Erin**, Director of Operations, CTMS
- **Howell, Michael**, Office of Chief Learning Officer
- **Karas, Robert**, Rapid Action Force Chief, CISA; Former Associate Director, CDET
- **Lynch, Christiane**, Contract Specialist
- **Maroon, Sam**, Academics Manager, CDET
- **McCord, Latasha**, Education Section Lead, CDET
- **Montano, Carmen**, Contract Specialist Trainee
- **Montes, Regina**, Management & Program Analyst
- **Pearce, Ashley**, Branch Chief, Innovation & Strategy, CDET
- **Vrooman, Kenneth**, IT Specialist, INFOSEC; Former Senior Advisor
- **Webster, Anastacia**, Office of Chief Learning Officer
- **Williams, Kerri**, Contracting Officer

Department of Defense

- **Isnor, Matthew,** Program Lead, Cyberspace Workforce Development

*Academy Fellow

Department of Education

- **Palacios, Albert**, Acting Lead for STEM Education, Division of Academic and Technical Education
- **Tambert, Scott**, Division Chief for Institutions of Higher Education, Cybersecurity, Enterprise Cybersecurity Group, Technology Directorate, Federal Student Aid

Department of Labor

- **Cooper-Morrison, Sasha**, Business Engagement Team Lead and Supervisory Program Analyst, Office of Apprenticeship, Employment and Training Administration
- **Jackson, Dave**, Supervisory Program Analyst, Office of Apprenticeship, Employment and Training Administration
- **Mitchell, Cierra**, Division Chief, National Office of Apprenticeship, Division of Industry-Recognized Apprenticeship, Employment and Training Administration
- **Slee, Wendy**, Program Analyst, Business Engagement, Office of Apprenticeship, Employment and Training Administration

Department of Veterans Affairs

- **Paris, Chris**, Senior Advisor, Cyber Workforce Management

National Institute of Standards and Technology/National Initiative for Cybersecurity Education

- **Merritt, Marian**, Deputy Director/Lead for Industry Engagement
- **Petersen, Rodney**, Director
- **Pruitt-Mentle, Davina**, Lead for Academic Engagement
- **Wetzel, Karen**, Manager, NICE Framework

National Laboratories

- **Dopita, Chris**, Deployed Operations Project Manager, Pacific Northwest National Laboratory (PNNL)
- **Gray, Jessica**, Research Analyst, PNNL
- **Ley, Ralph**, Task Lead and Department Manager, Workforce Development and Training, Idaho National Laboratory (INL)
- **Maughan, Jason**, Division Program Manager, INL
- **Permann, Mark**, Program Manager, Workforce Development & Training, INL
- **Peterson, Monica**, DHS Portfolio Manager, INL

National Science Foundation

- **Piotrowski, Victor**, Lead Program Director, CyberCorps: Scholarship for Service, Division of Graduate Education

National Security Agency

- **Clark, Lynne**, CAE Program Chief
- **Janosek, Diane,** Commandant, National Cryptologic School

Office of Management and Budget

- **Cooch, Shila**, Director of IT Policy
- **DeRusha, Chris,** Federal Chief Information Security Officer (Deputy National Cyber Director, Office of the National Cyber Director)
- **Martorana, Clare,** Federal Chief Information Officer
- **Roat, Maria,*** Deputy Federal Chief Information Officer

Office of the National Cyber Director

- **Inglis, Chris,** National Cyber Director
- **Mourtos, Harry**, Senior Policy Advisor (Former CISA Competition Lead, CDET)

Office of Personnel Management

- **DeRamus, Tim,** Education Program Director, Center for Leadership Development, Human Resources Solutions

US Congress

- **Cook, Chris**, Professional Staff, Senate Committee on Appropriations, Subcommittee on Homeland Security
- **Daumit, Jim**, Professional Staff, Senate Committee on Appropriations, Subcommittee on Transportation, Housing, Urban Development, and Related Agencies
- **Dudley, Drenan**, Former Professional Staff, Senate Committee on Appropriations, Subcommittee on Homeland Security
- **Joachim, Bob**, Professional Staff, House Committee on Appropriations
- **Koziatek, Adam**, Coast Guard Fellow, House Committee on Appropriations, Subcommittee on Homeland Security
- **Smith, Justin**, Coast Guard Fellow, Senate Committee on Appropriations, Subcommittee on Homeland Security

US Government Accountability Office

- **Cruz Cain**, **Marisol**, Assistant Director
- **Gilmore, Michael**, Assistant Director, Information Technology & Cybersecurity
- **Hinchman, Dave**, Acting Director, Information Technology & Cybersecurity
- **Kalugdan, Tammi**, Assistant Director, Information Technology & Cybersecurity
- **McCracken**, **Lee**, Senior IT Analyst

*Academy Fellow

Subject matter experts and stakeholders

- **Applegarth, Claire**, Manager, Cybersecurity Operations and Integration, Center for Securing the Homeland, MITRE
- **Baeckel, Jonathan,** Global Information Assurance Certification
- **Branch, Megan,** Chief Operating Officer, CertNexus
- **Brewer, Dustin,** Sr. Director of Emerging Technologies and Innovation, ISACA
- **Bryan, Tony,** Executive Director, CyberUp, (Co-Chair, NICE Apprenticeship Community of Interest)
- **Caswell, David,** Head of Critical Infrastructure Engineering, Microsoft
- **Correia, Brian,** Director, Workforce Development, The SANS Institute
- **Dean, Callie**, Academic Outreach Coordinator, CYBER.ORG
- **Frisk, Jeff,** Director, Global Information Assurance Certification
- **Hendler, James,*** Professor, Rensselaer Polytechnic Institute
- **Lawrence-Keuther**, **Maureen,** Communications and Development Manager, Virginia Cyber Range, Virginia Polytechnic Institute
- **Lewis, James,** Senior Vice President; Director, Strategic Technologies Program, Center for Strategic and International Studies
- **May, Christopher**, Software Engineering Institute, Carnegie Mellon University
- **Mongeon, John,** Senior Manager of Development, CompTIA
- **Nolten, Kevin**, Director of Academic Outreach, CYBER.ORG
- **Oddo, Jennifer**, Executive Director, Strategic Workforce Education and Innovation, Youngstown State University, (Co-Chair, NICE Apprenticeship Community of Interest)
- **Paller, Alan**, President, Cyber Talent Institute; Founder, SANS Institute
- **Petrella, Simone,** Chief Executive Officer, Co-Founder, CyberVista
- **Raymond, David,** Director, Virginia Cyber Range; Deputy Director, IT Security Lab, Virginia Polytechnic Institute
- **Reeder, Franklin,*** Director Emeritus and Founding Chair, Center for Internet Security
- **Reynolds, Rita**, Chief Information Security Officer, National Association of Counties
- **Robinson, Doug,** Executive Director, National Association of State Chief Information Officers
- **Rosinkski, Alyssa,** Director of Global Channel & Partners, International Association of Privacy Professionals
- **Sanders, Ronald,*** Staff Director, The Florida Center for Cybersecurity, University of South Florida
- **Sheingold, Peter**, Department Manager, Cybersecurity Operations and Integration, Center for Securing the Homeland, MITRE
- **Stanger, James,** Chief Technology Evangelist, CompTIA
- **Stempfley, Bobbie**, Vice President and Business Unit Security Officer, Dell Technologies

*Academy Fellow

- **Ward**, **Meredith,** Director of Policy & Research, National Association of State Chief Information Officers
- **Welgan, Jeff,** Executive Director, Cybersecurity Workforce Solutions, CyberVista
- **Young, Mat,** Vice President of Global Advocacy, $(ISC)^2$

Appendix D: Timeline of Major Federal Initiatives and Events in Cybersecurity and Workforce Development

Below is a timeline of selected events germane to cybersecurity and workforce development. More information on the programs and initiatives included in this timeline can be found in Appendix F.

1999	• National Security Agency (NSA) launched the National Centers of Academic Excellence (CAE) program
2000	• CyberCorps: Scholarship for Service (SFS) program created under the Federal Cyber Service Training and Education Initiative, led by the National Science Foundation (NSF)
2001	• DoD launched the Cybersecurity Scholarship Program
2004	• Department of Homeland Security (DHS) became a cosponsor of both the CAE and SFS programs
2007	• DHS National Protection and Programs Directorate established
2010	• National Institute of Standards and Technology (NIST) establishes the National Initiative for Cybersecurity Education (NICE)
2012	• First version of the *NIST/NICE Workforce Framework for Cybersecurity (NICE Framework)* published • Cyber Education and Training Assistance Program (CETAP) awarded a grant to the National Integrated Cyber Education Research Center (NICERC) to undertake K-12 education programs (NICERC renamed CYBER.ORG in 2020)
2015	• Cybersecurity Information Sharing Act of 2015 passed and was the impetus for the current role of DHS CISA as collectors of cybersecurity threat information for "private entities, nonfederal government agencies, state, tribal, and local governments, the public, and entities under threats"
2016	• CAE curricula aligned with *NICE Framework* and CAE national and regional resource centers created • OMB and OPM released *Federal Cybersecurity Workforce Strategy*
2017	• Executive Order 13800 on cybersecurity workforce released (provides the impetus for DHS Cybersecurity Talent Management System initiative) • Executive Order 13801 on expanding apprenticeships is released and calls for the Secretaries of Commerce and Labor to promote apprenticeships, including in the cybersecurity field.

2018	• President's *National Cyber Strategy of the United States of America* released • DHS National Protection and Programs Directorate reorganized and rebranded as the Cybersecurity and Infrastructure Agency (CISA) as a result of the CISA Act
2019	• CISA external cybersecurity education and training programs consolidated under newly formed Cybersecurity Defense Education and Training (CDET) • CISA established 120-day National Cybersecurity Defense University (NCDU) Task Force to inform strategy for a national cybersecurity education and training system; *NCDU Roadmap and Operating Concept* developed • CISA *Strategic Intent* released • CISA launched President's Cup Cybersecurity Competition program • NSA's CAE program adds a designation for two-year colleges.
2020	• MITRE's HSSEDI report delivered to CDET • Cyberspace Solarium Commission report released • Department of Education establishes the CyberNet program, strengthening the teacher support in cybersecurity by providing teachers with a better understanding and ability to teach cybersecurity skills.
2021	• CISA granted broad authority to educate and train the next generation of cybersecurity professionals and authorized to promote its mission and services for recruiting (FY 2021 National Defense Authorization Act, Sec 1719) • White House National Cyber Director appointed and confirmed by the Senate • Cyberspace Solarium Commission released *2021 Annual Report on Implementation*

Appendix E: Cybersecurity Workforce Challenges, Strategies, and Federal Government Responses

The federal government has developed various programs, projects, and activities to address challenges to meeting the nation's cybersecurity workforce needs. The Study Team identified five challenges and corresponding general strategies for addressing them. The Panel presents the challenges (column 1) and strategies (column 2) and identifies federal government programs, projects, and activities (column 3) that correspond to each challenge. In some cases, a program, project, or activity relates to more than one challenge. This document intends to help make sense of the array of federal government efforts related to the different challenges and places them in the broader context. Therefore, the table below encompasses some challenges, strategies, and government responses that extend beyond the scope of this study.

It is important to emphasize that most of the programs, projects, and activities featured in this table are new, small-scale, or still in the planning or conceptual stages. There are only a few well-established programs with national scale and major funding. These include the NSA's CAE program, the NSF's SFS program, NIST's NICE program, and DHS's CYBER.ORG. See Appendix F for summary descriptions for the operational programs presented in this table.

Challenge	Strategies	Programs, Projects, and Activities

Not enough people going into the cybersecurity field	• Getting more students to choose a career in cybersecurity, with two overlapping focuses
	  ○ Younger students, whose career choices are more likely to be influenced
	  ○ Students from underrepresented populations (e.g., minorities, women, and rural communities)
	• Reskilling/upskilling adults already in the noncybersecurity workforce. Strategic focuses include:
		• NIST/NICE
		  ○ Cybersecurity Career Awareness Week
		  ○ K12 Cybersecurity Education Conference
		  ○ K12 Cybersecurity Education Community of Interest
		• CISA/CDET grant programs
		  ○ CETAP K-12 workforce development activities, including curriculum development and teacher training
		  ○ Nontraditional Training Provider grant for providing cyber training and apprenticeship for underserved and underrepresented communities
		• NSA K-12 programs
		  ○ Team Cyber (cyber competition)

Challenge	Strategies	Programs, Projects, and Activities
	◦ Federal government ◦ Civilian workforce, with a focus on underrepresented populations (research suggests focus on working adults is relatively productive approach to increasing diversity	◦ Regions Investing in Next Generation (RING) – supports skills development for high school students ◦ GenCyber (cybersecurity camp) • Department of Education CyberNet program – provides professional development to high school teachers • NSF Advanced Technological Education (ATE) program grantee, National Cybersecurity Training and Education Center (NCyTE), and National Cyberwatch Center – focused on expanding cybersecurity education and career awareness, primarily in community colleges • OMB Federal Cybersecurity Reskilling Academy pilot initiative — provided training for non-IT federal personnel (discontinued, pending redesign, following failure to place students due to federal personnel system requirements)
Workers not ready to perform on the job • Lack of practical skills, including technical and soft skills • Lack of fundamental knowledge and skills[108]	• Complementing classroom instruction ◦ Practical exercises ◦ Work-based learning (e.g., internships, apprenticeships) • Incorporating fundamental knowledge and skill sets into education and training programs	• NICE Apprenticeships for Cybersecurity Community of Interest • NICE Cybersecurity Skills Competitions Community of Interest • US Cyber Games – funded by NICE in the National Institute of Standards and Technology • CDET is developing the National Cyber Training Academic Range, a cyber range to provide practical skill-building exercises to complement classroom instruction

108. For a discussion of this gap in cybersecurity education and training, see William Crumpler and James A. Lewis, *The Cybersecurity Workforce Gap*, (Washington, DC: Center for Strategic and International Studies, January 2019), 3. The relevant knowledge and skills sets are described as follows: "there are certain knowledge sets and skills that are essential for any new employee in a critical technical work role, regardless of the field they are in or the specialty they adopt. This includes an understanding of computer architecture, data, cryptography, networking, secure coding principles, and operating system internals, as well as working proficiency with Linux-based systems, fluency in low-level programming languages, and familiarity with common exploitation methods and mitigation techniques."

<table>
<tr><th>Challenge</th><th>Strategies</th><th>Programs, Projects, and Activities</th></tr>
<tr><td></td><td>Competency-based education (emphasis on outcome/performance-based measures of competency)</td><td>CDET PISCES program — university-SLTT partnerships whereby SLTT governments provide universities with access to real-time network data to enable hands-on (entry-level) training of students in exchange for free network monitoring
CDET Critical Infrastructure Protection Training — provides specialized cybersecurity training related to industrial control systems applicable to a variety of critical infrastructure systems
Department of Labor Registered Apprenticeship Program
Registers industry-based cybersecurity apprenticeship programs that meet certain criteria, including structured on-the-job training
Department of Labor to date has only registered industry-based apprenticeship programs but is in talks with individual federal agency programs to develop RAPs</td></tr>
<tr><td>Barriers to matching people with competencies to jobs
Low confidence of employers in credentials of applicants
Qualifications for job postings not aligned with actual skills needed</td><td>Setting common standards defining work roles and related competencies to guide the development of education/training curricula and job qualifications/credentials</td><td>NIST NICE Framework[109] — outlines cybersecurity work roles and the tasks, knowledge, and skills involved in each work role; is the product of a consensus-driven, collaborative standard-setting process involving public and private participation
CAE program (hosted by the NSA in partnership with DHS) — primarily aims to establish</td></tr>
</table>

109. Executive Order 13870 on America's Cybersecurity Workforce encourages "the voluntary integration of the *NICE Framework* into existing education, training, and workforce development efforts undertaken by SLTT, academic, nonprofit, and private-sector entities."

Challenge	Strategies	Programs, Projects, and Activities
	• Developing tools to assess technical skills (e.g., cyber range-based exams and competitions) • Developing alternative sets of job qualifications	common standards in cybersecurity education, designating institutions as CAE that meet certain academic requirements; predates the *NICE Framework* process and its curriculum standards (knowledge units) subsequently mapped to NICE standards • Department of Energy CyberForce Competition – a cyber range competition for college students, focused on industrial control systems cybersecurity • Department of Labor Registered Apprenticeship Program (see above) • CTMS initiative — aims to develop new cybersecurity job series that provides for nondegree qualifications and higher pay • NIST/NICE CyberSeek — an interactive, web-based tool intended to provide detailed information on supply and demand in the cybersecurity job market, including skill sets and certifications needed for jobs (aligned with *NICE Framework* work roles)
Barriers to the federal government recruiting and retaining skilled workforce vis-à-vis private sector • Pay not competitive • Lengthy hiring process, in particular, the security clearance process • Inadequate investment in professional development	• Paying for education/training in exchange for a term of service • Providing more competitive compensation ○ Taking advantage of pay flexibilities ○ Developing alternative pay schedules ○ Taking advantage of hiring flexibilities • Exploiting (nonpay) advantages of federal government service related to mission-focus and professional development opportunities	• Federal Cybersecurity Workforce Summit and Webinar Series—hosted by NICE in partnership with OPM, showcase effective practices and solutions for recruiting, hiring, developing, and retaining cybersecurity workers based on existing authorities and innovative practices. • NSF SFS ○ Grants to qualifying universities, which then award scholarships to students in exchange for a term of federal government service • DoD Cyber Scholarship Program — provides grants to students attending CAE programs in exchange for a term of service in the military

Challenge	Strategies	Programs, Projects, and Activities
	○ career path planning ○ systematic training tied to career path ○ rotational/exchange programs • Developing a reserve of cybersecurity talent to tap for surge capacity	• CTMS initiative — aims to develop a new cybersecurity job series that provides for nondegree qualifications and higher pay, streamline the hiring process within existing authorities, and institutionalize a focus on the career development of employees • US Interagency Federal Cyber Career Pathways Initiative — seeks to more systematically exploit existing federal pay and hiring authorities and standardize implementation of the *NICE Framework* by creating Cyber Career Pathways (Pathways) for *NICE Framework* work roles • CDET President's Cup — cyber range competition for federal government employees
Small SLTTs and private sector organizations unable to afford to maintain cybersecurity staff or contract for services	Service pooling	• CDET PISCES program provides small SLTTs (less than 150 full-time equivalent employees) with free cybersecurity monitoring service in exchange for providing network data to universities for student training

Appendix F: Summaries of Government Programs, Projects, and Activities Supporting Cybersecurity Workforce Development

This document summarizes major federal government programs, initiatives, and activities supporting cybersecurity workforce development, listed by the lead agency.

Department of Defense, including the National Security Agency (NSA)

National Centers of Academic Excellence in Cybersecurity (CAE)

The CAE program was started in 1999 and is run out of the National Intelligence Program. The NSA and numerous federal partners, including CISA and the DHS, manage the CAE program. The program aims to establish standards in curriculum, build experience for students, and expand cybersecurity education across institutions. The CAE requires institutions to follow specific academic requirements and criteria to qualify for the CAE designation. Institutions must meet different requirements to qualify for one or more of three designations: Cyber Defense Education (CAE-CDE), Cyber Research (CAE-R), and Cyber Operations (CAE-CO). CAE designations come with no commitment of federal funds.

Cybersecurity Scholarship Program (CySP)

The CySP was created in 2001 as the Information Security Scholarship, then was renamed the Cyber Youth Scholarship Program in 2017. The scholarships are sponsored by the DoD chief information officer and administered by the NSA. The program supports a recruitment scholarship, retention scholarship, and a capacity building grant. The recruitment scholarship is given to students enrolled in CAE- schools. After graduation, the recipient must work in the DoD for the same length of time they received the scholarship. The Retention Scholarship is granted to DoD employees, both civilian and military, to pursue cyber-related master's or doctoral degrees, usually at a CAE-designated DoD school. The capacity building grants help schools improve their cybersecurity research and education.

Regions Investing in the Next Generation (RING)

RING is an NSA-sponsored cybersecurity skills development program for students in high schools without existing cybersecurity programs. The program helps students develop their cybersecurity skills with minimal hardware (e.g., only a laptop). The program's pilot course ran from August 2021 to May 2022, and RING will publish the full curriculum in summer 2022. The NCAE-C funds RING through K-12 pipeline grants.

GenCyber

The GenCyber camp program was started in 2014 by the NSA. Camp partners include the NSF, DoD, and Office of the Director of National Intelligence. The camp aims to introduce K-12 students and teachers to college and career opportunities within the cybersecurity sector. The camps are in person and for students, teachers, or a combination of both. There is a virtual teacher camp pilot program planned for the future.

Department of Education

Career and Technical Education (CTE) CyberNet

The Department of Education established the Career and Technical Education (CTE) program in 1998. CyberNet is an initiative between the Department of Education and other departments to address the gap of cybersecurity educators. The program's objective is to increase the supply of CTE teachers, which will increase the number of students prepared to enter the cybersecurity field. Teachers attend academies over the summer to strengthen their understanding and ability to teach cybersecurity skills. Teachers can use the academy accelerator as a resource and teaching support during the school year. CyberNet operates out of the Department of Education's budget for state grant and national programs under the CTE.

Department of Energy

CyberForce Competition

The CyberForce competition was started in 2016 by the Department of Energy. The competition focuses on cyber defense with an emphasis on industrial control system cybersecurity. Up to 400 collegiate students compete in the national competition. Students also have the opportunity to discuss post-graduate career paths with national laboratory experts and private-sector companies. In addition to the competition, the CyberForce website offers a virtual career fair, webinar series, and workforce portal.

Department of Homeland Security (DHS), including the Cybersecurity and Infrastructure Security Agency (CISA) and Office of the Chief Human Capital Officer

Cybersecurity Education and Training Assistance Program (CETAP)

CISA's CETAP grant program was established in 2012 and is administered by CDET. Since that time, the sole grantee has been CYBER.ORG (formerly NICERC). The program aims to improve cyber education for K-12 students by developing curriculum and providing it and educator professional development at no cost. The program includes routes to obtaining certificates that allow students to enter the workforce right out of high school. Currently, the program is active in all fifty states. CETAP has launched Project REACH, a pilot project creating a cybersecurity talent feeder program between high schools and HBCUs, and PROJECT ACCESS, a pilot program for increasing blind and visually impaired high school students' access to cybersecurity education.

Public Infrastructure Security Cyber Education System (PISCES)

PISCES is a nonprofit that partners with the PNNL and CISA. The program has been collaborating with the PNNL since 2019. PISCES provides cybersecurity for municipalities with 150 or fewer workers at no cost. The data from municipalities are sent to universities and colleges to provide real data to students for hands-on learning and data analysis skill development. The municipalities and academic institutions in the program are in Washington state, but the program recently expanded to Alabama with the inclusion of Alabama A&M University.

Critical Infrastructure Protection Training: Industrial Control Systems (ICS)

The ICS Training program is a highly technical training program targeting the critical infrastructure community. The INL conducts the training. On-site training includes classroom and hands-on mock-ups of critical infrastructure dashboards and systems, enabling participants to see how their cyber actions impact critical infrastructure. The INL has expanded its virtual course offerings by transitioning some of its on-site training to the remote environment, including the critical infrastructure dashboards and systems.

President's Cup Cybersecurity Competition

CISA started the President's Cup in 2019 to identify, recognize, and reward cybersecurity talent in the federal executive workforce. The competition gathers cybersecurity professionals from across the federal workforce to compete against each other in various challenges to test cybersecurity skills and knowledge.

Cybersecurity Education and Awareness Website

Cybersecurity Education and Awareness is a website maintained by the CISA National Initiative for Cybersecurity Careers and Studies. The website promotes cybersecurity education, training, and workforce development tools and resources. Employers, educators, professionals, and students can use the website to access the national cybersecurity training catalog, workforce development toolkit, the interactive *NICE Framework*, and more.

Cybersecurity Talent Management System (CTMS)

The CTMS is an initiative run by the DHS Office of the Chief Human Capital Officer that includes creating a job series for cybersecurity professionals with qualifications that allow for nondegree applicants and compensation that is more competitive with the private sector.

Non-Traditional Training Provider Grant (NTTP)

The NTTP is a new grant program (2021) to expand the cybersecurity talent pipeline. CISA awarded two separate grants for building three-year pilot projects in underserved communities. The grantees are building job placement programs that include cybersecurity certifications and apprenticeships.

National Institute of Standards and Technology (NIST)/National Initiative for Cybersecurity Education (NICE)

NICE Strategic Plan, Implementation Plan, and National K12 Cybersecurity Education Roadmap

The Cybersecurity Enhancement Act of 2014 requires the development of a strategic plan every five years to guide Federal programs and activities in support of a national cybersecurity awareness and education program. The NICE Strategic Plan was most recently updated in 2020, and an Implementation Plan was established in 2021. Additionally, a *National K12 Cybersecurity Education Roadmap* was introduced at the NICE K12 Cybersecurity Education Conference in December 2021.

NICE Interagency Coordinating Council

The NICE Interagency Coordinating Council convenes federal government partners for consultation, communication, and coordination of programs, projects, and initiatives that are focused on cybersecurity education, training, and workforce development to grow and sustain the nation's cybersecurity workforce. The monthly meetings provide an opportunity for the NICE Program Office, located at NIST, to communicate strategic priorities and program updates with key partners in the federal government and to learn about other federal government activities in support of the broader NICE community that includes the federal government, academia, industry, and SLTT governments. The group will also identify and discuss policy issues and provide input into the strategic direction for the NICE community.

NICE Community Coordinating Council

The NICE Community Coordinating Council was established to provide a mechanism in which public and private sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development. The Council includes three working groups that correspond to NICE Strategic Plan Goals (Promote Career Discovery, Transform Learning Process, and Modernize Talent Management) and four communities of interest (Apprenticeships, Competitions, K12 Education, and *NICE Framework* Users Group).

Workforce Framework for Cybersecurity (NICE Framework)

The first version of the *NICE Framework* was created in 2012, then updated in 2014, 2017, and 2020. The *NICE Framework* sets out a lexicon and standards to create uniformity in the cybersecurity field. Both employers and job seekers can use the *NICE Framework* to identify skills, standards, and capabilities suitable for different cybersecurity jobs. NIST intends for the *NICE Framework* to build the foundation for reducing the cybersecurity risks of organizations and serve as a guide for employers, education and training providers, and learners.

NICE Annual Conference & Expo

The NICE Conference is the annual convening of community members and thought leaders from education, government, industry, and nonprofits to explore ways of developing a skilled cybersecurity workforce ready to meet the challenges of the future. The event provides an opportunity to signal NICE strategic directions and priorities and a forum to showcase best practices. The event is hosted by Florida International University and New America and is supported by a cooperative agreement from NICE in the National Institute of Standards and Technology.

NICE K12 Cybersecurity Education Conference

The Annual NICE K12 Cybersecurity Education Conference, supported by the National Initiative for Cybersecurity Education (NICE), and hosted by iKeepSafe, features presentations that highlight effective collaborations in Cybersecurity workforce development in K-12, educational experiments and innovations, and other potentially impactful methods in support of growing the cybersecurity workforce. Attendees include training and educational leaders from academia, business, and government for two days of focused keynotes, panels, concurrent sessions, and discussions in support of the NICE Strategic Plan.

Federal Cybersecurity Workforce Summit and Webinar Series

The annual Federal Cybersecurity Workforce Summit and quarterly Webinar Series provides strategic and program updates from key departments and agencies that influence cybersecurity workforce legislation, policy, guidance, and standards. It also serves to highlight key projects and initiatives that support the growth and sustainment of the federal cybersecurity workforce. It also creates a sense of community among individuals in federal departments and agencies with similar responsibilities for building a superior cybersecurity workforce

CyberSeek

CyberSeek was launched in November of 2016 to provide accurate and actionable data about the cybersecurity job market in the public and private sectors. The website is a free tool for learning more about available cybersecurity jobs, including certifications, job titles, and alignment with the *NICE Framework*. The interactive career pathways tool shows common job transitions, key jobs within the sector, and information about the roles. The main partners for the website are NICE, Emsi-Burning Glass Technologies, and Computing Technology Industry Association (CompTIA). Funding is provided by a grant from NICE.

US Cyber Games

The US Cyber Games will result in the selection of the first-ever US Cyber Team to represent the United States at the 2022 International Cybersecurity Challenge held in Athens, Greece. The program consists of the US Cyber Open (anyone can enter) and the US Cyber Combine Invitational and culminates in selecting the US Cyber Team (Invitational participants and Team members must be US citizens aged eighteen to twenty-six). The program is operated by Katzcy in cooperation with NICE and is funded through a NIST cooperative agreement.

National Science Foundation (NSF)

CyberCorps: Scholarship for Service (SFS)

The SFS was started in 2000 and is operated by the NSF. The NSF program has professional partnerships with the DHS and OPM. The scholarships support undergraduate and graduate students for up to three years. After graduation, the recipient repays the scholarship through service in a US government position related to cybersecurity for the same length of time as the scholarship. In 2018, the SFS started a pilot program to expand into community colleges. The program supported institution capacity building until 2019 when that funding moved under another NSF program.

Advanced Technological Education Program

The Advanced Technological Education program has been active for over twenty-five years. The program supports and develops technicians in the STEM fields, beginning with high school and undergraduate students. The Advanced Technological Education program works on capacity building in educational institutions through curriculum development, professional development, and career pathways.

National Cybersecurity Training and Education Center

The National Cybersecurity Training and Education Center, housed by Whatcom Community College, received an Advanced Technological Education program grant in October 2021 from the NSF, which elevated the National Cybersecurity Training and Education Center to an Advanced Technological Education National Center. Over five years, the program will use this funding to expand cybersecurity education pathways, provide curriculum, engage industry, and support faculty through cybersecurity education professional development programming.

Office of Personnel Management (OPM)

Federal Cybersecurity Reskilling Academy

The Federal Cybersecurity Reskilling Academy pilot program was launched in 2019 by the Chief Information Officer Council in conjunction with the OMB, OPM, and Department of Education. The program aimed to equip current federal employees with cyber skills that would allow them to fill open cyber-related positions. Two pilot groups have completed the reskilling training through the SANS Institute. The first group of applicants had no cybersecurity or IT background, and the second was open to all federal employees, including those with a cyber background. The program could not place its graduates because they did not meet a one-year experience requirement for federal positions. This initiative was transferred to CISA and is under evaluation to determine how this challenge can be addressed.

Other Federal

Interagency Federal Cyber Career Pathways Working Group

The Interagency Federal Cyber Career Pathways Working Group (Working Group) was established by human capital management officials from the DoD, DHS/CISA, and Department of Veterans Affairs in July 2019 with federal endorsement from the Chief Information Officer Council, Chief Human Capital Officer Council, and Chief Learning Officer Council. The Working Group operates with the ultimate intent of working collectively with interagency partners to develop baseline cyber career resources aligned with *NICE Framework* work roles. More specifically, the Working Group seeks to merge disparate federal cyber workforce efforts, develop and promote cyber workforce guidance and best practices, and standardize implementation of the *NICE Framework* by creating Cyber Career Pathways (Pathways) for *NICE Framework* work roles.

Appendix G: Bibliography

(ISC)². *Cybersecurity Professionals Stand Up to a Pandemic: (ISC)² Cybersecurity Workforce Study*. Clearwater: (ISC)², 2020. https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.as.

Corbett, Christianne, and Hill Catherine. *Solving the Equation: The Variables for Women's Success in Science and Computing*. Washington: American Association of University Women, 2015. https://files.eric.ed.gov/fulltext/ED580805.pdf.

Crumpler, William, and James A. Lewis. 2019. *The Cybersecurity Workforce Gap*. Washington, DC: Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf.

CYBER.ORG. "Our Impact." Accessed September 22, 2021. https://cyber.org/about-us/our-impact.

"CyberCorps: Scholarship for Service," National Initiative for Cybersecurity Careers and Studies (NICCS), accessed December 21, 2021. https://niccs.cisa.gov/formal-education/cybercorps-scholarship-service-sfs.

CyberSeek. "CyberSeek Heatmap and Job Openings by NICE Cybersecurity Workforce Framework Category." Accessed August 25, 2021. https://www.cyberseek.org/heatmap.html.

EdWeek Research Center. *The State of Cybersecurity Education in K-12 Schools, Results of a National Survey*. 2020. https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf.

Homeland Security Systems Engineering and Development Institute. *Technical Options and Recommendations for Strengthening the Cyber Ecosystem*. 2020. *Note: this report is not for distribution.*

Ignatius, David. "Opinion: An Undeclared War Is Breaking out in Cyberspace. The Biden Administration Is Fighting Back." The Washington Post, August 10, 2020. https://www.washingtonpost.com/opinions/2021/08/10/an-undeclared-war-is-breaking-out-cyberspace-biden-administration-is-fighting-back/.

Maurer, Tim, and Arthur Nelson. *International Strategy to Better Protect the Financial System Against Cyber Threats*. Washington: Carnegie Endowment for International Peace, 2020. https://carnegieendowment.org/files/Maurer_Nelson_FinCyber_final1.pdf.

National Academy of Public Administration. *Increasing the Effectiveness of the Federal Role in the Cybersecurity Education*. 2015. https://napawash.org/academy-studies/increasing-the-effectiveness-of-the-federal-role-in-cybersecurity-education.

National Institutes of Standards and Technology, Workforce Framework for Cybersecurity (NICE Framework) – SP 800-181 Rev. 1, November 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

Office of the National Cyber Director, A Strategic Intent Statement for the Office of the National Cyber Director, 2021, https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf.

Partnership for Public Service and Booz Allen Hamilton. *Cyber In-Security II: Closing the Federal Talent Gap*. 2015. https://ourpublicservice.org/publications/cyber-in-security-ii-closing-the-federal-talent-gap/.

President's National Security Telecommunications Advisory Committee. *Report to the President on a Cybersecurity Moonshot*. November 14, 2018. https://www.cisa.gov/sites/default/files/publications/NSTAC_CyberMoonshotReport_508c.pdf.

US Bureau of Labor Statistics. "Employment Projections Database." Accessed August 25, 2021. https://data.bls.gov/projections/occupationProj.

US Cyberspace Solarium Commission. *2021 Annual Report on Implementation*. 2021. https://www.solarium.gov/public-communications/2021-annual-report-on-implementation.

———. *Final Report*. 2020. https://www.solarium.gov/report.

US Department of Commerce, National Institute of Standards and Technology. *Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181, Revision 1*. Washington, DC: US Department of Commerce, National Institute of Standards and Technology. 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

US Department of Defense Inspector General. *Audit of the Department of Defense Recruitment and Retention of the Civilian Cyber Workforce*. 2021. https://media.defense.gov/2021/Aug/02/2002819100/-1/-1/1/DODIG-2021-110.PDF.

US Department of Homeland Security. "Secretary Mayorkas Announces Most Successful Cybersecurity Hiring Initiative in DHS History." Press release. July 1, 2021. https://www.dhs.gov/news/2021/07/01/secretary-mayorkas-announces-most-successful-cybersecurity-hiring-initiative-dhs#:~:text=WASHINGTON%20%E2%80%93%20Today%2C%20Secretary%20of%20Homeland,additional%20500%20tentative%20job%20offers.

US Government Accountability Office. *CISA: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation, GAO-21-236*. 2021. https://www.gao.gov/products/gao-21-236.

———. *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges, GAO-21-288*. 2021. https://www.gao.gov/products/gao-21-288.

US Office of Management and Budget and US Office of Personnel Management. *Federal Cybersecurity Workforce Study*. Jul 12, 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf.

White House. "FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity." August 25, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-.

NATIONAL ACADEMY OF PUBLIC ADMINISTRATION®

1600 K Street, NW
Suite 400
Washington, DC 20006

Phone: (202) 347-3190
Fax: (202) 821-4728
Website: www.NAPAwash.org