National Cyber Workforce and Education Strategy

Unleashing America's Cyber Talent

JULY 31, 2023

OFFICE OF THE NATIONAL CYBER DIRECTOR
EXECUTIVE OFFICE OF THE PRESIDENT

THE WHITE HOUSE
WASHINGTON

July 31, 2023

Technology and humanity are intertwined. Technology itself does not have a value system; rather it carries the values of its owners and operators. Cyberspace is composed not only of *technology* and *protocols*, but also *people*. People are an integral part of cyberspace, both in creating and using it. In less than a generation, technology has transformed our daily lives – among other things, we pay bills, connect with families and friends, build businesses, and build communities. We rely on cyberspace for our national security, economic development, and innovation. More than any other domain – air, space, sea, or land – people conceived of and created cyberspace and will continue to improve it. The Biden-Harris Administration's 2023 National Cybersecurity Strategy establishes an affirmative, values-driven vision for a secure and resilient cyberspace that enables us to achieve our collective aspirations. To achieve a vision aligned with our values, we must ensure that *people* are appropriately equipped. This National Cyber Workforce and Education Strategy provides a critical element of the President's approach to securing cyberspace.

Today's digital landscape is defined by ever-increasing demand for cybersecurity skills. Frontier technologies that can address climate change, secure our nation, and advance the health and welfare of communities are creating a demand for early career and historically untapped talent. We must align these jobs of tomorrow to our approaches to skilling. However, there are structural challenges to building our cyber workforce and education system: hundreds of thousands of vacant cyber jobs; an insufficiently diverse workforce to fill those jobs; and barriers to accessing cyber education and training. The National Cyber Workforce and Education Strategy charts a path to resolving these challenges by working towards filling cyber jobs for working families. This Strategy leverages generational investments such as the Bipartisan Infrastructure Law, the Inflation Reduction Act, and the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act to achieve this goal.

The Office of the National Cyber Director will collaborate with the private and public sectors to realize the Biden-Harris Administration's vision to ensure cyberspace reflects our values: national security; economic security and prosperity; respect for human rights and fundamental freedoms; trust in our democracy and democratic institutions; and an equitable and inclusive society. Strengthening our cyber workforce and equipping every American to realize the benefits of cyberspace is a whole-of-nation endeavor. Each individual can contribute but no single actor can alone effect the necessary change at scale. Today, we call upon public and private partners to contribute to the implementation of this National Cyber Workforce and Education Strategy. We must drastically scale up our cyber skills to deliver this future, keep America secure, and ignite the next generation of American innovation.

Kemba Eneas Walden

Acting National Cyber Director

CONTENTS

INTRODUCTION 1
PILLAR ONE | EQUIP EVERY AMERICAN WITH FOUNDATIONAL CYBER SKILLS 8
PILLAR TWO | TRANSFORM CYBER EDUCATION 14
PILLAR THREE | EXPAND AND ENHANCE AMERICA'S CYBER WORKFORCE 25
PILLAR FOUR | STRENGTHEN THE FEDERAL CYBER WORKFORCE 33
IMPLEMENTATION 43
APPENDIX A: Definitions 44
APPENDIX B: Foundational Cyber Skills 47
APPENDIX C: RFI Respondents 49

"Digital technologies today touch nearly every aspect of American life."
President Joe Biden, March 2023

INTRODUCTION

This strategy details how we will strengthen our cyber workforce, connect people to well-paying, quality jobs, and advance the welfare, prosperity, and security of our society. The strategy seeks to transform cyber education. It advocates for a skills-based approach to build more robust cyber career pathways. The strategy aims to foster extensive collaboration between employers, educators, government and other key stakeholders to meet both urgent and long-term workforce needs. By equipping every American with cyber skills, they will be better prepared for today's jobs and able to participate in our interconnected society.

In less than a generation, digital technology has transformed our daily lives. Paying bills, taking classes, applying for jobs, and connecting with friends and family are just a few of the activities that increasingly occur online.

Together, we will continue to address cyber workforce demands, build long-term workforce capacity, and position all Americans to benefit from the enormous potential of our interconnected future.

Cyber education and workforce development have not kept pace with demand and the rapid pace of technological change.[1] Moreover, skills in demand in the cyber workforce are evolving.[2] For example, developments in artificial intelligence (AI) and machine learning (ML) may change how workers at all levels of experience perform their jobs.

Every American should have the skills needed to efficiently and confidently use computers and the internet to accomplish a growing list of daily activities. We must also make cyber training and education more broadly available so that even those persons currently underrepresented in the cyber workforce are qualified to pursue well-paying, fulfilling cyber jobs. Many of these jobs do not require four-year degrees and offer pathways to acquire cyber skills in high demand.

The Bipartisan Infrastructure Law[3] and CHIPS and Science Act are providing historic investments in our digital economy—including $65 billion for affordable high-speed internet and support for American semiconductor research, development, and production. These game-changing efforts create substantial opportunities to expand the cyber workforce and put Americans into good jobs that pay well.[4] Together, we will address cyber workforce demands, build long-term workforce capacity, and position all Americans to benefit from the enormous potential of our interconnected future.

THE STRATEGY AT A GLANCE

This strategy is organized into four pillars: (1) Equip Every American with Foundational Cyber Skills, (2) Transform Cyber Education, (3) Expand and Enhance America's Cyber Workforce, and (4) Strengthen the Federal Cyber Workforce (see Figure 1).

The first two pillars focus on developing cyber skills needed in the workforce and society. Efforts related to enhancing the national cyber workforce are discussed in the third pillar, while the final pillar addresses the unique opportunities and challenges of federal employment. Wherever possible, the federal government will lead by example in implementing positive change.

Three guiding imperatives inform objectives throughout this strategy: (1) leverage collaborative workforce development ecosystems to meet cyber workforce demands; (2) enable the lifelong pursuit of cyber skills; and (3) strengthen the cyber workforce through greater diversity and inclusion.

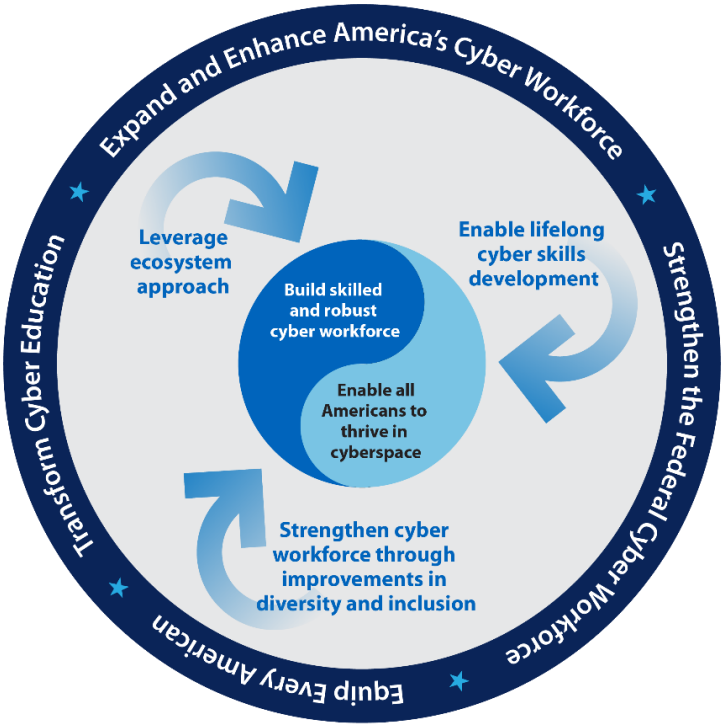

Figure 1. Strategy Overview

MANDATE AND SCOPE

MANDATE

The President's National Cybersecurity Strategy (NCS) states our current strategic landscape presents both tremendous opportunity and significant challenges.[5] This document builds on the NCS by setting forth an approach to cyber education and workforce development. The United States and its partners must navigate this decisive decade to build a defensible, resilient, values-aligned digital environment that furthers security, economic prosperity, and technological innovation.

The NCS calls for two major shifts. First, responsibility for defending cyberspace should be shifted from individuals and small businesses to the most capable actors in cyber space. Accordingly, cybersecurity must be built into education and workforce development programs relevant to sustaining the digital environment. (For the definition of *cybersecurity*, see Appendix A.). The second shift seeks to alter incentives across public and private sectors to favor long-term investments in security. Consistent with this shift, we focus on foundational cyber skills, changes in education, and collaborative cyber education and workforce development ecosystems.

The growing use of cloud computing, AI, ML, virtual reality, quantum computing, and other emerging technologies place ever-changing demands on the cyber workforce. Thus, this strategy

emphasizes robust collaboration between employers, educators, government, and other stakeholders to ensure that cyber workforce needs are met in a decentralized yet strategic fashion.

SCOPE

Many dynamics will shape America's cyber workforce needs, but meeting demand for skilled cyber workers is an urgent concern. One industry study estimated unmet demand for 411,000 cybersecurity workers in 2022, a 9.0% increase from 2021.[6] Another study estimates that employer demand exceeds supply by 32%.[7] From a global perspective, the situation is even more stark. The difference between global demand and cyber workforce capacity in 2022 was estimated at 3.4 million, a 26% increase over the previous year.[8]

Cyber skills are becoming important to a greater number of occupations across all sectors of our economy. For example, one 2023 publication found that 92% of jobs across industries in the United States require at least some digital skills.[9] This demand outstrips supply, as nearly 33% of U.S. workers between ages 16 and 64 lack these skills[10] (see Figure 2). Cyber skills are becoming increasingly essential to U.S. economic competitiveness in the global economy.[11]

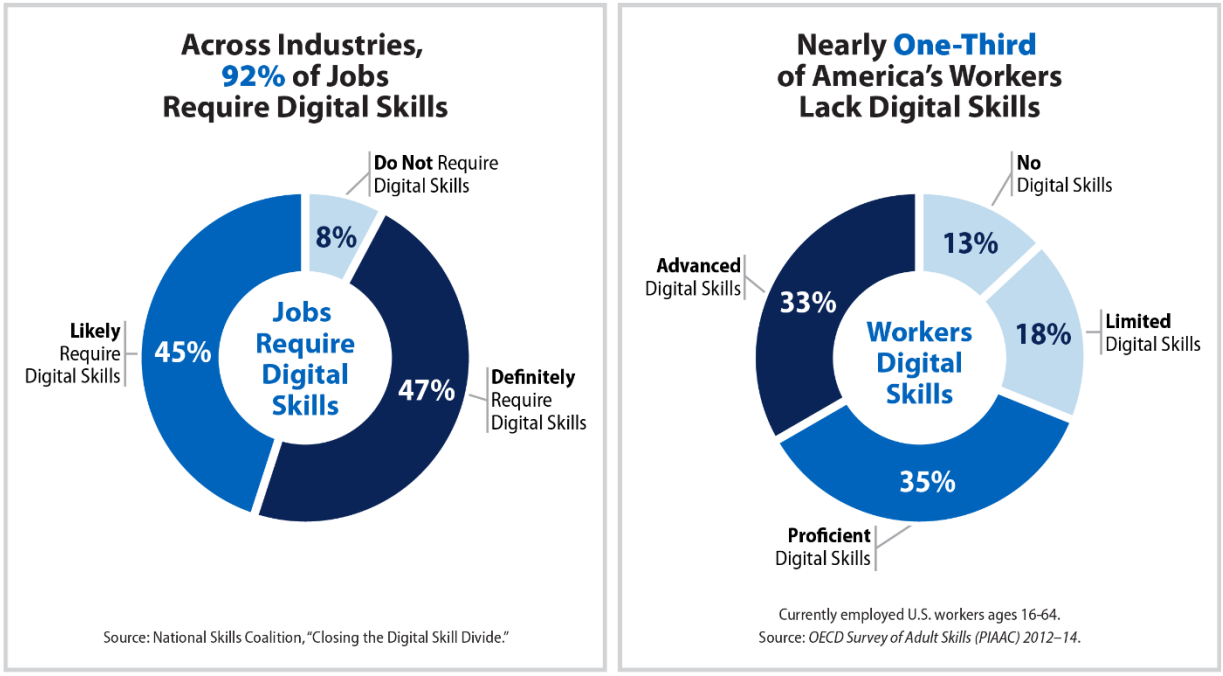

Figure 2. Demand Exceeds Supply

The COVID-19 pandemic accelerated the digital transformation of workplaces.[12] Consequently, limitations predominantly among those with low incomes, in underserved minority and rural communities were uncovered.[13] Cyber skills also became increasingly important to people simply to meet the demands of daily life.[14]

This strategy focuses on the American workforce across all sectors and occupations that requires cyber skills. It sets out a plan to build the foundational cyber skills—digital literacy, computational

literacy, and digital resilience—that prepare today's learners for the workforce and enable full access to the digital resources in our interconnected society.

GUIDING IMPERATIVES

The three imperatives discussed below guide the work that must be done. By focusing on these imperatives, stakeholders in academia and the public and private sectors will advance American prosperity and cybersecurity while better enabling all Americans to embrace cyberspace as a source of opportunity.

LEVERAGE ADAPTABLE ECOSYSTEMS TO EFFECT CHANGE AT SCALE

No individual stakeholder can address the growing cyber workforce demands at scale. Vigorous collaboration among education, labor, and commercial stakeholders is essential to success. Further development of robust cyber education and workforce development ecosystems must prepare workers to thrive in the digital environment.

A model cyber education and workforce development ecosystem[15] should include the following elements:

- Diverse stakeholders;[16]
- Multisector partners;[17]
- Strategies and Long-term plans;[18]
- Career opportunities;[19]
- Continuous assessment;[20]
- Widespread communication;[21] and
- Experiential learning.[22]

The ecosystem approach reflects the Department of Commerce's best practices and principles for highly effective workforce investments, including the provision of wraparound services to vulnerable populations, the prioritization of earn and learn models, and other approaches that create the conditions for economic growth and opportunity for all communities. It also supports the Biden-Harris Administration's emphasis on building quality partnerships, encouraging industry investments in workforce development, and supporting workers' voice. These areas of emphasis will further help reduce barriers, provide pathways into high-demand jobs, and enable ongoing adaptation as technological innovations continue to shape the demand for cyber workforce skills in the future. [23] Ecosystems may operate in varied geographic areas, including locally, within a state, regionally, across the country, or globally.[24]

As cyber education and workforce development ecosystems mature, stakeholders may identify and overcome systemic barriers to positive change. Such barriers could include persistent disadvantages

★ ★ ★ ★ ★ ★

faced by underserved communities, insufficient or unclear incentives for collaboration between key stakeholders, or particular local and state education policies.

Enable the Lifelong Development of Cyber Skills

Every American should have lifelong opportunities to acquire cyber skills, beginning with foundational cyber skills. Today, such skills are what literacy has long been—a source of empowerment in work and life. They help people meet workforce demands and enable full access to the benefits of our interconnected society. With foundational cyber skills — digital literacy, computational literacy, and digital resilience — individuals develop technical skills, the ability to draw on multi-disciplinary perspectives to understand security, ethical, and societal issues, and the ability to adapt with rapid changes in technology. (See Figure 4 and Appendix B.)

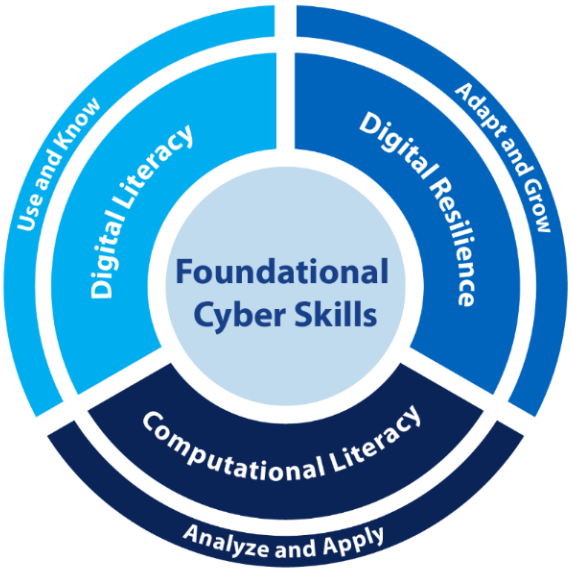

Figure 4. Foundational Cyber Skills

Those who work in industries such as manufacturing, space, health care, retail, finance, utilities, and construction require additional industry-specific or occupation-specific cyber skills. Education and training systems, including those offered by employers, should equip Americans with the skills to work efficiently, effectively, safely, and securely.

For example, participants in the software development process—from business leaders to software developers and product managers—must be equipped to manage the security and privacy implications of the software they create. A model can be found in the Department of Energy's 2022 National Cyber-Informed Engineering Strategy, which recognizes the need to incorporate cybersecurity principles into engineering work from the earliest to the final stages.[25]

Grow and Enhance the Cyber Workforce Through Improvements in Diversity and Inclusion

To advance our collective prosperity, security, and well-being, we must draw on the full diversity of the American talent pool. Improvements in diversity, equity, inclusion, and accessibility in cybersecurity have tremendous potential to strengthen the cyber workforce,[26] including gains in innovation,[27] creative problem solving,[28] improved decision making,[29] and profitability.[30] It can improve recruitment even more broadly, as America's younger generations increasingly expect and value robust DEIA practices in the workplace.[31] One of the most effective ways to grow our supply of cyber talent is to attract people of all ages and all demographics from underrepresented communities, such as women, veterans, military spouses, people of color, first-generation

professionals, individuals with disabilities, LGBTQI+ individuals, Tribal nations, and members of rural and other underserved communities.[32] To create inclusive work environments where effective mentoring is likely to occur, organizations also need to establish diverse representation within senior levels of leadership and management.

The underrepresentation of key demographic groups is most striking when it comes to women, who make up 49% of the nation's workforce but only 26% of those in the cyber workforce.[33] Studies also continue to reveal challenges in inclusion and career progression for women in cyber careers, with negative implications for retention.[34]

Women make up 49% of the nation's workforce and only 26% of the cyber workforce.

Due to lack of granularity in the data available on other portions of the population, tech occupation data is used here instead.[35] Black Americans make up 12% of the workforce but only 8% of those in tech occupations, while Hispanic Americans comprise 16% of the workforce but only 8% of those in tech occupations.[36] There appears to be similar underrepresentation of rural workers in tech occupations.[37] People with disabilities, who are underrepresented in the workforce in general, have untapped potential to enter the cyber workforce.[38] For example, there are initiatives to increase the participation of persons with neurodiversity-related attributes in the cyber workforce.[39] Until we draw more talent from groups underrepresented in the cyber workforce, we will not meet the demand for more cybersecurity-trained capacity.

A Foundation for Progress

Earlier efforts to strengthen our cyber workforce inform and provide a starting point for the development of this strategy. Key milestones include the creation of the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program in 1998, the start of the Cyber Corps Scholarship for Service (SFS) program in 2000, the Comprehensive National Cybersecurity Initiative in 2008, and the creation of NICE[40] in 2010, followed by three NICE Strategic Plans, with the most recent published in 2021.[41] This strategy relies on the NICE Workforce Framework for Cybersecurity (NICE Framework) which enables entities across the public and private sectors to use a common lexicon to describe work done by those who need specific knowledge and skills to perform cybersecurity-related tasks and manage risks to the enterprise.[42] In addition, the Department of Defense (DoD) leveraged the NICE Framework to create the DoD Cyber Workforce Framework to meets its needs.[43]

Legislative achievements and policy precedents also provide a strong foundation for progress. Important laws include the Cybersecurity Enhancement Act of 2014 and the Federal Cybersecurity Workforce Assessment Act of 2015. Policy foundations include: the "Federal Cybersecurity Workforce Strategy" in 2016; Executive Order (EO) 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," in 2017 and its mandated report to the President,

"Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce," in 2018; EO 13870, "America's Cybersecurity Workforce," in 2019; EO 13932, "Modernizing and Reforming the Assessment and Hiring of Federal Job Candidates," in 2020; EO 13985, "Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government," January 20, 2021; and EO 14091, "Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government." This strategy is also integrated with the President's Management Agenda and builds on National Security Memorandum (NSM) 3, "Revitalizing America's Foreign Policy and National Security Workforce, Institutions, and Partnerships."

Industry, educational institutions, training providers, non-profit organizations, philanthropies, and government have made progress. In some cases, these entities formed collaborative ecosystems that are models for other states or regions.

Guiding the Way Ahead

Extensive collaboration between stakeholders across academia and the public and private sectors will be supported by multiple departments and agencies at the federal level, as well as public–private partnerships.

A Coherent Federal Approach

In December 2022, the National Cyber Director established the National Cyber Workforce Coordination Group (NCWCG).[44] This body serves as the principal interagency forum for departments and agencies to address the challenges and opportunities associated with cyber education, training, and workforce development. The NCWCG coordinates efforts across the interagency. The Office of the National Cyber Director (ONCD) will work through the NCWCG to implement this strategy by defining roles and responsibilities and establishing metrics and timelines.

A Whole-of-Nation Call to Action

Sustained collaboration between federal entities is critical but not sufficient. Stakeholders across academia and the public and private sectors have central roles to play. Every entity involved in cyber workforce development should see themselves in this strategy and feel called upon to advance implementation.

PILLAR ONE | EQUIP EVERY AMERICAN WITH FOUNDATIONAL CYBER SKILLS

America's economic competitiveness and security improve when workers have the cyber skills needed to meet workforce demands. Equipped with these skills, Americans will be positioned to find and keep good jobs that support families and strengthen communities.

Foundational cyber skills must become universal like reading and math. We must expand programs offering foundational cyber skills, and design learning opportunities to support education systems that are accessible and effective.

Foundational cyber skills consist of three components (see also Figure 5 and Appendix B):

- **Digital literacy**: The cognitive and technical skills needed to use information and technologies to find, evaluate, create, and communicate information.[45]
- **Computational literacy**: The ability to consume information and use applications and systems to: analyze data, draw conclusions, and solve problems; safely, ethically, and securely interact in networked environments; and understand how computing, data, and connectivity affects society.[46]
- **Digital resilience**: The awareness, skills, agility, and confidence to be empowered users of new technologies and adapt to changing digital skill demands.[47]

Key stakeholders from across academia and the public and private sectors have important roles to play in enabling Americans to develop foundational cyber skills. This collaboration will need to be active, dynamic and forward-looking.

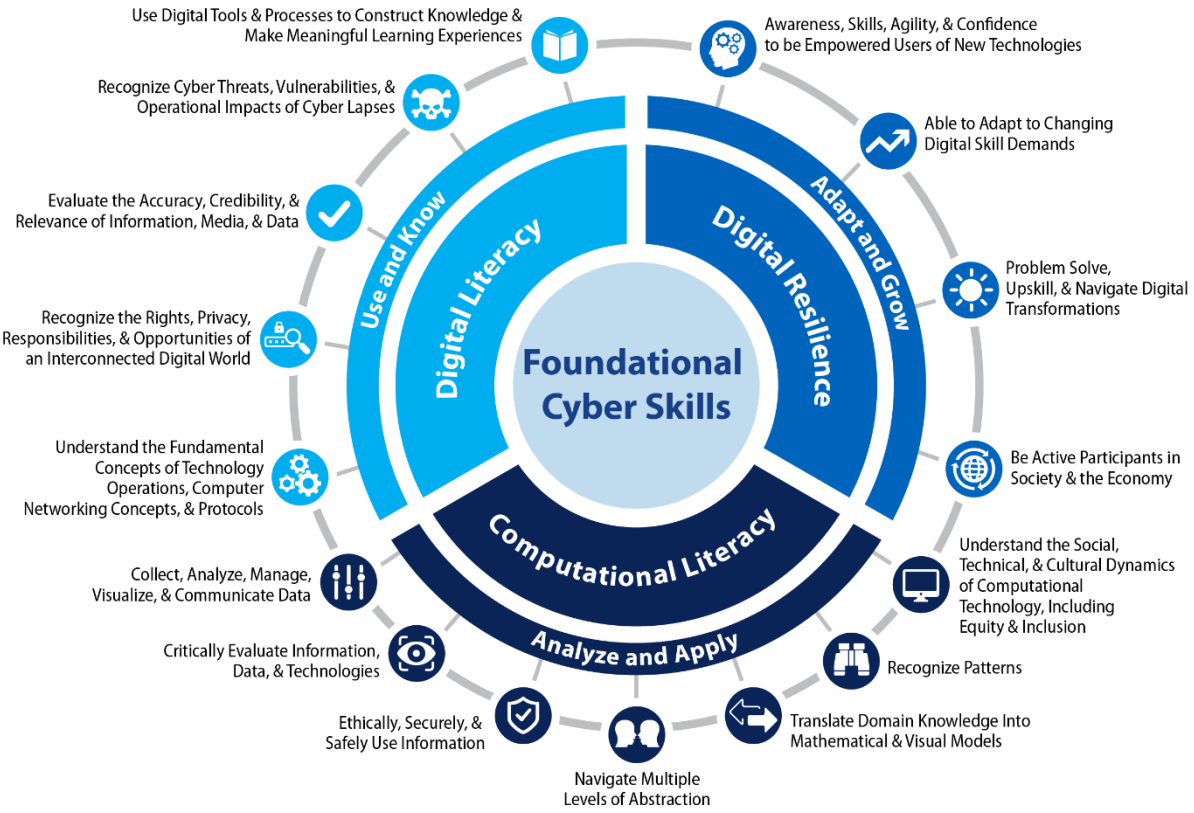

Figure 5. Foundational Cyber Skills (see also Appendix B)

Collaboration within ecosystems will broaden the opportunities to acquire foundational cyber skills while providing on-ramps to more job opportunities.

STRATEGIC OBJECTIVE 1.1: MAKE FOUNDATIONAL CYBER SKILL LEARNING OPPORTUNITIES AVAILABLE TO ALL

To equip every American with foundational cyber skills, high-quality learning opportunities must be available to everyone. Ecosystem stakeholders across academia and the public and private sectors are best suited to determine the most effective ways to provide learning opportunities within their communities. Every learner interested in acquiring foundational cyber skills should be able to access formal and informal learning opportunities, including in no-cost or low-cost online environments. Increasing the availability of data that can be used to align the demand for foundational cyber skills with the supply of programs and learning opportunities will assist stakeholders in prioritizing their investments.

★ ★ ★ ★ ★ ★

Lines of Effort

1.1.1 Enhance foundational cyber skills learning opportunities through Federal investments.

The NCWCG will coordinate with the National Science and Technology Council's Committee on STEM, led by the Office of Science and Technology Policy, and departments and agencies to maximize federal investments in foundational cyber skills and foster alignment to existing standards and frameworks. Areas of focus include existing programs and initiatives, grant opportunities, and technical assistance. The NCWCG will coordinate the dissemination of criteria for department and agency solicitations to improve consistency across funding opportunities. Departments and agencies will explore publicly sharing models and resources for teaching foundational cyber skills that are produced through grants and contracts.

ONCD and the NCWCG will work with departments and agencies to include, where appropriate and legally permissible, requirements for digital inclusion plans in federal grants to minimize barriers that could inhibit participation in the learning opportunities funded by the grant. Digital inclusion plans will take into account the needs and perspectives of local communities, including those that are underrepresented and underserved.[48]

1.1.2 Foster ecosystem approaches to enhance foundational cyber skill learning opportunities.

Industry experts, educators, colleges and universities, community organizations, and relevant professional societies are encouraged to create content for use in teaching foundational cyber skills. This content should be made publicly available to ecosystem stakeholders, including state, local, Tribal, and territorial (SLTT) governments, education agencies, academia, libraries, community-based organizations, and businesses. Potential models include Digital US,[49] a coalition that includes employers, service providers, and philanthropists, and the Future Workforce Now initiative,[50] led by the National Governors Association, which seeks to close technological and digital literacy gaps.

1.1.3 Encourage the development of an open knowledge network for foundational cyber skills.

SLTT governments, industry, and non-profit organizations are encouraged to partner in the development of a non-proprietary, web-based open knowledge network (OKN) containing resources on foundational cyber skills.[51] A comprehensive and public effort to develop a nationwide OKN would enable the costs to be distributed while building a large stakeholder base.

Departments and agencies will explore opportunities to support the development of an OKN through existing programs, and make available learning resources produced through federal investments.

★ ★ ★ ★ ★ ★

1.1.4 Use data and tools to guide investments in foundational cyber skills learning opportunities.

SLTT governments are encouraged to use existing datasets and resources to assess their digital environments and help guide investments. For example, several states have developed maps to assist citizens in finding locations to obtain low-cost or free foundational cyber skills classes or tutoring.[52] In addition to serving individuals, these maps help employers find training providers to upskill or reskill their employees. For example, the State Digital Equity Scorecard provides a numerical score for each state based on six indicators.[53] The data provided by such scorecards should inform the targeted development of programs.

1.1.5 Include foundational cyber skills in existing educational frameworks, programs, and activities.

Academia, libraries, trade associations, and non-profit organizations, with support from federal and SLTT governments and education agencies, are encouraged to integrate foundational cyber skills into existing education programs (see also Appendix B). Standards vary widely, which causes confusion among stakeholders. Efforts to advance foundational cyber skills should be connected to the NICE Framework where possible.

STRATEGIC OBJECTIVE 1.2: INVIGORATE THE PURSUIT OF FOUNDATIONAL CYBER SKILLS AND CYBER CAREERS

We must inspire Americans to understand how acquisition of foundational cyber skills serves themselves and society. While some may gain the foundational cyber skills needed to navigate daily life, others may be inspired to go further and make cybersecurity their focus.

Lines of Effort

1.2.1 Promote the economic and societal benefits of foundational cyber skills.

Public and private sector entities, including non-profit and community organizations, are encouraged to enrich the narrative around foundational cyber skills, highlighting their importance to the economy and societal welfare. The NCWCG will coordinate efforts across the government to more accurately depict and promote cyber careers and skills in public communications.

1.2.2 Encourage foundational cyber skills as a corporate social responsibility.

Private sector actors are encouraged to promote foundational cyber skills in corporate social responsibility portfolios. Investments in foundational cyber skills will expand future candidate pools and help inform consumers about corporate security and privacy practices.

★ ★ ★ ★ ★ ★

1.2.3 Leverage national outreach and awareness initiatives to encourage the development of foundational cyber skills and the pursuit of cyber careers.

Ecosystem stakeholders are encouraged to develop or expand campaigns, such as Cybersecurity Awareness Month, Cybersecurity Career Week, Supply Chain Integrity Month, Digital Citizenship Week, Internet Safety Week, and Media Literacy Week, which are focused on cyber workforce development and increasing awareness of how cyber skills advance individual and societal interests.

The NCWCG will coordinate commemorative activities, such as Engineering Week, Quantum Day, STEM Week, Computer Science Week, World Space Week, and Mathematics and Statistics Month, to amplify the need for cyber skills while expanding awareness of pathways to a wide array of potential careers. Departments and agencies will use outreach efforts such as ambassador and mentoring programs, speaker events, take your child to work days, and open houses to increase awareness of the value of cyber skills across different careers.

1.2.4 Establish a presidential award for foundational cyber skills.

ONCD will work with departments and agencies, community service organizations and industry partners to explore the development of a Presidential Cyber Award, similar to the Presidential Youth Fitness Award,[54] to recognize students for foundational cyber skills.

STRATEGIC OBJECTIVE 1.3: FOSTER GLOBAL PROGRESS IN FOUNDATIONAL CYBER SKILLS

Democracy around the world depends on the free flow of ideas, informed public discourse, and trust in institutions. Increased interconnectedness may foster these elements of democracy, but it can also be used to spread disinformation, plant mistrust, and undermine and repress fundamental rights and freedoms. International cooperation plays a vital role in preserving our national security and promoting democratic values. International engagements to strengthen connectivity and foundational cyber skills advance our prosperity, our security, and our values.

In the Declaration of the Future of the Internet of April 2022, the United States and more than 60 international partners expressed a shared commitment to an internet that: is "open, free, global, interoperable, reliable, and secure;" that furthers democratic values; and promotes shared prosperity.[55] In support of this common vision, the United States will exchange best practices with partners and allies. The United States promotes global digital connectivity and will also include foundational cyber skills in U.S. capacity building abroad. American values, interests, and security are strengthened when best practices and frameworks are developed with active participation.

★ ★ ★ ★ ★ ★

Lines of Effort

1.3.1 Exchange best practices in improving foundational cyber skills with international partners and allies.

The Department of State, with support from other departments and agencies, will exchange best practices in promoting foundational cyber skills among international partners and allies. These exchanges should include best practices to avoid manipulation by online campaigns of misinformation and disinformation that can threaten democratic cohesion.[56]

1.3.2 Include foundational cyber skills development and awareness in international capacity-building programs.

The Department of State and the United States Agency for International Development (USAID), with support from federal, private sector, and international partners will include foundational cyber skills development in international partner capacity-building programs.[57]

1.3.3 Promote the development of international standards and frameworks relating to foundational cyber skills.

The National Institute of Standards and Technology (NIST), with support from ONCD as well as relevant civil society organizations will actively participate in international convenings to develop standards and frameworks related to the development of foundational cyber skills.

PILLAR TWO | TRANSFORM CYBER EDUCATION

Cyber education in the United States must address the immediate demand for a skilled cyber workforce while also preparing learners to meet the future needs of a dynamic technological environment. Connections between cyber education systems, training providers, and employers must be improved so people have reliable, clear pathways into fulfilling jobs.

The work of transforming cyber education cannot rest solely on the shoulders of educators. Local ecosystems that leverage the active participation and commitment of education and training providers, employers, government, and other stakeholders show promising results. Expanding access to populations underrepresented in cyber careers is also critical to success. We must encourage appropriate investments by an array of stakeholders to ensure that effective cyber education and workforce development ecosystems receive the resources and support required to be sustainable and replicable.

The work of transforming cyber education cannot rest solely on the shoulders of educators.

The future of cyber education includes theoretical and applied learning skills needed to succeed in cyber careers. Cyber education and training opportunities should be aligned with the cognitive and technical capacities of an individual over the course of a lifetime. Consistent with a competency-based instructional approach, learners of any age and background should be able to acquire skills through individualized experiences that align with their capabilities and interests, with additional attention given to neurodiversity. Cyber education should be integrated across disciplines so learners can gain the requisite knowledge and skills in relevant and contextualized learning experiences.

With support from an ecosystem of engaged partners, cyber education can help produce a future digital environment that is secure by design. Those who create the software that shapes the contours of cyberspace, as well as those who design and build the OT and ICS essential to the operation of critical infrastructure, should have a strong understanding of cybersecurity.

STRATEGIC OBJECTIVE 2.1: BUILD AND LEVERAGE ECOSYSTEMS TO IMPROVE CYBER EDUCATION

Education systems will better meet workforce demands when ecosystem partners contribute their knowledge and resources to improve cyber education programs. Ecosystem stakeholders should consider the best partners to engage, including, but not limited to, economic development agencies, workforce development systems, employment and education intermediaries, industry

representatives, and education agencies. For example, a local hospital system may collaborate with municipal governments and postsecondary educational institutions to develop curricula and mentor students.

Ecosystem projects may leverage funding from government at various levels. Examples of federal investments include Regional Innovation Engines[58] and Secure and Trustworthy Cyberspace,[59] both led by the National Science Foundation (NSF), Regional Technology and Innovation Hubs funded by the Economic Development Administration in the Department of Commerce,[60] NICE Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education, Training, and Workforce Development funded by NIST,[61] and the Career and Technical Education (CTE) CyberNet program funded by the Department of Education and the National Security Agency (NSA).[62]

Lines of Effort

2.1.1 Expand and support cyber education ecosystems.

The Biden-Harris Administration will work with Congress to promote successful ecosystem models in every state by funding cyber education ecosystems through programs such as the NSF Regional Innovation Engines, NICE RAMPS, and CTE CyberNet.

ONCD will identify and highlight examples of successful cyber education and workforce development ecosystems across the United States, especially models that exhibit best practices in the areas of sustainability, adaptation, and replicability. This effort will foster the nationwide sharing of effective strategies and best practices.

2.1.2 Increase engagement in cyber education ecosystems.

Employers, industry groups, labor organizations, service organizations, and chambers of commerce are encouraged to participate actively in the development and delivery of cyber education and training programs. Stakeholders should engage in formal education systems, such as K-12 schools, community colleges, and institutions offering four-year and advanced degree programs. They should also engage in informal programs such as summer camps, hackathons, boot camps, and online learning content. Programs should increase awareness of cyber skills in demand in the workforce and be accessible to community partners, including learners, families, counselors, and mentors.

The NCWCG will explore how the federal government can provide incentives to employers to engage actively in ecosystems and highlight examples of success. SLTT governments are encouraged to do the same.

Education and Workforce Development Ecosystems in Action

The **Carolina Cyber Network**, founded with the support of the state of North Carolina in 2020, serves students looking to advance their cyber knowledge and training, educators looking for collaborative resources, and employers looking to build their cyber workforce. https://carolinacybernetwork.net

The **Commonwealth Cyber Initiative**, established by the Virginia General Assembly in 2018 with roots in an earlier 2016 NICE RAMPS grant, is a network of industry, higher education, and economic development partners across Virginia. https://cyberinitiative.org

Cybersecurity San Antonio is a partnership between San Antonio, Bexar County, and area employers led by the San Antonio Chamber of Commerce. Members include industry, public school districts, higher education, workforce development organizations, non-profits, state and local government, and federal and military partners. https://cybersecuritysa.org

The **Georgia Cyber Center** is a collaboration between academia; federal, state, and local government; law enforcement; the U.S. Army; and the private sector. Its collaborative mission is to meet the growing need for cyber talent in Georgia. https://gacybercenter.org

The **CAE Regional Midwest Hub**, led by Moraine Valley Community College connects state education agencies, employers, and educational institutions in the Midwest to discuss workforce needs, trends, data, and cybersecurity education resources. The project is funded by a grant from NSA. https://cssia.org/caeregionalhubs

The **Ohio Cyber Range Institute**, a partnership involving the state government and the University of Cincinnati, has three missions: education, workforce, and economic development. Twenty two 22 Ohio institutions currently participate in this partnership, which has roots in a 2016 NICE RAMPS grant. https://ohiocyberrangeinstitute.org

The **Cyber Center of Excellence** in San Diego, CA, brings together companies, academic institutions, military organizations, local governments, critical infrastructure operators, service providers, and non-profits to address infrastructure challenges, improve cybersecurity in the region, and promote cyber workforce development. https://sdccoe.org

The Idaho Cyber Research Project, formed by Idaho National Lab, helps Idaho's employers, colleges and universities, and potential employees understand the knowledge, skills, and abilities that industrial cybersecurity roles require. This informs training and apprenticeship opportunities. https://inl.gov/idaho-cyber

CyberHawaii, founded as an affiliate of CyberUSA in 2016, is dedicated to accelerating pathways from high school through two- and four-year institutions into the cyber workforce. It has members from across academia and the public and private sectors. Its activities include meetings, workshops, webinars, cyber exercises, and an annual conference. https://www.cyberhawaii.org

Cyber Florida, funded by the state of Florida since 2014, is hosted by the University of South Florida and involves all State University System of Florida institutions as well as public and private sector partners. Its main missions include education to increase the number of cybersecurity professionals, research, and outreach. https://cyberflorida.org

★ ★ ★ ★ ★ ★

2.1.3 Integrate cybersecurity across disciplines to prepare the cyber workforce to build systems that are secure by design.

Federal departments and agencies will review selection criteria for grants, expand outreach, and collaborate with academic programs, where legally permissible and appropriate, to ensure that cybersecurity, including but not limited to secure-by-design theories and practices, is an integral part of relevant federal funding opportunities.

The NCWCG will explore ways to encourage ecosystem stakeholders to integrate cybersecurity – including security by design, threat modeling, memory safe languages, privacy, standards, ethics, and other elements of cybersecurity – into computer science, software engineering, operational technology, and related college courses, as well as K-12 education, boot camps, employer-led training, and other forms of cyber education.

2.1.4 Protect learners in safe and secure cyber learning environments.

Federal departments and agencies will review requirements in relevant grants and contracts, where legally permissible and appropriate, to ensure that safety and privacy protocols are used in the programs, systems, and social media platforms accessed by learners.

Ecosystem stakeholders are encouraged to explore ways to ensure that the systems used in K-12 education protect learners from harmful content and harassment. For example, technology companies can proactively pursue industry standards and actions to advance safe and secure learning environments.

Strategic Objective 2.2: Expand Competency-Based Cyber Education

Education and training ecosystems should expand the availability of competency-based cyber education opportunities that accelerate knowledge acquisition and allow learners to demonstrate mastery at their own pace.[63] Learners of every age get introduced to complex cyber concepts through a variety of channels in both theoretical and applied methods (see also Pillar One). Cyber skills acquisition is a lifelong endeavor. Learners will build on foundational cyber skills as they gain occupation-specific and industry-specific cyber skills. This Strategic Objective supports the general progression of learning from early childhood to seasoned professional.

Cyber skills acquisition is a lifelong endeavor. Learners will build on foundational cyber skills as they gain occupation-specific and industry-specific cyber skills.

The phases of cyber-related learning described in this section do not rigidly define when cyber content should be learned. Alternative models may be appropriate depending on individual cognitive capabilities, physical abilities,

and method of intervention. Security concepts that increase the understanding of threats, and benefits of cyber secure practices should be included at every practical learning opportunity.

Lines of Effort

2.2.1 Focus federal cyber education investments on developing learning resources aligned with stages of cognitive development.

Federal departments and agencies will, where permissible and appropriate, leverage grants and Small Business Innovation Research programs to fund research that evaluates effective learning practices and the development of cyber learning resources aligned with stages of cognitive development. They will also use competitive priorities and selection criteria in education grants to require access to high-quality cyber education and training, where legally permissible and appropriate.

2.2.2 Enhance applied cyber content in interdisciplinary education programs.

SLTT education agencies are encouraged to promote interdisciplinary programs, from K-12 to postsecondary education, that equip learners with the cyber skills needed to succeed in their chosen career pathways.

Colleges and universities are encouraged to incorporate more applied technical skills in certificate and degree programs, including the attainment of industry-recognized certifications. Innovative models, such as cybersecurity clinics and school-based enterprises, give students work experience while providing services to businesses and organizations in the community.[64]

Federal departments and agencies will explore incentives to encourage colleges and universities to offer industry-recognized certifications, and encourage private providers to make certifications more affordable.

2.2.3 Increase the availability of curricula for cyber education programs.

The NICE program office, the Cybersecurity and Infrastructure Security Agency (CISA), NSA, DoD, NSF, and other federal departments and agencies will collaborate to develop teaching resources that reduce costs of cyber education. Where possible, resources will be made available to SLTT education agencies, such as the Regions Investing in the Next Generation (RING) resources funded by NSA,[65] CISA's Cybersecurity Education and Training Assistance Program,[66] and the Advanced Technological Education (ATE) National Resource Centers funded by NSF.[67] Employers are encouraged to contribute to the development of cyber curricula for education systems to reduce the cost to educators.

Cyber-Related Learning Phases

Cyber Device Interaction and Career Awareness

As children are developing basic motor skills, the introduction of technology and safety concepts can be delivered with or without electronic devices. Skill development requires understanding cause and effect through interactions with technological devices and provides an opportunity for educators to introduce the risks in an age-appropriate manner. Grammar school is a prime opportunity to illuminate foundational cyber skills across professions.

Cyber Career Exploration

Project-based learning with cyber components can help middle schoolers explore career aspirations. Ecosystem stakeholders should provide learners access to career exploration activities while bolstering technical and employability skills that improve understanding of workplace expectations.

Cyber Career Preparation

As learners prepare to enter the workforce education programs that serve teens should increase the availability of applied and interdisciplinary approaches to provide hands-on learning opportunities. Interdisciplinary approaches to cyber education have the added benefit of attracting underserved and underrepresented populations to cyber careers.

State and local education agencies should ensure students are prepared for both college *and* careers when they graduate from high school or achieve high school equivalency. Approaches such as early college models, career academies, Junior Reserve Officers' Training Corps (JROTC), career and technical education programs of study, and paid work learning opportunities that include sector-relevant cyber skills development should be available to all learners.

Cyber Skill Training

Education and training programs become more differentiated in design and specialized in content as learners enter the workforce and further their education. Institutions are adapting to accommodate the demands of learners and labor markets with project-based and work-based applied learning approaches incorporated in greater numbers of academic programs. Integrated education and training (IET) programs and the introduction of applied learning and skill development in four-year academic programs are emerging best practices, which leverage the strengths of both education and training within a single program.

★ ★ ★ ★ ★ ★

2.2.4 Increase concurrent and transferrable credit opportunities.

Consistent with the "Raise the Bar: Unlocking Career Success Initiative" led by the Department of Education in partnership with the Departments of Commerce and Labor,[68] SLTT education agencies are encouraged to enable high school students to earn college credits for cyber coursework that are transferrable to a broad range of postsecondary institutions, as well as concurrent high school and college credit and stackable industry-recognized cyber credentials. NSA will work with NCAE-C institutions to develop a model credit transfer agreement. Other departments and agencies will explore the use of federal formula and discretionary grant programs to expand the availability of cyber credit transfer agreements.

2.2.5 Expand innovative models for academic credit.

ONCD will collaborate with departments and agencies to explore incentives for SLTT education agencies to establish programs and processes that allow students to earn transcript credit for validated cyber learning experiences outside of school systems. These experiences might also be captured as part of a learning and employment record (LER). Education agencies are encouraged to develop and expand access to innovative cyber learning opportunities that enable learners to earn credit toward graduation requirements.

Education ecosystem stakeholders are encouraged to enable students to earn academic credit, including fractional credits, through experiential learning or validated content that can be assigned credit on transcripts and credentials. Activities such as cyber competitions, games, clubs, career and technical student organizations, and paid work learning are a few examples of complementary learning experiences.

STRATEGIC OBJECTIVE 2.3: INVEST IN EDUCATORS AND IMPROVE CYBER EDUCATION SYSTEMS

Cyber education and workforce development ecosystems should be responsive, resilient, sustainable, and flexible enough to accommodate emerging innovations and sociopolitical dynamics. To support more efficient knowledge acquisition and enable employers to improve skills-based hiring approaches, ecosystems should emphasize individualized and competency-based learning. Current education systems are in need of educators to teach the next generation of cyber professionals.

All ecosystem stakeholders are encouraged to improve response to labor market needs and make long-term investments necessary to increase our cyber education capacity. This will require reskilling and upskilling educators, and providing support in the form of supplies, equipment, training, funding, and staff. SLTT education agencies and ecosystem partners are encouraged to improve cyber teaching environments, recognize successful programs, and build community support for cyber educators. We encourage collaboration between cyber educators to exchange ideas and resources through communities of practice.

★ ★ ★ ★ ★ ★

Lines of Effort

2.3.1 Increase the cyber teaching capacity of K-12 systems and postsecondary institutions.

Colleges and universities are encouraged to collaborate with SLTT education agencies to develop innovative programs, including with support from industry experts, to increase the number of educators who teach cyber skills in K-12 systems, DoD Education Activity schools, and postsecondary institutions.

Federal departments and agencies will explore the use of grants and contracts to increase the pool of experts available to teach cyber.

The NCWCG will explore opportunities to share best practices for expanding cyber learning opportunities, such as career academies, JROTC, pre-apprenticeships, the GenCyber program funded by NSA and NSF,[69] school-based enterprises, and work-based learning opportunities.

SLTT education agencies are encouraged to support policies that give educators flexibility to teach cyber in both secondary and postsecondary institutions and reduce barriers resulting from credentialing requirements. They should also consider how course coding and curricula can enable the integration of cyber content and credentials across K-12 institutions and school districts.

Federal departments and agencies will explore grants, credentials and other mechanisms to enhance the cyber content of programs across disciplines in postsecondary institutions.

2.3.2 Establish a national cyber educator fellowship program.

The NCWCG will work with federal departments and agencies to leverage public–private partnerships to develop a paid fellowship program for educators in the cyber workforce. Educators need cyber work experience that they can bring back to their communities and classrooms. Community and philanthropic organizations are encouraged to complement federal efforts with their own fellowship programs, in both public and private sector organizations.

2.3.3 Increase enrollment in advanced degree programs to strengthen research and development in cyber.

The NCWCG will explore mechanisms, including grant and scholarship programs, to grow the number of cyber learners in advanced degree programs which will drive cyber innovation and support implementation of security by design principles.

NSF, through the Secure and Trustworthy Cyberspace (SaTC) program,[70] will support advanced degree programs to strengthen research and development in cyber fields.

The NCWCG will work to support cyber research and development by increasing the number of graduates with advanced degrees in cyber. It will examine obstacles to and prospects for cultivating a workforce equipped with both technical expertise and transferable professional skills. The NCWCG

★ ★ ★ ★ ★ ★

will also explore potential financial models that enable post-secondary institutions to broaden access to advanced cyber degree programs for underrepresented populations and increase graduation rates.

2.3.4 Increase participation in advanced degree programs to expand the cyber faculty pipeline.

The NCWCG will work with departments and agencies, SLTT governments, and colleges and universities to assess the cyber faculty pipeline in postsecondary institutions. It will prioritize grant funding and other investments to support faculty experienced in cyber curricula integration and other effective cyber pedagogical strategies.

NSF will continue working to strengthen the cyber faculty pipeline by supporting funding for the CyberCorps Scholarship For Services[71] and SaTC programs.

2.3.5 Encourage interdisciplinary approaches to teaching cyber.

Federal departments and agencies will explore investing in the expansion of applied interdisciplinary cyber learning approaches in high schools and postsecondary institutions, including programs such as teacher academies, that increase the capacity of educators to teach cyber skills across disciplines. Ecosystem stakeholders are encouraged to support paid training opportunities for teachers, connect cyber educators with peers, and elevate cyber teaching as a profession.

2.3.6 Incorporate cyber education and training into career pathway initiatives.

The Career Pathway Interagency Working Group led by the Departments of Commerce, Education, and Labor will explore opportunities to better position cyber in career pathways and foster the use of common terminology across all stakeholders.

The NCWCG will explore ways to expand the use of LERs to publicize achievements, credentials, and skills among learners, employers, and education and training providers. Possible models include the T3 Innovation Network, Credential Engine, and the Open Skills Network.[72]

To facilitate learners' transition from education institution into the cyber workforce, departments and agencies will explore supporting expansion of programs that target adults seeking to pursue cyber careers.

2.3.7 Expand opportunities to earn credits for experiential learning in cyber.

Departments and agencies will include, where appropriate and permissible, selection criteria and terms in grants and contracts that incentivize recipients to award academic credit toward graduation for experiential cyber learning. Ecosystem stakeholders are encouraged to develop extensible systems for validating, accepting, and articulating credits between post-secondary institutions.

★ ★ ★ ★ ★ ★

2.3.8 Establish and support national cyber award programs for schools and teachers.

The Department of Education, in coordination with ONCD, will explore the development of a Cyber Schools Initiative (similar to the Green Ribbon Schools Initiative) to recognize cyber best practices used in schools, districts, postsecondary institutions, and early learning centers.[73] ONCD will seek opportunities to elevate the visibility and stature of the Presidential Cybersecurity Education Award.[74]

STRATEGIC OBJECTIVE 2.4: MAKE CYBER EDUCATION AND TRAINING MORE AFFORDABLE AND ACCESSIBLE

Cyber education and training should be equitable, inclusive, and accessible to all learners.

Cyber education and training providers are encouraged to take deliberate and decisive actions to make cyber training available to all Americans, and in doing so, address barriers that may inhibit the advancement of underrepresented and underserved communities. Historically Black Colleges and Universities (HBCUs), Tribal Colleges and Universities (TCUs), and Minority Serving Institutions (MSIs) such as Hispanic–Serving Institutions (HSIs), are well positioned to produce qualified graduates to meet the increasing cyber workforce demand. Post-secondary institutions are encouraged to create learning environments that include access to services that give all students the opportunity to pursue successful cyber careers.

Lines of Effort

2.4.1 Enhance the cyber workforce talent pipeline in underrepresented communities.

The NCWCG will work with departments and agencies to coordinate federal cyber education programs that serve populations underrepresented in the cyber workforce. The NCWCG will lead an effort to provide a continuum of opportunities, from foundational cyber skills acquisition to the development of specialized cyber skills needed to advance in cyber career pathways. Departments and agencies are encouraged to invest in programs that expand access through wraparound support services such as transportation, child care, and stipends.

Industry, service organizations, and philanthropists are encouraged to invest in the cyber workforce talent pipeline through programs that serve underrepresented populations.

2.4.2 Increase access to learning opportunities and culturally connected cyber content.

Education institutions are encouraged to increase co-curricular and extracurricular cyber skill development programs such as cyber competitions and e-sports clubs that attract learners from all backgrounds. Post-secondary institutions, community organizations, and other groups are

encouraged to enable the broadest possible participation in these programs by providing support services.

The NCWCG will coordinate an effort with government, academic, and private sector partners to encourage the development of culturally connected, in-language education content. This should include exploring the role of community, faith-based, and service organizations in the development of this content.

2.4.3 Increase the participation of students and teachers in cyber scholarship programs.

The NCWCG will coordinate efforts across departments and agencies to leverage scholarships and other programs to reduce the financial burden on cyber learners. Departments and agencies will explore providing incentives in grants for colleges and universities to include scholarships and wraparound services in cyber education programs. The CyberCorps Scholarship For Service will continue to support undergraduate and graduate students pursuing teaching and other careers in cybersecurity. Non-profit and philanthropic organizations are encouraged to increase the availability of scholarships that support participation in cyber education and training programs by communities underrepresented in the cyber workforce.

2.4.4 Incorporate cyber instruction into public programs that serve local communities.

Governments are encouraged to leverage services provided through public programs at libraries, museums, faith-based, Tribal, and community organizations, military installations, and federal extension programs to improve access to cyber education for those underrepresented in the cyber workforce.

PILLAR THREE | EXPAND AND ENHANCE AMERICA'S CYBER WORKFORCE

Growing and enhancing the cyber workforce requires collaboration. Ecosystem stakeholders are encouraged to coalesce around common frameworks to develop cyber skills that can adapt to evolving demands in our dynamic technological environment. This includes adopting a skills-based approach, rather than relying solely on college degrees, job experience, and industry-recognized certifications as definitive indicators of qualification.

To support workforce development in the private sector, ecosystem stakeholders are encouraged to utilize the NICE Framework, which establishes a common lexicon for cybersecurity work roles and the knowledge and skills needed for those roles. The websites hosted by NIST, CISA,[75] the Department of Labor,[76] and other agencies are also good resources. The federal government actively participates in ecosystems through workforce development investments, including those led by the Departments of Commerce, Education, and Labor. These investments are supported by legislation, including the Workforce Innovation and Opportunity Act, Carl D. Perkins Career and Technical Education Act, Higher Education Act, and more recently, the Good Jobs Challenge, CHIPS and Science Act, American Rescue Plan, and Bipartisan Infrastructure Law. The federal government must build on these investments by providing incentives for collaboration in ecosystems, promoting best practices, and highlighting effective examples.

Efforts to strengthen the cyber workforce must encompass all Americans, and address barriers that have prevented underserved and underrepresented populations from joining the cyber workforce. A dynamic cyber workforce that draws on all Americans will lead to innovation and long-term economic and technological competitiveness.

We must strengthen our efforts to grow the cyber workforce through exchanges of best practices with international partners and allies. Given the borderless nature of cyberspace, we must also include cyber workforce development in U.S. capacity-building efforts around the world.

STRATEGIC OBJECTIVE 3.1: GROW THE CYBER WORKFORCE BY PROLIFERATING AND STRENGTHENING ECOSYSTEMS

Effective, sustainable ecosystems require incubation, cultivation, investment, information sharing, and above all the collaboration of all stakeholders in the pursuit of common goals. They draw on the

capabilities and strengths of all participants to produce results greater than any could have achieved separately.

Cyber education and workforce development ecosystems need access to better data. Currently, state or federal longitudinal data do not completely describe the national cyber workforce in ways that enable workforce development, economic development, and education agencies to track the demand for cyber skills and labor market trends.

Access to low or no-cost workforce development tools would empower ecosystems. Departments and agencies have made significant strides in developing free online tools to assist employers in understanding and meeting their cyber skill needs. Examples include the Workforce GPS from the Department of Labor,[77] the National Training Catalog from CISA,[78] the CyberSeek Education and Training Provider listing,[79] and free and low-cost online cybersecurity learning content from NICE.[80] Industry, non-profit groups, and education institutions have also made important contributions. Increasing access to these vital tools would help more workers enter or advance in the cyber workforce.

Lines of Effort

3.1.1 Encourage more robust stakeholder involvement in ecosystems.

ONCD and NCWCG will explore and share methods of developing cyber talent and connecting employers to workers with cyber skills. Federal departments and agencies will explore using funding to support cyber workforce development ecosystems using approaches embodied in the Department of Commerce strategic plan,[81] the Good Job Principles jointly developed by the Departments of Commerce and Labor,[82] and the Unlocking Career Success initiative at the Department of Education.[83]

Employers, labor organizations, and trade associations are encouraged to be active leaders in cyber workforce development ecosystems. As they bring industry cyber expertise to training and education programs, all stakeholders will benefit from the creation of a more robust pool of potential future cyber workers.

3.1.2 Improve cyber workforce data interoperability and analysis.

ONCD and the NCWCG will assess systems and processes that collect, analyze, and share data to improve our ability to describe the state of the national cyber workforce by industry and occupational classification. The Department of Labor's Bureaus of Labor Statistics and the Department of Commerce's Census Bureau will work across the government to refine and map cyber-related economic and employment statistics to provide ecosystem stakeholders with insights into current and anticipated cyber workforce needs.

★ ★ ★ ★ ★ ★

Departments and agencies will continue using public–private partnerships to synthesize and share cyber workforce data while protecting privacy, safety, and security, similar to the NICE collaborative effort that supports CyberSeek.org.[84]

ONCD will explore establishing an independent National Center for Cyber Data to serve as an authoritative resource.

3.1.3 Expand the availability of low- or no-cost workforce development tools for small enterprises.

Federal departments and agencies will explore partnering with academia and industry to increase the availability of upskilling and reskilling training materials to cyber workers, entrepreneurs, and employers in small enterprises and non-profit organizations.

Cyber workforce ecosystems should address the needs of small businesses related to cybersecurity planning, operating without cybersecurity staff, and meeting federal cybersecurity requirements.

Strategic Objective 3.2: Promote Skills-Based Hiring and Workforce Development

A skills-based approach is critical to connect more Americans to good careers. They should compete for jobs based on what they can do rather than merely credentials. Skills-based approaches also assist employers. Hiring by demonstrated skills is more predictive of job performance than hiring by education or work experience.[85] Once hired, workers will need timely and accessible upskilling and reskilling opportunities. A skills-based approach assists employees seeking to advance in the workplace and improves retention.

Integrated education and training models that include work-based learning, paid internships, externships, pre-apprenticeships, or registered apprenticeships have proven to be effective. Through these and other work-based learning opportunities, cyber workers can earn a wage as they gain hands-on experience and develop their skills.

Community and technical colleges make critical contributions to the cyber workforce. They also offer an avenue to reach women, who represent over half of learners enrolled in community colleges, as well as members of other groups currently underrepresented in the cyber workforce. Education-based and employer-led workforce development programs are more effective when industry actively engages in shaping curricula and provides work-based experiential learning opportunities.

All ecosystem stakeholders are encouraged to be active participants in developing rewarding cyber career pathways. Hiring managers and human resource professionals can collaborate to develop and implement skills-based talent management practices. Employers with skills-based programs can

★ ★ ★ ★ ★ ★

share best practices in skills-based workforce development. As an example of a constructive approach, NICE is supporting the Business Roundtable's Cybersecurity Workforce Initiative, which involves collaborative efforts to strengthen talent pipelines and skills-based career pathways.[86]

Lines of Effort

3.2.1 Leverage community colleges to enhance cyber workforce diversity and better meet local workforce needs.

Industry is encouraged to enhance partnerships with community and technical colleges to support cyber education opportunities with resources to align with industry-specific technologies and work roles.

ONCD and the NCWCG will promote the benefits of community and technical colleges as a robust source for cyber talent ranging from entry-level workers to reskilled and upskilled cyber professionals.

The Office of Personnel Management (OPM), working with other departments and agencies as appropriate, will explore opportunities to better align scholarship-for-service programs to learners in community college programs.

3.2.2 Build and enhance industry partnerships in cyber education and workforce development ecosystems to enhance diversity and improve programs.

Employers across industry sectors are encouraged to increase their participation in the development of cyber education and training programs in formal and informal learning environments. Investments by Microsoft,[87] Mastercard,[88] AT&T,[89] IBM,[90] and JPMorgan Chase[91] are examples of such industry commitments.

Industry and community and technical colleges are encouraged to partner to support the creation of cyber education and training content.

ONCD and the NCWCG will highlight best practices and encourage departments and agencies to collaborate with industry and increase the reach of cyber workforce development programs supported by federal funds.

3.2.3 Expand the use of skills-based hiring practices.

Employers are encouraged to increase the adoption of skills-based recruitment and talent development processes by evaluating their position descriptions and hiring approaches to better focus on needed cyber skills. Employer associations, labor organizations, and trade associations are encouraged to use common terminology, such as that included in the NICE Framework, when referencing skills requirements in position descriptions and job postings.

★ ★ ★ ★ ★ ★

3.2.4 Expand the use of skills-based workforce development practices.

The NCWCG will work across departments and agencies to coordinate skills-based talent development programs, resources, and technical assistance, such as the Networking and Information Technology Research and Development (NITRD) STEM Portal,[92] to support workforce development ecosystems.

NICE will continue to promote, energize, and support adoption of the NICE Framework to strengthen skills-based workforce development efforts. The Administration will work with Congress to secure funding for these efforts.

3.2.5 Increase on-ramps to cyber careers through work-based learning opportunities.

Public and private sector employers are encouraged to increase registered apprenticeships, pre-apprenticeships, and paid internships. To reach underrepresented and underserved communities, employers are encouraged to partner with organizations focused on enhancing the talent pipeline in these communities. Employers are also encouraged to establish entry-level positions that provide avenues for advancement.

Colleges, universities and SLTT governments are encouraged to increase the use of hands-on learning opportunities, such as cyber clinics and cyber ranges, to enable students to work directly with organizations in their communities and develop cyber skills in simulated environments.

Departments and agencies will explore including incentives in grants and contracts to increase the number of work-based learning opportunities that develop cyber skills and on-ramps to employment. This may include working with the Department of Labor to review and revise the education and work experience requirements to allow registered apprentices and others in skills-based development pathways to participate. Doing this may create opportunities for those who have aptitude but not a formal degree, including many veterans.

3.2.6 Encourage the adoption of flexible employment models, such as fractional employment.

Employers, labor organizations, unions and intermediaries are encouraged to embrace fractional employment models that would make cyber experts available to multiple employers. For example, an AI developer could work for a large technology firm for 20 hours per week, a local government for 10 hours per week, and a non-profit organization for 10 hours. Unlike freelancing or contracting, each employer, or an intermediary, would provide proportional benefits that constitute a comprehensive benefits package across the different employers. This approach may provide small businesses access to highly skilled cyber talent they might not otherwise be able to. ONCD will convene employers, industry representatives, and cyber experts to identify barriers to expanding fractional employment models and solutions to reframe employment structures while embodying Good Job Principles.

★ ★ ★ ★ ★ ★

3.2.7 Engage with employers and human resource professionals on skills-based strategies.

Together with human resources (HR) organizations, the NCWCG will facilitate conversations between departments and agencies to determine how government resources—such as the NICE Framework, the Department of Labor's O*NET,[93] and employment data—can be improved to identify cyber workforce needs and support skills-based best practices. One such best practice is aligning position descriptions, recruitment postings, and staff development programs with the cyber skills required. Use of the NICE Framework can support such alignment. The NICE program office will continue to engage with human resources organizations to encourage skills-based hiring practices.

Employers are encouraged to empower hiring managers to advocate for cyber skills recruiting.

STRATEGIC OBJECTIVE 3.3: LEVERAGE THE DIVERSITY OF AMERICA TO STRENGTHEN THE CYBER WORKFORCE

The success and competitive strength of the cyber workforce depends on ensuring all workers, including those from underserved and underrepresented populations, have foundational cyber skills.

A diverse and inclusive cyber workforce will broaden the range of ideas brought to bear on complex cyber challenges while enabling employers to retain staff. Recruiting and retaining members of underserved and underrepresented communities will grow the supply of talent to meet growing workforce demands.

All stakeholders in cyber workforce development ecosystems are encouraged to play constructive roles in enabling veterans and their spouses to participate in the cyber workforce. Veterans represent a large, diverse, and technologically skilled community of people who have served the country and are committed to mission success. As the military has already provided them with the opportunity to gain skills and experience, veterans may have a decreased need for employer-sponsored training and a higher rate of success during the first year of employment. Many veterans separate from service with active security clearances, which make them good candidates for sensitive cyber jobs.

Lines of Effort

3.3.1 Explore incentives in federal cyber grants and contracts addressing underrepresented and underserved communities.

Federal departments and agencies will explore including provisions addressing underrepresented or underserved communities, where legally permissible and appropriate, in cyber grant and contract opportunities in order to leverage talent from the broadest possible pool of workers. This effort will draw on the Good Jobs Principles as well as the Department of Commerce's best practices for highly effective workforce investments.[94]

★ ★ ★ ★ ★ ★

3.3.2 Expand the availability of low- or no-cost competency-based credentials.

The NCWCG will explore programs across agencies that can contribute to the development of low- or no-cost industry-valued cyber credentials. SLTT governments and employers are also encouraged to increase awareness of cyber skills that industry-recognized credentials represent and help hiring managers develop position descriptions that better reflect needed skills. Credential providers are encouraged to develop such cyber credentials to facilitate broad access.

3.3.3 Increase collaboration with organizations that serve or operate within underserved and underrepresented communities.

The NCWCG will promote collaboration with public and private organizations that represent, support, and engage underserved and underrepresented populations to help develop more inclusive cyber hiring practices, work-based learning programs, and training programs. (Several organizations that do this work can be found at Appendix C.)

Industry and education institutions are encouraged to partner with federal, state, Tribal, and local entities that support workforce boards, Small Business Development Centers, American Job Centers, and Job Corps Centers, to incorporate cyber skills development.

3.3.4 Facilitate and support greater participation by veterans in the cyber workforce.

The Department of Labor's Veterans' Employment and Training Service (VETS)[95] and Regional Veterans' Employment Coordinators, the Department of Health and Human Services' Centers for Medicare and Medicaid Services (CMS), and other departments and agencies will continue to help veterans join the cyber workforce. They will communicate the benefits of hiring veterans and help employers hire veterans by translating military experiences, skills, credentials, certifications and nomenclature into terms in use in the civilian workforce. Ecosystem stakeholders are encouraged to do the same, with a particular focus on public-private partnerships that support job training, industry certifications, and upskilling to prepare veterans for entry or advancement in high-demand cyber occupations. The NSA-funded CyberSkills2Work Program, which involves more than 40 business entities may serve as a model for such partnerships,[96] as does the Veteran and Military Spouse Talent Engagement Program (VMSTEP),[97] led by the Department of Veterans Affairs (VA), which supports the Hiring Our Heroes organization and other activities with résumé help, career counseling, and hiring events.

3.3.5 Develop immigration policies to welcome and retain foreign-born talent into the nation's cyber workforce.

ONCD will work with stakeholders in the executive branch to support the development of policies and procedures to welcome and retain foreign-born talent in the cyber workforce, especially those educated and trained in the United States. Because the immigration changes necessary to significantly increase the retention of foreign-born talent trained in the United States can be

accomplished only through legislation, the Administration also calls on Congress to enact meaningful immigration reform.

Strategic Objective 3.4: Enhance International Engagements

Global connectivity brings tremendous opportunities for increased prosperity, but it also brings great risks. Malign activity can easily cross borders, and technologies essential to our society are increasingly online. Building a robust, secure, and resilient cyberspace that advances our values will require extensive cooperation with America's partners and allies around the world.

America's global partnerships are critical national resources, and we should more fully realize their potential. To advance America's cyber workforce development, we will exchange cyber workforce development best practices with international partners. As discussed in the NCS, the federal government will also engage in efforts to strengthen the capacity of like-minded states and grow the global cyber workforce.

Lines of Effort

3.4.1 Collaborate with international partners and allies on workforce development best practices.

The Department of State and NICE will continue to lead international collaboration on cyber workforce development best practices. Where possible, these efforts will build on NICE's ongoing work to broaden use of the NICE Framework, including with Five Eyes Partners and the Global Forum on Cyber Expertise.[98] ONCD will foster alignment of federal activities and enhance public–private partnerships related to international cyber workforce development.

3.4.2 Include cyber workforce development in U.S. capacity-building efforts abroad.

The Department of State will lead to ensure international capacity-building priorities are strategically aligned and advance the interests of the United States and its allies and partners. ONCD will support the Department of State and USAID in these efforts. We will look for opportunities to incorporate cyber workforce development into capacity-building initiatives across federal departments and agencies and foster collaboration with public and private sector actors.

PILLAR FOUR | STRENGTHEN THE FEDERAL CYBER WORKFORCE

The federal cyber workforce performs vital work, including: protecting government IT systems, networks, and data from the most sophisticated adversaries; supporting and protecting critical infrastructure; and investigating and prosecuting malicious cyber activity. It is essential to the design, development, and provision of essential products and services that enable the government to deliver high-quality, equitable, and secure services to the American people. This workforce plays a central role in formulating and executing on domestic, foreign, and national security policies that advance our national interests and values and those of international partners and allies, improving the prosperity and security of our country and building resilience around the world.

Although many people are attracted to federal service out of a desire to contribute to the government's mission, departments and agencies can find it challenging to offer competitive salaries.[99] Administrative challenges associated with extended hiring and onboarding timelines, currently being addressed through implementation of the President's Management Agenda and initiatives that include the formation of the Hiring Experience Group by OPM, can make it challenging for departments and agencies to hire top talent.[100] Many federal cyber positions require security clearances, leading to further delay in hiring timelines that may deter otherwise qualified job seekers. The Trusted Workforce 2.0 initiative is working to improve personnel vetting, reducing the time required to bring new hires onboard and better enabling the mobility of the federal workforce.[101]

The federal cyber workforce also faces demographic challenges, including a growing population of workers eligible for retirement and a shortage of workers who are women or members of younger age cohorts.[102] The federal government must strengthen its cyber workforce and to do so more effectively it must attract members of underserved and underrepresented groups. A clear description of the varied cyber roles, responsibilities and missions may help to increase interest.

The federal government should be a leader in the use of skills-based hiring best practices, which includes using skills-based assessments.[103] Qualified professionals with diverse backgrounds, perspectives, and experiences may be deterred from pursuing opportunities in the federal government by job postings that reference obscure occupational classification series and require credentials such as four-year degrees and certifications. Skills-based hiring appropriately puts the focus on what candidates can do, creating greater openness to candidates with the important cyber skills.[104]

★ ★ ★ ★ ★ ★

STRATEGIC OBJECTIVE 4.1: DRIVE SUSTAINED PROGRESS THROUGH GREATER FEDERAL COLLABORATION

Strengthening the federal cyber workforce requires active and sustained collaboration. Studies have identified gaps in interagency coordination as a factor contributing to persistent challenges in the federal cyber workforce.[105]

The Federal Cyber Workforce Working Group (FCWWG), a subordinate body of the NCWCG, develops government-wide policies and coordinates the planning and execution of actions to strengthen the federal cyber workforce. Co-chaired by the Office of Management and Budget (OMB) and ONCD, in close consultation with OPM, this group brings together department and agency representatives to craft approaches that are both feasible and effective. The work of the FCWWG is aligned and integrated with other key federal workforce efforts, including the implementation of the President's Management Agenda. The FCWWG will also advance mandates set forth in NSM-3, "Revitalizing America's Foreign Policy and National Security Workforce," that pertain to the federal cyber workforce.[106]

Efforts to improve federal cyber workforce management should rest on high-quality data. Where possible, departments and agencies will evaluate information on current and projected cyber workforce needs to craft and execute evidence-based workforce strategies. To assist, OPM created a cyber workforce dashboard for use by agencies and the general public.[107]

OPM's dashboard is an important foundation for further improvements to the data supporting cyber workforce management decisions. Currently, many federal human resources (HR) professionals manage cyber positions using an occupational series that is often outdated or insufficiently precise. While the Federal Cyber Workforce Assessment Act (FCWAA) of 2015 required departments and agencies to add the three-digit NICE Framework code to IT, cybersecurity, or other cyber-related positions and to report cyber work roles of critical need to OPM on an annual basis, inconsistent application of the NICE Framework across agencies reduces the utility of the resulting data.[108] The FCWAA mandate expired in 2022 with no plan for renewal.

This strategy includes a strong commitment to the holistic integration of NICE Framework work roles into existing federal workforce management practices, and the deployment of strategic initiatives based on cyber work roles instead of the outdated occupational series.

Lines of Effort

4.1.1 Use the FCWWG to drive sustained improvements in the federal cyber workforce.

The FCWWG will play a leading role in driving federal coherence in the implementation of this pillar of the strategy, approving refined cyber roles and responsibilities, metrics, and timelines.

★ ★ ★ ★ ★ ★

The FCWWG will strengthen the sense of community among federal cyber workforce leaders across departments and agencies who are dedicated to improving federal cyber workforce development through collaboration to meet common challenges.

4.1.2 Enable better data-informed decision making to guide federal cyber workforce management.

In an effort coordinated by the FCWWG, the NICE program office, OPM, and select department and agency representatives will evaluate ways to strengthen the use of work roles derived from established workforce frameworks, including the NICE Framework, in cyber workforce management. Work roles can be used to better understand the size, disposition, composition, and developmental needs of the federal cyber workforce. Departments and agencies should also be able to use these work roles to determine skills demands now and in the future, and focus their strategic human capital efforts appropriately.

STRATEGIC OBJECTIVE 4.2: ATTRACT AND HIRE A QUALIFIED AND DIVERSE FEDERAL CYBER WORKFORCE

To meet its current and future cyber workforce needs, the federal government must articulate the benefits of public service and provide robust on-ramp opportunities at every stage of career development. Recruitment must highlight the unique and challenging missions performed by federal departments and agencies, which often require the use of expertise, skills, and insights that can be developed only through government service. Important on-ramps include scholarships, paid internships, registered apprenticeships, and reskilling opportunities. The government must also seek to attract professionals from the private sector.

Two proven programs that provide scholarships in return for federal service are CyberCorps Scholarship For Service, managed by the NSF in collaboration with OPM and CISA, and the DoD Cyber Scholarship Program (CySP).[109] The federal government will explore expanding the capacity of programs such as these.

Another valuable way to attract additional talent to the federal government is the use of internships, such as those listed on the Federal Internship Portal,[110] that enable students from high schools, technical schools, and colleges and universities to explore careers in the federal government. The Intelligence and Cybersecurity Diversity Program in the Department of Homeland Security (DHS) offers a potential model for strengthening the cyber workforce through improvements in diversity.[111] Other potential models include the Department of Energy Omni Technology Alliance Internship Program, which provides paid rotational internships in cybersecurity, information technology, and related fields to talented undergraduate and graduate students from underserved communities.[112] A third potential for paid internships is the Homeland Security Investigations (HSI)—Human

★ ★ ★ ★ ★ ★

Exploitation Rescue Operation (HERO) Child-Rescue Corps Program,[113] which recruits and trains veterans to be digital forensic analysts.

In addition to providing paid internships to current students, the federal government must seek to attract recent college graduates to government service. One example is the U.S. Digital Corps, launched in August 2021 and operated by the General Services Administration's (GSA) Technology Transformation Services.[114] The U.S. Digital Corps has attracted qualified, diverse, early career talent to government service. Another example is the Cyber Fellowship program established at the Department of Justice.[115] This three-year program provides selected attorneys experience in combatting emerging national security and criminal cyber threats, as they rotate through multiple department components.

Registered apprenticeships are another valuable mechanism for growing the federal cyber workforce. Existing programs can serve as models, including the DoD's United Services Military Apprenticeship Program (USMAP), in existence since 1999.[116] In January 2022, USMAP established the first and largest cybersecurity registered apprenticeship program in the federal government, with 15 approved occupational tracks. A civilian-focused model can be found in the VA, which recently designed and established the first civilian federal cybersecurity registered apprenticeship program, and will bring on its initial cohorts in 2023.

Reskilling or upskilling enables departments and agencies to take advantage of existing human capital investments, as military veterans and federal civilian employees already have professional training, experience, and mission knowledge and understanding. They may also possess security clearances, making onboarding more efficient. One opportunity is provided by the DoD SkillBridge Program.[117] As 200,000 service members transition out of uniform each year, this program enables them to gain valuable civilian work experience during their last 180 days of service. This time could be spent exploring opportunities to serve as a civilian in the federal cyber workforce. Additional potential reskilling or upskilling opportunities include the Veteran Employment Through Technology Education Courses (VET TEC) [118] and Veteran Readiness and Employment (VRE),[119] two programs administered by the VA. VET TEC matches veterans with approved training providers to help develop high-tech skills, while VRE helps veterans with service-connected disabilities explore employment options and address education or training needs.

As the federal government increases the use of skills-based assessments in cyber workforce hiring, position descriptions developed using the NICE Framework provide a strong starting point issuing job announcements that focus on needed skills and do not overstate credential requirements. This is an area in which the federal government can continue to lead by example, as one study found that 46% of federal cybersecurity jobs were open to applicants without a bachelor's degree, compared to only 20% of cybersecurity jobs in the private sector.[120]

Department and agency collaboration on cyber hiring strategies will lead to efficiencies and economies of scale. For example, OPM recently coordinated a hiring action for data analysts in which candidates were assessed by subject matter experts in the field. Over 100 candidates received

job offers from 33 agencies and components from this one hiring action, helping to recruit talent in an efficient and effective manner.

Lines of Effort:

4.2.1 Lead the development and implementation of skills-based hiring practices.

The FCWWG will coordinate efforts to assist departments and agencies in expanding the use of skills-based assessments to hire individuals for the federal cyber workforce.[121] As a supplement to résumé reviews, skills-based candidate assessments such as job knowledge tests and job-related simulations could greatly improve hiring efficacy for critical cyber skills.

The FCWWG will support an OPM initiative to enable departments and agencies to refocus position announcements on cyber skills. To maximize the effectiveness of a skills-based approach, position descriptions will be developed using work roles, such as those found in the NICE Framework. This initiative will draw on ongoing efforts by the NICE Program Office to identify needed skills, including professional skills such as teamwork and communication, as well as tools for assessing proficiency.

4.2.2 Grow programs that provide scholarships for federal service.

Departments and agencies will explore the steps needed, including work with Congress, to expand the number of people matriculating through proven programs such as CyberCorps Scholarship For Service and CySP that provide scholarships in return for federal service.

While the federal government benefits from skills-based hiring, it also requires a cyber research and development workforce with advanced degrees. Currently, the ability of CyberCorps Scholarship For Service to meet this need is limited, as the program is authorized to provide only two years of funding. The Administration will work with Congress to enable scholarship recipients pursuing doctoral programs to be eligible for five years of funding.

The FCWWG will explore opportunities to grow the Cybersecurity Talent Initiative. This public–private partnership enables selected students to gain valuable work experience during a two-year placement in the federal government and the opportunity to receive student loan assistance if hired during that period by a private sector partner.[122]

4.2.3 Scale paid internship and Registered Apprenticeship opportunities.[123]

The FCWWG will coordinate work by departments and agencies to expand the use of paid internships to attract talent to the federal cyber workforce, encouraging the use of OPM's internship portal to support these efforts.[124] The FCWWG will also provide assistance with investments in programs designed to attract recent graduates.

The FCWWG, in coordination with the Department of Labor Office of Apprenticeship, will facilitate the sharing of best practices using registered apprenticeships for cyber positions.

★ ★ ★ ★ ★ ★

4.2.4 Reduce barriers to better enable cyber professionals to transition between private and public service.

The FCWWG will facilitate the sharing of best practices among departments and agencies for former government employees returning to federal service, as they take advantage of new OPM guidance that facilitates this transition.

The FCWWG will also explore opportunities to attract individuals with private sector experience to public service. As an example, in the midst of technology sector layoffs, OPM partnered with over 50 agencies to hold a "Tech to Gov" event in early 2023 that drew over 1,800 potential job seekers. Beyond the immediate hires, events like this build relationships with possible job candidates and institutions and publicize opportunities available in federal service.

Departments and agencies will, where possible, review security clearance requirements for cyber positions to ensure that job announcements do not overstate vetting requirements. They are encouraged to remain abreast of reforms under consideration in the Trusted Workforce 2.0 initiative so that they benefit from its work and act in compliance with federal policy.

4.2.5 Improve awareness of job opportunities.

The FCWWG will coordinate efforts by departments and agencies to support OPM's CyberCareers.gov as a central hub for federal cyber career resources and for recruitment. As a supplement to USAJOBS, CyberCareers.gov serves as a useful employment hub with resources for job seekers, hiring managers, federal employees, students, and educational institutions.

It is critical that employment opportunities advertised on USAJOBS include meaningful job titles, and allow departments and agencies to track metrics for specific opportunities. The FCWWG will support agency use of descriptive job titles and seek to phase out generic position titles—such as IT Specialist—for recruitment purposes. It will provide assistance on using the NICE Framework with the ultimate goal of including NICE work roles in all relevant federal cyber positions.[125] As usage increases, OPM will deploy a work role filter on USAJOBS that enables job seekers to more readily identify positions of interest.

The FCWWG will coordinate department and agency involvement in a recruiting campaign for the federal cyber workforce that presents public service as an attractive career path offering unique opportunities to acquire skills and advance an important public mission. The campaign will target all Americans, and include outreach to underserved and underrepresented communities and individuals with disabilities. It will include partnerships with state and local workforce boards, colleges and universities, and organizations focused on strengthening the talent pipeline by increasing the diversity of trainees and federal cyber professionals. The campaign will also feature interviews with civil servants who will provide stories from their federal cyber service.

★ ★ ★ ★ ★ ★

4.2.6 Expand the use of shared hiring actions.

The FCWWG will encourage departments and agencies to partner on shared hiring actions, drawing on the expertise of OPM's Hiring Experience (HX) group, and focusing on positions of critical need.[126] As this effort matures, the FCWWG will encourage agencies to provide subject matter experts to review certificates of qualified candidates, advertise shared certificates within agencies, and publish agency procedures for hiring managers to leverage shared certificates.

STRATEGIC OBJECTIVE 4.3: IMPROVE CAREER PATHWAYS IN THE FEDERAL CYBER WORKFORCE

The federal government must explore the development of model cyber career pathways that present attractive careers, helping federal cyber workers to understand how to advance throughout their careers.[127] These model pathways could be informed by NICE Framework work roles. Given the variety of rewarding positions in federal service, model career pathways could be a key resource for departments and agencies as they strengthen recruiting, engage employees, and improve retention.

Federal workers in in roles that require significant cyber skills will need professional development guidance that is specific to their position and potential career pathway. In the NICE Framework, work roles provide descriptions of cyber work, aligned tasks, and the corresponding knowledge and skills required to perform those tasks effectively.[128] These components are helpful for identifying the right skill development opportunities. Furthermore, workforce frameworks can assist employees and their supervisors to better understand how their current skills might be applied in different ways in related cyber roles.

The 2023 DoD Cyber Workforce Strategy provides insight into how standardized work role data can be used to identify workforce needs and support the recruitment, development, and retention of cyber talent.[129] Use of the work roles in the DoD Cyber Workforce Framework (DCWF) will enable DoD to strengthen workforce management, training, and career pathways. The recent expansion of the DCWF to encompass work roles related to emerging technologies—such as AI and ML—will help DoD keep pace with a dynamic technological and threat environment.

Departments and agencies will, where possible, leverage standardized learning opportunities – such as the Federal Virtual Training Environment (FedVTE) [130] managed by CISA, the Open Opportunities platform run by OPM, and the CyberVets Program[131] managed by CMS – to support employee development of transferable skills and disrupt barriers to career advancement.

In addition, federal cyber workers need access to tools that enable them to record their developing professional capabilities throughout their careers, including for example the Federal Emergency Management Agency's (FEMA) OneResponder System, which tracks relevant training and qualifications for first responders.[132] Such tools would not only empower employees, but also enable

the government to maintain a current inventory of cyber workforce readiness capabilities for use by management.

Hiring and pay flexibility are powerful employment tools that could assist departments and agencies in strengthen their cyber workforce. Solutions available under existing personnel authorities include student loan repayment, critical pay authority, and recruitment, retention, and relocation pay incentives.[133] For example, DoD's Cyber Excepted Service (CES) provides for flexibility in hiring, pay, professional development, and promotions, and this enables DOD to attract, retain, and employ civilian talent more effectively. Similarly, DHS's Cyber Talent Management System (CTMS) includes exceptions to the competitive service terms of employment and financial incentive structure.[134] Notwithstanding CES and CTMS, such solutions are not being fully utilized, and several agencies face challenges in retaining personnel with critical cyber skills. Departments and agencies should assess their ability to take advantage, within their budgets, of existing as well as new hiring and retention flexibilities.

Lines of Effort

4.3.1 Develop and publicize model career pathways.

The FCWWG will work with OPM, CISA, the NICE program, DoD, the VA, and other agencies, as appropriate, to assess the Cyber Careers Pathway Tool, which was developed using the NICE Framework. This assessment will: evaluate the Tool's ability to mapping cyber careers in an effective, understandable manner; determine whether modifications are warranted; and develop an approach to updating it using emerging best practices. If appropriate, the government will promote its use among employees.[135]

4.3.2 Invest in professional development.

The FCWWG will inventory existing training and work-based learning and skills assessment programs, assess their adequacy and alignment with other workforce development efforts, and explore enhancements, as appropriate.

ONCD will support the continued use of competitions, such as the President's Cup managed by CISA and the Codebreaker Challenge at NSA, to identify, recognize, and reward cyber talent across the federal workforce.

ONCD and the FCWWG will explore the creation of a Federal Cyber Workforce Development Institute (Institute), which would provide standardized, role–specific skilling, reskilling, and upskilling opportunities. By providing curriculum guidance and training for entry-level positions, the Institute could create valuable pathways into federal service and rapidly strengthen the cyber talent pipeline. The Institute would also facilitate career progression for current cyber practitioners by providing continuing education and professional development opportunities.

★ ★ ★ ★ ★ ★

The FCWWG will assess the utility of an LER system that enables members of the cyber workforce to develop, record, and obtain endorsements for their work-based learning experiences and the cyber skills they possess.

Where possible, departments and agencies will take advantage of the Cyber Rotational Program, a new governmentwide program established under the 2021 Federal Rotational Cyber Workforce Program Act,[136] which allows federal cyber employees to experience 6-month to 1-year interagency details to positions where they can achieve higher skill levels or skills in different areas. Departments and agencies will also explore employing internal rotation programs to enhance cyber skills development, employee engagement, and retention.

In order to foster skills development while improving the security and resilience of critical open-source software, the FCWWG will evaluate methods of incentivizing federal employees and contractors to make contributions to the open-source software on which the government depends.

4.3.3 Make hiring and pay flexibilities, as well as other talent management tools, more available to meet critical needs across the entire federal cyber workforce.

The Administration will work with Congress on proposals that complement the flexible hiring and compensation authorities in CES and CTMS by establishing similar hiring, pay, and talent management authorities in departments and agencies across the federal government.

The FCWWG will work with OPM and other departments and agencies to study human capital solutions available under existing administrative authorities, and the barriers to robust utilization of such authorities.

The FCWWG will facilitate the sharing of on-the-job cyber training and mentorship best practices among departments and agencies.

★ ★ ★ ★ ★ ★

STRATEGIC OBJECTIVE 4.4: INVEST IN HUMAN RESOURCES CAPABILITIES AND PERSONNEL

As recognized in the President's Management Agenda, investments in HR are necessary for enabling departments and agencies to deliver on their missions. The federal government must, where possible, train HR personnel across the executive branch to ensure that a sufficient number in each department or agency have sufficient expertise in cyber job requirements to build a stronger federal cyber workforce. Working in close partnership with hiring managers, this cadre of HR personnel trained in cyber would facilitate recruitment and hiring processes that result in the hiring of qualified cyber workers.

Lines of Effort

4.4.1 Train HR professionals in cyber talent management.

The FCWWG will coordinate with OPM to develop a training program for HR specialists who will be able to apply best practices to the recruitment and hiring of federal cyber workers. This cadre would also be equipped with the knowledge and tools for cyber personnel management, as tailored to the needs of each department or agency. The Federal Cyber Workforce Development Institute proposed in Line of Effort 4.3 would also serve as a ground for train HR specialists on the unique dimensions, requirements, and talent acquisition challenges associated with the cyber workforce.

4.4.2 Provide tools and capabilities to support cyber talent management.

OPM, with support from the FCWWG, will make existing hiring and pay flexibilities more accessible to departments and agencies. While OPM has created tip sheets, an executive talent playbook, and a cyber workforce hub[137] relating to these authorities, widespread lack of familiarity inhibits their use.

★ ★ ★ ★ ★ ★

IMPLEMENTATION

As directed by the President in the NCS, ONCD will oversee the implementation of this National Cyber Workforce and Education Strategy. ONCD will work within the Executive Office of the President and with interagency partners to refine roles and responsibilities and to establish metrics and timelines. The NCWCG will with the FCWWG and other subordinate working groups, as necessary, to oversee implementation.

With regard to the non-federal entities that are called upon to take action in this strategy, many have already embarked on initiatives aligned with the strategy's objectives. These activities should continue, hopefully marked by ever-increasing collaboration with other key stakeholders in cyber workforce and education ecosystems. To encourage, further inform, and support these efforts, ONCD will explore the establishment of a standing advisory committee to provide a regular venue for receiving public advice and input on cyber workforce and education strategies, plans, programs, and activities. In addition, ONCD and the NCWCG will leverage existing Federal stakeholder engagement efforts, such as interagency groups and public–private partnerships, and potential new mechanisms such as periodic summits to drive action with the support of ecosystem stakeholders and partners.

In implementing this strategy, ONCD and the NCWCG will adopt a data-driven approach. ONCD and the NCWCG will identify gaps, develop performance measures for outcome-based goals, regularly communicate progress to stakeholders, and use data to assess progress toward goals.

At this important inflection point in our country's history, building a workforce that fuels the prosperous economy that Americans deserve while advancing the security interests of the country will require targeted investments by government at all levels, industry, academia, and non-profit institutions, ONCD will work with OMB to ensure alignment of department and agency budget proposals to achieve the goals set out in this strategy.

The Administration will work with Congress to prioritize cyber workforce and education activities to meet the challenges of today and tomorrow, and equip Americans with the cyber skills necessary to thrive and prosper in our increasingly interconnected society.

★ ★ ★ ★ ★ ★

APPENDIX A: Definitions

Computational literacy: The ability to use information, information processing agents, digital assets, networking components, and applications and systems that, combined, allow people and organizations to interact in a digital world to solve problems, either individually or with a team; to draw meaning and reasonable conclusions from digital information in both personal and professional contexts; to safely, ethically, and securely use networks (wired and wireless) and data; and to understand how computing, data, and connectivity affects society (Source: https://www.whitehouse.gov/wp-content/uploads/2023/02/Final_2022_CoSTEM_Progress_Report.pdf, p. 12).

Cyber: A term that refers to both information and communications networks (Source: https://csrc.nist.gov/glossary/term/cyber).

Cyber education and workforce development ecosystem: Ideal cyber education and workforce development systems may involve learners (students, job seekers, and employees), employers, educators, trainers, government at all levels, non-profit organizations, philanthropists, and other influential civil society organizations; include multisector partners united by a common vision of cyber education or workforce development; seek to advance accessible, inclusive cyber learning opportunities across all education stages and career pathways; continuously evaluate their activities and adapt as needed; plan for the long term; communicate their work broadly to build support and advance best practices; and reflect the multidisciplinary nature of cyber roles, embracing not only science, technology, engineering, and mathematics (STEM) but also other disciplines, including business, the social sciences, and the humanities (Source: adapted from the definition of a STEM education ecosystem, https://www.whitehouse.gov/wp-content/uploads/2022/01/2021-CoSTEM-Progress-Report-OSTP.pdf, p. 4, n. 5).

Cyber workforce: Those who design, build, secure, operate, analyze, protect, and defend cyberspace resources. It encompasses those who work in the frequently overlapping fields of technology manufacturing, software development, information technology (IT), operational technology (OT)/industrial control systems (ICS), cybersecurity, cyberspace operations, cyber investigations and prosecutions, some intelligence roles, and related research and development. The cyber workforce also includes those who lead or support work in these fields through activities that include governance, law and compliance, policy, strategy and planning, privacy, acquisition, program and program management, and workforce management and development (Source: adapted from DoD Directive 8140.01, "Cyberspace Workforce Management," October 5, 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.pdf, and informed by the NICE Framework, https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/getting-started).

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity,

★ ★ ★ ★ ★ ★

authentication, confidentiality, and nonrepudiation (Source: https://csrc.nist.gov/glossary/term/cybersecurity).

Cyberspace: A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (Source: https://csrc.nist.gov/glossary/term/cyberspace).

Digital inclusion: The activities that are necessary to ensure that all individuals in the United States have access to, and the use of, affordable information and communication technologies, such as—(i) reliable broadband internet service; (ii) internet-enabled devices that meet the needs of the user; and (iii) applications and online content designed to enable and encourage self-sufficiency, participation, and collaboration[.] [It] includes—(i) obtaining access to digital literacy training; (ii) the provision of quality technical support; and (iii) obtaining basic awareness of measures to ensure online privacy and cybersecurity (Source: https://www.congress.gov/117/bills/hr1841/BILLS-117hr1841ih.pdf, p. 5).

Digital literacy: The ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills (Source: https://tech.ed.gov/files/2022/10/DLA_Report_Launching_Digital_Literacy_Accelerator.pdf, p. 1).

Digital resilience: Having the awareness, skills, agility, and confidence to be empowered users of new technologies and adapt to changing digital skill demands. Digital resilience improves capacity to problem-solve and upskill, navigate digital transformations, and be active participants in society and the economy (Source: https://digitalus.org/wp-content/uploads/2020/06/DigitalUS-Report-pages-20200602.pdf, p. 6).

Digital skills: Technology skills, such as social media or computer literacy, or those that pertain to a named software product, hardware tool, or category of products, such as Google Docs or AutoCAD (Source: adapted from "definitely digital skills," https://nationalskillscoalition.org/wp-content/uploads/2023/02/NSC-DigitalDivide_report_Feb2023.pdf, p. 53).

Foundational cyber skills: The combination of digital literacy, computational literacy, and digital resilience that equips every individual to thrive in an interconnected society.

Industrial control system: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes (Source: https://csrc.nist.gov/glossary/term/industrial_control_system).

Information technology: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive

agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources (Source: https://csrc.nist.gov/glossary/term/information_technology).

Operational technology: Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms (Source: https://csrc.nist.gov/glossary/term/operational_technology).

★ ★ ★ ★ ★ ★

APPENDIX B: Foundational Cyber Skills

Foundational cyber skills are essential preparation for today's workforce and enable persons with these skills to enjoy full, safe, and secure access to resources in our interconnected society. This appendix explains the three components of foundational cyber skills: digital literacy, computational literacy, and digital resilience.

Digital Literacy

Background. The definition of digital literacy is taken from the Museum and Library Services Act of 2010, Pub. L. No. 111-340, 124 Stat. 3594 (2010).

Purpose. Both the Workforce Innovation and Opportunity Act of 2014 (WIOA) and Digital Equity Act of 2021 (DEA) apply the Museum and Library Services Act definition, recognizing that digital literacy will become increasingly important to securing a quality job and the advancement of the American workforce.

Definition. The ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills.[138]

The importance of digital skills is reflected in the development of a number of frameworks. Among these are

International Society for Technology in Education (ISTE)
Global Media and Information Literacy (MIL) Framework
International Standards for Technological and Engineering Literacy
Digital Citizenship Education Framework
American Association of School Librarians (AASL)
Global Digital Literacy Council Framework
Standards for Libraries in Higher Education | Association of College & Research Libraries (ACRL)
Principles for Digital Development
USAID Digital Literacy Primer
UNESCO ICT Competency Framework for Teachers
Digital Intelligence (DQ) Framework
Common Sense Education K-12 Digital Citizenship
UNESCO Global Framework of Reference on Digital Literacy Skills
Mozilla Web Literacy Framework
Common Framework of Reference for Intercultural Digital Literacies
SkillsUSA Framework
Employability Skills Framework
Teaching Tolerance Digital Literacy Framework
Principles for Digital Development

★ ★ ★ ★ ★ ★

Computational Literacy

Background. The definition of computational literacy used here was developed after extensive research and input across the interagency of the federal government.

Purpose. It was intended to bring coherence to federal efforts to promote lifelong education in science, technology, engineering, and math (STEM) for all Americans.

Definition. Computational literacy is the ability to use information, information processing agents, digital assets, networking components, and applications and systems that, combined, allow people and organizations to interact in a digital world to solve problems, either individually or with a team; to draw meaning and reasonable conclusions from digital information in both personal and professional contexts; to safely, ethically, and securely use networks (wired and wireless) and data; and to understand how computing, data, and connectivity affects society.[139]

Computational literacy helps an individual –

A. ethically, securely, safely, and efficiently use information processing agents, digital tools, and digital platforms to teach, learn, and solve problems, including problems with sensitive information;
B. problem-solve (e.g., decomposing problems into manageable pieces; heuristic reasoning; algorithmic thinking; computational thinking);
C. think recursively;
D. navigate multiple levels of abstraction;
E. recognize patterns;
F. collect, analyze, manage, visualize, and communicate data;
G. translate domain knowledge into mathematical and visual models;
H. understand the social, technical, and cultural dynamics of computational technology, including equity, inclusion, and accessibility; and
I. critically evaluate related technologies.[140]

Digital Resilience

Background. The definition of digital resilience was developed for the inaugural report by Digital US titled "Building a Digitally Resilient Workforce: Creating On-Ramps to Opportunity.".

Purpose. Digital US, a coalition of companies and organizations, argues that it is imperative to design, build, and scale the on-ramps and support that adult learners and workers need. Digital resilience enables people to meet the constantly evolving technical skills requirements of employers.

Definition. Having the awareness, skills, agility, and confidence to be empowered users of new technologies and adapt to changing digital skill demands. Digital resilience improves capacity to problem-solve and upskill, navigate digital transformations, and be active participants in society and the economy.[141]

★ ★ ★ ★ ★ ★

APPENDIX C: RFI Respondents

The following organizations and individuals contributed valuable insights in response to ONCD's nationwide request for information (RFI) on cyber workforce, education and training:[142]

2U, Heartland Cyber Coalition
418 Intelligence
A.J. Boggs & Company
Bethany Abbate
Accenture
ACT | The App Association
Air Force Research Laboratory
Alexandria Technical and Community College
American Cybersecurity Institute
Amyx
AnitaB
Ankura
Aspen Digital
Aspen Tech Policy Hub
Astrolytes, CyberCo-op
Atlantic Council
Nancy Austin
Bank of America
Boeing
Boise State University
Booz Allen Hamilton
BSA | The Software Alliance
Matt Burton and Klee Dienes
C Evans Consulting
California State University, San Bernardino
Cambridge Global Advisors
Capture the Flag Coalition
Carahsoft Technology Corporation
Cedarville University
Cengage Group
Center for Strategic and International Studies
Centers of Academic Excellence in Cybersecurity Community
Agnes Chan
Cisco
Collin College
Common Sense Media
Commonwealth Cyber Initiative, Coastal Virginia
CompTIA
Comtech Telecommunications Corp.
Adom Cooper
Craig Newmark Philanthropies
Crowdstrike
CSC 2.0, Foundation for Defense of Democracy
Cyber Future Foundation
Cyber Pop-up
Cyber Readiness Institute
Cyber Warrior Network
Cyber.org
Cyberbit
Cybergenic Systems, LLC
CyberVista
CYBERWORKERZ
CyberWyoming
Dakota State University
DARK Enterprises
Daytona State College
Deloitte Services LP
Duke Energy
ESOP Advisors, Inc.
Fordham University, Center for Cybersecurity
Fortinet
Fusion Cyber
Georgetown University, Center for Security and Emerging Technology
Georgia Institute of Technology, School of Cybersecurity and Privacy
Girls Who Code
Grindstone PBC
Hacking the Cyber Threat
Haiku, Inc.
Harvard University, Belfer Center for Science and International Affairs
Holy Cross College and Consortium, Cybersecurity Workforce Certificate Training Program
Howard Community College
Huvr Inc.
IBM
Idaho National Laboratory
Idaho State University
Immersive Labs
Information Technology Industry Council
ISACA
Coretta Jackson and Sovereign Newell
Javilud
Leidos
Lightcast
The Linux Foundation

★ ★ ★ ★ ★ ★

Ryan Louie
LucidCoast
ManTech Advanced Systems International, Inc.
MassCyberCenter
Metropolitan State University of Denver
Microsoft
Middle Georgia State University
MITRE
Moraine Valley Community College (MVCC), Education Pathway National Center (EPNC)
National Academy of Public Administration
National Association of Black Journalists
National Cyber Scholarship Foundation
National Cybersecurity Alliance
National Intelligence University
Naval Postgraduate School
New America
NextGen Cyber Talent
Npower
Jonathan Obar
Okta, Inc.
Orca Intelligence
Pacific Northwest National Laboratory
Palo Alto Networks
Per Scholas
Peraton
Pluralsight
The Presidents Forum
Project Cyber
Protection Group International (PGI)
Purdue University Northwest, Center for Cyber Security
RAND
Right to Be
Salesforce
SANS
SAP America, Inc.
SecurityScorecard
Siemens Energy, Inc.
Sinclair Community College
SkillStorm
Socratic Arts
Space ISAC
Jon Stivers
TeraDact
ThriveDX
Tiffin University, Center for Cyber Defense and Forensics
The Accelerated Training Program (T-ATP)
Trellix
Tufts University, The Fletcher School
UC Berkeley Center for Long-Term Cybersecurity, the Consortium of Cybersecurity Clinics
United Cybersecurity Alliance
University of Alabama in Huntsville, Center for Cybersecurity Research and Education
University of Maryland Global Campus, Center for Security Studies
University of North Carolina Wilmington
University of Pittsburgh, Swanson School of Engineering
University of South Florida, the Florida Center for Cybersecurity (aka "Cyber Florida")
University of Washington Bothell
University of West Florida, Center for Cybersecurity
U.S. Marine Corps
VetsinTech
Vmware
WalkMe
Tom Woods
Women in Cybersecurity (WiCyS)
Workday

★ ★ ★ ★ ★ ★

Notes

[1] Cyberspace is defined here as "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (https://csrc.nist.gov/glossary/term/cyberspace).
[2] The cyber workforce includes those who securely design, build, and operate information technology (IT) and operational technology (OT), as well as those who analyze, protect, and defend cyberspace resources. It encompasses those who work in the frequently overlapping fields of technology manufacturing, software development, IT, OT and industrial control systems (ICS), cybersecurity, cyberspace operations, cyber investigations and prosecutions, certain intelligence community roles, and related research and development. The cyber workforce also includes those who support work in these fields through activities that include governance, risk management, law, compliance, public policy, strategy and planning, privacy, insurance, acquisitions, procurement, and workforce management and development. This paragraph draws on the definitions of "cyberspace workforce" and "cyberspace enabler workforce" used by the Department of Defense, DoDD 8140.01, "Cyberspace Workforce Management," October 5, 2020, pp. 11–12, as well as the NICE Framework.
[3] "Bipartisan Infrastructure Law (BIL)" https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf
[4] As used in this strategy, the term "good jobs" refers to the principles articulated by the Department of Labor and the Department of Commerce in "The Good Jobs Initiative" (https://www.dol.gov/general/good-jobs/principles).
[5] "National Cybersecurity Strategy," March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
[6] "(ISC)² Cybersecurity Workforce Study, 2022," p. 8, ISC2-Cybersecurity-Workforce-Study.ashx.
[7] "Cybersecurity Supply/Demand Heat Map," Cyber Seek, https://www.cyberseek.org/heatmap.html (accessed September 29, 2022).
[8] "(ISC)² Cybersecurity Workforce Study, 2022," p. 8, ISC2-Cybersecurity-Workforce-Study.ashx.
[9] Amanda Bergson-Shilcock and Roderick Taylor, with Nye Hodge, "Closing the Digital Skill Divide," National Skills Coalition, February 2023, p. 4, https://nationalskillscoalition.org/wp-content/uploads/2023/02/NSC-DigitalDivide_report_Feb2023.pdf.
[10] Amanda Bergson-Shilcock, "The New Landscape of Digital Literacy," National Skills Coalition, May 2020, p. 4, https://nationalskillscoalition.org/wp-content/uploads/2020/12/05-20-2020-NSC-New-Landscape-of-Digital-Literacy.pdf.
[11] Stephen Ezell, "Assessing the State of Digital Skills in the U.S. Economy," Information Technology and Innovation Foundation, November 29, 2021, https://itif.org/publications/2021/11/29/assessing-state-digital-skills-us-economy/.
[12] Niam Yaraghi and Samantha Lai, "How the Pandemic Has Exacerbated Online Privacy Threats," Brookings, January 13, 2022, https://www.brookings.edu/blog/techtank/2022/01/13/how-the-pandemic-has-exacerbated-online-privacy-threats//; the definition of "digital resilience" used in this strategy can be found at Digital US Coalition, "Building a Digitally Resilient Workforce: Creating On-Ramps to Opportunity," May 2020, p. 6, https://digitalus.org/wp-content/uploads/2020/06/DigitalUS-Report-pages-20200602.pdf.
[13] Amanda Bergson-Shilcock and Roderick Taylor, with Nye Hodge, "Closing the Digital Skill Divide," National Skills Coalition, February 2023, https://nationalskillscoalition.org/resource/publications/closing-the-digital-skill-divide/.
[14] Diego Deleersnyder, Jaime Fall, Victoria Prince, and Martena Reed, "10 Things We Learned About Digital Skills During the Pandemic," Aspen Institute, June 2022, https://www.aspeninstitute.org/wp-content/uploads/2022/06/10-Things-We-Learned-About-Digital-Skills-During-the-Pandemic.pdf.
[15] The following description borrows from and modifies the Federal definition of a science, technology, engineering, and mathematics (STEM) education ecosystem; "Progress Report on the Implementation of the Federal STEM Education Strategic Plan," December 2021, p. 4, n. 5, https://www.whitehouse.gov/wp-content/uploads/2022/01/2021-CoSTEM-Progress-Report-OSTP.pdf.
[16] Diverse stakeholders include learners (students, job seekers, and employees), employers, labor organizations, educators and academic institutions, training providers, government at all levels, non-profit organizations, philanthropists, and civic organizations

★ ★ ★ ★ ★ ★

[17] Multisector partners should be united by a common vision of cyber education and workforce development, and engaged in collaboration, public-private partnerships, information sharing and problem solving to expand access to cyber learning opportunities
[18] These strategies and long term plans must advance accessible, inclusive cyber learning opportunities across multiple education stages and career pathways.
[19] Opportunities are necessary to successfully enter into cyber careers from education and training programs that embrace not only science, technology, engineering, and mathematics (STEM), but also business, social sciences, law the humanities, and other disciplines;
[20] A successful ecosystem approach requires continuous evaluation and improvement of education and workforce development activities;
[21] Communication and transparency builds support and advance best practices;
[22] Experiential learning that develops technical skills as well as other professional skills needed in the workplace broaden the on-ramps to cyber careers by enabling students of different backgrounds and majors to learn cyber skills
[23] "Workforce Development," U.S. Department of Commerce, https://www.commerce.gov/issues/workforce-development.
[24] Initiatives that provide potential models include the Carolina Cyber Network, https://www.carolinacybernetwork.net/; CyberVirginia, https://www.cyberva.virginia.gov/; and the MassCyberCenter, https://masscybercenter.org/.
[25] U.S. Department of Energy, "National Cyber-Informed Engineering Strategy," June 2022, https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf. See also the 2021 NIST update to Special Publication 800-160, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final.
[26] This strategy uses the definitions of these terms found in EO 14035, "Executive Order on Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce," June 25, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/25/executive-order-on-diversity-equity-inclusion-and-accessibility-in-the-federal-workforce/.
[27] Jason Reed and Jonathan Acost-Rubio, "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce," (ISC)² Global Information Security Workforce Study, 2018, https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx.
[28] Katherine W. Phillips, "How Diversity Makes Us Smarter," *Scientific American*, October 1, 2014, https://www.scientificamerican.com/article/how-diversity-makes-us-smarter/.
[29] David Rock and Heidi Grant, "Why Diverse Teams Are Smarter," *Harvard Business Review*, November 4, 2016, https://hbr.org/2016/11/why-diverse-teams-are-smarter.
[30] "Delivering Through Diversity," McKinsey & Company, https://www.mckinsey.com/about-us/diversity/overview; and "Diversity Wins: How Inclusion Matters," McKinsey & Company, May 19, 2020,https://www.mckinsey.com/~/media/mckinsey/featured%20insights/diversity%20and%20inclusion/diversity%20wins%20how%20inclusion%20matters/diversity-wins-how-inclusion-matters-vf.pdf. See also Robin J. Ely and David J. Thomas, "Getting Serious About Diversity," *Harvard Business Review*, November–December 2020, https://hbr.org/2020/11/getting-serious-about-diversity-enough-already-with-the-business-case.
[31] "(ISC)² Cybersecurity Workforce Study, 2022," p. 32, ISC2-Cybersecurity-Workforce-Study.ashx.
[32] This strategy uses the definition of "underserved communities" found in EO 13985, "Executive Order On Advancing Racial Equity and Support for Underserved Communities Through the Federal Government," January 20, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/. See also EO 14091, "Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government." 2023-03779.pdf (govinfo.gov)
[33] Estimate provided to ONCD by (ISC)², April 2023.
[34] Women in Cybersecurity and Aleria, "Executive Summary: The State of Inclusion of Women in Cybersecurity, 2023," https://www.wicys.org/wp-content/uploads/2023/03/Executive-Summary-The-State-of-Inclusion-of-Women-in-Cybersecurity.pdf.

★ ★ ★ ★ ★ ★

[35] Irving Lachow, "Diversity in the Cyber Workforce: Addressing the Data Gap," MITRE, January 28, 2022, https://www.mitre.org/news-insights/publication/diversity-cyber-workforce-addressing-data-gap. This use of "tech" occupations draws on the Standard Occupational Classification Codes (SOC) for IT occupations. See CompTIA, *State of the Tech Workforce: Cyberstates 2022*, 2022, p. 156, https://www.cyberstates.org/pdf/CompTIA_Cyberstates_2022.pdf.
[36] CompTIA, *State of the Tech Workforce: Cyberstates 2022*, 2022, p. 10, https://www.cyberstates.org/pdf/CompTIA_Cyberstates_2022.pdf.
[37] Center on Rural Innovation, "Where are all the tech jobs in rural America, and where could we see more of them?" (May 2022), ruralinnovation.us/blog/where-are-tech-jobs-in-rural-america/.
[38] "Persons with a Disability: Labor Force Characteristics—2022," Bureau of Labor Statistics News Release, February 23, 2023, https://www.bls.gov/news.release/pdf/disabl.pdf; see also Sally Lindsay et al., "A Systematic Review of the Benefits of Hiring People with Disabilities," *Journal of Occupational Rehabilitation* 28 (2018): 634–55, https://pubmed.ncbi.nlm.nih.gov/29392591/.
[39] As an example, see Bradley Hague, "The Value of Thinking Differently: MITRE's Neurodiversity@Work's Inclusive Outreach," MITRE, April 2,2, 2022, https://www.mitre.org/news-insights/impact-story/value-thinking-differently-mitres-neurodiversityworks-inclusive-outreach.
[40] During the drafting of this strategy, the National Initiative for Cybersecurity Education went through a rebranding and is now known simply by the program name "NICE."
[41] Each of NICE's strategic plans are available at https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan.
[42] "The Workforce Framework for Cybersecurity (NICE Framework)," Applied Cybersecurity Division / NICE, NIST, https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice.
[43] "DoD Cyber Workforce Framework," DoD Cyber Exchange, https://public.cyber.mil/wid/dcwf/.
[44] The following entities are members of the NCWCG, which is chaired by ONCD: the Office of Management and the Budget, the National Security Council, the Domestic Policy Council, the Office of Science and Technology Policy, the National Economic Council, the Department of State, the Department of the Treasury, the Department of Defense, the Department of Justice, the Department of Commerce, the Department of Education, the Department of Labor, the Department of Energy, the Department of Homeland Security, the Department of Transportation, the Department of Veterans Affairs, the Office of the Director of National Intelligence, the General Services Administration, the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, the National Security Agency, the National Institute for Science and Technology, the Office of Personnel Management, and the National Science Foundation.
[45] Defined by the American Library Association Digital Literacy Task Force, as quoted in "Launching a Digital Literacy Accelerator: An Overview and Lessons Learned," Office of Educational Technology, U.S. Department of Education, p. 1, https://tech.ed.gov/files/2022/10/DLA_Report_Launching_Digital_Literacy_Accelerator.pdf.
[46] White House Office of Science and Technology Policy, "2022 Progress Report on the Implementation of the Federal STEM Education Strategic Plan," January 2023, p. 12, https://www.whitehouse.gov/wp-content/uploads/2023/02/Final_2022_CoSTEM_Progress_Report.pdf.
[47] Digital US Coalition, "Building a Digitally Resilient Workforce: Creating On-Ramps to Opportunity," May 2020, p. 6, https://digitalus.org/wp-content/uploads/2020/06/DigitalUS-Report-pages-20200602.pdf.
[48] For more on digital inclusion plans, see "Five Digital Inclusion Trends in the United States," National Telecommunications and Information Administration, U.S. Department of Commerce, https://ntia.gov/blog/five-digital-inclusion-trends-united-states.
[49] Digital US homepage, https://digitalus.org/.
[50] "10 Transformation Pathways for States," National Governors Association, https://www.nga.org/futureworkforce/pathways/close-technological-and-digital-literacy-gaps/.
[51] "Open Knowledge Network: Summary of the Big Data IWG Workshop, October 4–5, 2017," Executive Office of the President of the United States, https://www.nitrd.gov/pubs/Open-Knowledge-Network-Workshop-Report-2018.pdf.
[52] "Digital Skills in Pennsylvania," Opendata PA, https://data.pa.gov/stories/s/PA-Digital-Literacy-Programs/bry2-xj2e.
[53] "Welcome to the State Digital Equity Scorecard," https://digital-skills-map.digitalinclusion.org/.

★ ★ ★ ★ ★ ★

[54] "Presidential Youth Fitness Program," Office of Disease Prevention and Health Promotion, U.S. Department of Health and Human Services, https://health.gov/our-work/nutrition-physical-activity/presidents-council/programs-awards/presidential-youth-fitness-program.
[55] "Declaration for the Future of the Internet," U.S. Department of State, https://www.state.gov/declaration-for-the-future-of-the-internet.
[56] "The Summit for Democracy," U.S. Department of State, https://www.state.gov/summit-for-democracy/.
[57] "Sustainable Development Goals," United Nations, https://www.un.org/sustainabledevelopment/education/.
[58] "Regional Innovation Engines," National Science Foundation, https://beta.nsf.gov/funding/initiatives/regional-innovation-engines.
[59] "Secure and Trustworthy Cyberspace (SaTC)," National Science Foundation, https://new.nsf.gov/funding/opportunities/secure-trustworthy-cyberspace-satc.
[60] "Regional Technology and Innovation Hubs (Tech Hubs)," U.S. Economic Development Administration, U.S. Department of Commerce, https://www.eda.gov/funding/programs/regional-technology-and-innovation-hubs.
[61] "RAMPS Communities," Information Technology Laboratory / Applied Cybersecurity Division, NIST, https://www.nist.gov/itl/applied-cybersecurity/nice/regional-alliances-and-multistakeholder-partnerships-stimulate-ramps.
[62] "CTE CyberNet Academies," Perkins Collaborative Resource Network, U.S. Department of Education, https://cte.ed.gov/initiatives/cte-cybernet-academies.
[63] "Competency-Based Learning or Personalized Learning," Office of Elementary & Secondary Education, U.S. Department of Education,https://oese.ed.gov/archived/oii/competency-based-learning-or-personalized-learning/.
[64] "Welcome to the Consortium: Cybersecurity for the Public Good," the Consortium of Cybersecurity Clinics, https://cybersecurityclinics.org/.
[65] "RING: Regions Investing in the Next Generation," Center of Academic Excellence in Cybersecurity Community, https://caecommunity.org/initiative/k12-ring.
[66] "Cybersecurity Education and Training Assistance Program," NICCS: National Initiative for Cybersecurity Careers and Studies, Cybersecurity and Infrastructure Security Agency, https://niccs.cisa.gov/cybersecurity-career-resources/cybersecurity-education-and-training-assistance-program.
[67] "Advanced Technological Education (ATE)," National Science Foundation, https://beta.nsf.gov/funding/opportunities/advanced-technological-education-ate.
[68] "Raise the Bar: Unlocking Career Success," U.S. Department of Education, https://cte.ed.gov/unlocking-career-success/.
[69] GenCyber program homepage, https://www.gen-cyber.com/.
[70] "Secure and Trustworthy Cyberspace (SaTC)," National Science Foundation, https://new.nsf.gov/funding/opportunities/secure-trustworthy-cyberspace-satc.
[71] "CyberCorps: Scholarship for Service," U.S. Office of Personnel Management, https://sfs.opm.gov/.
[72] "The T3 Innovation Network," U.S. Chamber of Commerce Foundation, https://uschamberfoundation.org/t3-innovation; Credential Engine homepage, https://credentialengine.org/; Open Skills Network homepage, https://openskillsnetwork.org/.
[73] "U.S. Department of Education Green Ribbon Schools," U.S. Department of Education, https://ed.gov/programs/green-ribbon-schools.
[74] "Presidential Cybersecurity Education Award," Perkins Collaborative Resource Network, U.S. Department of Education, https://cte.ed.gov/cyberaward.
[75] NICCS: National Initiative for Cybersecurity Careers and Studies homepage, https://niccs.cisa.gov/.
[76] "Cybersecurity Competency Model," Competency Model Clearinghouse, U.S. Department of Labor, Employment and Training Administration, https://www.careeronestop.org/CompetencyModel/Competency-Models/cybersecurity.aspx.
[77] WorkforceGPS homepage, https://www.workforcegps.org/.
[78] "Education & Training," NICCS: National Initiative for Cybersecurity Careers and Studies, Cybersecurity and Infrastructure Security Agency, https://niccs.cisa.gov/education-training.
[79] "Cybersecurity Education and Training Providers," CyberSeek, https://www.cyberseek.org/training.html.
[80] "Free and Low Cost Online Cybersecurity Learning Content," Information Technology Laboratory / Applied Cybersecurity Division, NIST, https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content.

★ ★ ★ ★ ★ ★

[81] "Workforce Development," U.S. Department of Commerce, https://www.commerce.gov/issues/workforce-development.
[82] "The Good Jobs Initiative: Department of Commerce and Department of Labor Good Job Principles," U.S. Department of Labor, https://www.dol.gov/general/good-jobs/principles.
[83] "Raise the Bar: Unlocking Career Success," U.S. Department of Education, https://cte.ed.gov/unlocking-career-success.
[84] CyberSeek homepage, https://www.cyberseek.org.
[85] Amanda Bergson-Shilcock, "The New Landscape of Digital Literacy," National Skills Coalition, May 2020, https://nationalskillscoalition.org/wp-content/uploads/2020/12/05-20-2020-NSC-New-Landscape-of-Digital-Literacy.pdf.
[86] "Business Roundtable Launches New Cybersecurity Workforce Corporate Initiative," Business Roundtable, December 8, 2022, https://www.businessroundtable.org/business-roundtable-launches-new-cybersecurity-workforce-corporate-initiative.
[87] Brad Smith, "American Faces a Cybersecurity Skills Crisis: Microsoft Launches National Campaign to Help Community Colleges Expand the Cybersecurity Workforce," Official Microsoft Blog, October 28, 2021, https://blogs.microsoft.com/blog/2021/10/28/america-faces-a-cybersecurity-skills-crisis-microsoft-launches-national-campaign-to-help-community-colleges-expand-the-cybersecurity-workforce/.
[88] As an example, see "Gain Cybersecurity Apprenticeship Experience with Apprenticeship Opportunity from LaGuardia and Mastercard!," LaGuardia Community College, https://www.laguardia.edu/uploadedfiles/main_site/content/home/news/lagcc-mastercard.pdf.
[89] "AT&T Invests $1 Billion in Employee Reskilling," UpskillAmerica: Aspen Institute, March 12, 2018, https://www.aspeninstitute.org/of-interest/upskilling-news-att-invests-1-billion-employee-reskilling/.
[90] "IBM Tackles Talent Shortage and Cybersecurity Crisis with New and Expanded Partnerships," IBM Newsroom, May 10, 2022, https://newsroom.ibm.com/2022-05-10-IBM-Tackles-Talent-Shortage-and-Cybersecurity-Crisis-with-New-and-Expanded-Partnerships.
[91] "Career Readiness," JPMorgan Chase, https://www.jpmorganchase.com/impact/our-approach/jobs-and-skills/career-readiness.
[92] "R&D Workforce Training: Federal Agencies' STEM Internships, Scholarships, and Training Opportunities," Networking and Information Technology Research and Development (NITRD), https://www.nitrd.gov/STEM4ALL/.
[93] "O*NET Online," U.S. Department of Labor, https://www.onetonline.org.
[94] "The Good Jobs Initiative: Department of Commerce and Department of Labor Good Jobs Principles," U.S. Department of Labor, https://www.dol.gov/general/good-jobs/workers/good-jobs; "Workforce Development," U.S. Department of Commerce, https://www.commerce.gov/issues/workforce-development.
[95] "Veterans Employment and Training Service," Veterans' Employment and Training Service, U.S. Department of Labor, https://www.dol.gov/agencies/vets.
[96] CyberSkills 2Work homepage, National Centers of Academic Excellence in Cybersecurity, https://cyberskills2work.org/i/.
[97] "VA for Vets," Veteran and Military Spouse Talent Engagement Program (VMSTEP), https://www.vaforvets.va.gov/.
[98] GFCE (Global Forum on Cyber Expertise) homepage, https://thegfce.org/.
[99] "Securing a Nation: Improving Federal Cybersecurity Hiring in the United States," Burning Glass Technologies, 2021, https://www.datocms-assets.com/62658/1661873045-securing_nation_federal_cybersecurity_hiring1.pdf.
[100] "President's Management Agenda: Priority 1: Strategy 1," performance.gov, General Services Administration, May 2023, https://www.performance.gov/pma/workforce/strategy/1/.
[101] "Trusted Workforce 2.0," performance.gov, General Services Administration, https://www.performance.gov/trusted-workforce/.
[102] CIO Council, "Future of the Federal IT Workforce Update," May 2020, https://www.cio.gov/assets/resources/Future_of_Federal_IT_Workforce_Update_Public_Version.pdf; women represent about 26% of the Federal cyber workforce and 44% of the entire Federal workforce (2020–2022 OPM FedScope; figures provided by OPM, February 2023).

★ ★ ★ ★ ★ ★

[103] As of early 2023, only 17% of IT Specialist announcements used a second assessment to assess skills (data provided by OPM). Agencies can track progress at GSA's D2D (Data to Decisions) Hiring Assessment and Selection Outcome Dashboard at https://d2d.gsa.gov/report/hiring-assessment-and-selection-outcome-dashboard.
[104] Kiran A. Ahuja, Director, U.S. Office of Personnel Management, memorandum, "Guidance Release – E.O. 13932; Modernizing and Reforming the Assessment and Hiring of Federal Job Candidates," May 19, 2022, https://chcoc.gov/content/guidance-release-eo-13932-modernizing-and-reforming-assessment-and-hiring-federal-job.
[105] Laura Bate and Mark Montgomery, "Workforce Development Agenda for the National Cyber Director," CSC 2.0, June 2022, https://cybersolarium.org/wp-content/uploads/2022/05/CSC2.0_Report_WorkforceDevelopmentAgenda_FullText.pdf; National Academy for Public Administration, "A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation," January 2022, https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf.
[106] President Joseph R. Biden Jr., "Memorandum on Revitalizing America's Foreign Policy and National Security Workforce, Institutions, and Partnerships," February 4, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/04/memorandum-revitalizing-americas-foreign-policy-and-national-security-workforce-institutions-and-partnerships/.
[107] Cyber Workforce Dashboard," U.S. Office of Personnel Management, https://www.opm.gov/data/data-products/cyber-workforce.
[108] "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs," GAO-19-144, U.S. Government Accountability Office, March 12, 2019, https://www.gao.gov/products/gao-19-144.
[109] Both scholarship programs serve multiple valuable purposes. For example, SFS encourages participating institutions to adopt best practices in education, training, community impact, and workforce development, as well as conduct valuable research in these areas, through NSF's grant process. The program also helps meet the needs of SLTT governments and participating institutions of higher education, as a small portion of SFS Scholars are able to fulfill their service obligations by working for these entities. The DoD's CYSP supports workforce development and retention as well as new entrants into government service.
[110] Federal Internship Portal," USAJOBS, U.S. Office of Personnel Management, https://intern.usajobs.gov.
[111] "Homeland Security Careers," U.S. Department of Homeland Security, https://www.dhs.gov/homeland-security-careers/icdf.
[112] "DOE Omni Technology Alliance Internship Program," Oak Ridge Institute for Science and Education, https://orise.orau.gov/doe-omni/index.html.
[113] "HSI HERO Child-Rescue Corps," U.S. Immigration and Customs Enforcement, https://www.ice.gov/hero.
[114] "Build a Brighter Future," U.S. Digital Corps, U.S. General Services Administration, https://digitalcorps.gsa.gov/.
[115] "Cyber Fellowship," U.S. Department of Justice, https://www.justice.gov/legal-careers/cyber-fellowship.
[116] "Navigate to an Apprenticeship," USMAP: United Services Military Apprenticeship Program, U.S. Department of Defense, https://usmap.osd.mil/.
[117] DOD SkillBridge homepage, https://skillbridge.osd.mil.
[118] "Veteran Employment Through Technology Education Courses (VET TEC)" https://www.va.gov/education/about-gi-bill-benefits/how-to-use-benefits/vettec-high-tech-program/
[119] "Veteran Readiness and Employment (VRE) program" https://www.benefits.va.gov/vocrehab/
[120] "Securing a Nation: Improving Federal Cybersecurity Hiring in the United States," Burning Glass Technologies, 2021, p. 23, https://www.datocms-assets.com/62658/1661873045-securing_nation_federal_cybersecurity_hiring1.pdf.
[121] EO 13932, "Modernizing and Reforming the Assessment and Hiring of Federal Job Candidates," June 26, 2020, https://www.govinfo.gov/content/pkg/FR-2020-07-01/pdf/2020-14337.pdf; and Kiran A. Ahuja, Director, U.S. Office of Personnel Management, memorandum, "Guidance Release – E.O. 13932; Modernizing and Reforming the Assessment and Hiring of Federal Job Candidates," May 19, 2022, https://chcoc.gov/content/guidance-release-eo-13932-modernizing-and-reforming-assessment-and-hiring-federal-job.
[122] "Cybersecurity Talent Initiative," Go Government: Partnership for Public Service, https://gogovernment.org/fellowship/cybersecurity-talent-initiative/.

★ ★ ★ ★ ★ ★

[123] U.S. Office of Personnel Management, "Guide to Internships, Fellowships, Apprenticeships, and Other Programs," January 2023, https://chcoc.gov/sites/default/files/Guide%20to%20Internships%20Fellowships%201-19-2023.pdf.
[124] "Federal Internship Portal," USAJOBS, U.S. Office of Personnel Management, https://intern.usajobs.gov/Search/Results?hp=student&wt=15328&s=salary&sd=desc&p=1.
[125] To date, only about 6% of cyber job postings by departments and agencies have included this NICE work role information (data provided by OPM).
[126] OPM's efforts have already produced shared hiring certificates for IT Product Manager, GS-2210-14, 15 (Originating Agency: DHS- CISA), and Human-Centered Designer, GS-2210-14, 15 (Originating Agency: DHS-CISA).
[127] "Securing a Nation: Improving Federal Cybersecurity Hiring in the United States," Burning Glass Technologies, 2021, p. 23, https://www.datocms-assets.com/62658/1661873045-securing_nation_federal_cybersecurity_hiring1.pdf.
[128] In addition, the NICE Framework includes competency areas, which are defined as "a cluster of related Knowledge and Skill statements that correlates with one's capability to perform Tasks in a particular domain." Competency areas can help learners discover areas of interest, inform career planning and development, identify gaps for knowledge and skills development, and provide a means of assessing or demonstrating a learner's capabilities in the domain.
[129] U.S. Department of Defense, "DoD Cyber Workforce Strategy, 2023–2027," March 1, 2023, https://dodcio.defense.gov/Portals/0/Documents/Library/CWF-Strategy.pdf.
[130] "Federal Virtual Training Environment (FedVTE)" https://fedvte.usalearning.gov/
[131] "CyberVets Program" https://www.cms.gov/about-cms/careers-cms/cms-cybervets-program

[133] For example, in fiscal year 2019, only 320 IT Specialists out of the more than 84,000 eligible benefited from student loan repayments. As a second example, critical pay authority is currently available for 800 positions, and only 47 have been used (data provided by OPM).
[134] Recently, the Secretary of Homeland Security and the Attorney General have been granted the authority (by sec. 401 of the Abolish Trafficking Reauthorization Act of 2022, Public L. No. 117-347, 136 Stat. 6199 (2023)) to provide increased incentive pay to DHS and Department of Justice employees identified as possessing cyber skills. As of this writing, these authorities have not yet been implemented.
[135] "Cyber Career Pathways Tool," NICCS: National Initiative for Cybersecurity Careers and Studies, https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool.
[136] Kiran A. Ahuja, Director, U.S. Office of Personnel Management, memorandum, "Guidance for Implementing Federal Rotational Cyber Workforce Program," March 17, 2023, https://chcoc.gov/content/guidance-implementing-federal-rotational-cyber-workforce-program.
[137] OPM tip sheets are available at https://www.opm.gov/policy-data-oversight/future-of-the-workforce/cybersecurity-hiring-resource-hub/memo-attachment-2-infographic-48.pdf; an executive playbook that outlines hiring authorities available to agencies can be found at https://chcoc.gov/sites/default/files/TalentSurgeHiringAuthorities.pdf; and the cybersecurity hiring resource hub is at https://www.opm.gov/policy-data-oversight/future-of-the-workforce/cybersecurity-hiring-resource-hub/.
[138] Defined by American Library Association Digital Literacy Task Force, as quoted in "Launching a Digital Literacy Accelerator: An Overview and Lessons Learned," Office of Educational Technology, U.S. Department of Education, p. 1, https://tech.ed.gov/files/2022/10/DLA_Report_Launching_Digital_Literacy_Accelerator.pdf.
[139] White House Office of Science and Technology Policy, "2022 Progress Report on the Implementation of the Federal STEM Education Strategic Plan," January 2023, p. 12, https://www.whitehouse.gov/wp-content/uploads/2023/02/Final_2022_CoSTEM_Progress_Report.pdf.
[140] White House Office of Science and Technology Policy, "2022 Progress Report on the Implementation of the Federal STEM Education Strategic Plan," January 2023, p. 12, https://www.whitehouse.gov/wp-content/uploads/2023/02/Final_2022_CoSTEM_Progress_Report.pdf.
[141] Digital US, "Building a Digitally Resilient Workforce: Creating On-Ramps to Opportunity," May 2020, p. 6, https://digitalus.org/wp-content/uploads/2020/06/DigitalUS-Report-pages-20200602.pdf.
[142] "The Office of the National Cyber Director Requests Insight and Expertise on Cyber Workforce, Training, and Education: An RFI & Virtual Reverse Stakeholder Day Effort," https://www.whitehouse.gov/wp-content/uploads/2022/10/ONCD-Workforce-and-Education-RFI.pdf.