National Cyber Workforce and Education Strategy

Initial Stages of Implementation

JUNE 25, 2024

★ ★ ★ ★ ★ ★

Cyber Workforce Strategy Advances National Security and Connects Americans to Good-Paying Jobs.

First-of-its-kind plan removes barriers to entering the cyber workforce.

INTRODUCTION

The National Cybersecurity Strategy (NCS), released by President Biden on March 1, 2023, positions the United States and its allies and partners to build a digital ecosystem that is more defensible, more resilient, and better aligned with our values. The National Cyber Workforce and Education Strategy (NCWES), published by the White House Office of the National Cyber Director (ONCD) on July 31, 2023, charts a course for fostering White House–level coordination to meet cyber workforce demand. It fulfills the need to create a skills-based digital future in which workers have access to good-paying, meaningful jobs in cyber within their communities.

Demand for cyber workers exceeds the current capacity of workforce development and education systems. This challenge is compounded by the dynamic nature of the national security environment and the rapid acceleration of global crises, new technologies, and novel threats. To meet these challenges, the guiding imperatives in the NCWES aim to broaden the appeal of cyber careers to more Americans, transition to skills-based hiring and talent development approaches, and encourage the development of cyber workforce and education ecosystems. These imperatives are driving the implementation of the strategy to respond to the most immediate need to fill the hundreds of thousands of open cyber positions, improve data on the Federal and national cyber workforce, and transition to skills-based hiring and talent development approaches.

The Federal Government is one part of the whole-of-nation approach outlined in the NCWES. It is necessary for the public and private sectors as well as academia to do their part to effect change at scale. The content of this report includes the actions being taken by Federal departments and agencies to strengthen the Federal cyber workforce and support cyber workforce development and education though existing Federal programs. The initiatives and accomplishments in this report are a direct result of action by the Biden-Harris Administration to prioritize and initiate changes to support the goals of the NCWES. ONCD, in close partnership with the Office of Personnel Management (OPM) and Office of Management and Budget (OMB), among others, is leading by example, coordinating efforts to expand and enhance the Federal cyber workforce and education efforts through public and private sector actions. For example, the Administration is working to expand the pipeline for cyber workers by reducing barriers and improving the efficiency of Federal hiring processes. These Federal actions are supported by private sector commitments to educate, hire, and train the growing cyber workforce. The commitments, included in Appendix A,

demonstrate the need and interest for involvement and bring resources from organizations positioned to lead change.

In fulfilling its responsibility to drive cohesion across the Federal Government and the larger cyber community, ONCD has worked with workforce and education stakeholders in the public and private sectors to introduce new approaches to expand and enhance the national cyber workforce. In collaboration with Federal departments and agencies, ONCD is coordinating efforts in accordance with the President's Management Agenda and National Security Memorandum 3, "Revitalizing America's Foreign Policy and National Security Workforce, Institutions, and Partnerships," as well as aligning the cyber workforce efforts with other Federal initiatives such as Workforce Hubs, Tech Hubs, and Technology and Innovation Partnerships.

Industry, educational institutions, training providers, community organizations, philanthropies, and government at all levels must collaborate extensively to expand and enhance the cyber workforce, and must transform education to make progress at scale. The Administration is committed to working with stakeholders to meet the demand for cyber workers. Implementation of the NCWES is in its early stages, and ONCD has begun to track outcomes as initiatives progress. The content of this report details Federal departments' and agencies' ongoing efforts to execute the NCWES and outlines upcoming activities that will be included in the first full implementation report, anticipated to be released in the fall of 2025.

EMBARKING ON FEDERAL ACTION

Cyber education and workforce development have not kept pace with demand and with the rapid pace of technological change. In 2023, ONCD met with a range of public and private sector stakeholders across industries, academic disciplines, and nonprofit organizations to better focus its implementation efforts for the NCWES and to emphasize the need for cyber skills in all occupations and industries. The actions that departments and agencies have taken to implement the NCWES and begin to lay the groundwork for implementation are described in what follows.

Whole-of-government approach addresses Federal cyber workforce needs

Federal departments and agencies are aligning Federal investments in the national workforce, infrastructure, and economy to have a greater impact on the development of the cyber workforce. In early 2023, ONCD established the National Cyber Workforce Coordination Group (NCWCG) and the Federal Cyber Workforce Working Group (FCWWG), co-chaired with OMB in consultation with OPM, to help advance the work that needs to be completed to implement the NCWES. In November 2023, to expedite these efforts, two more groups were established under the NCWCG: the Working Group on Cyber Workforce and Education and the Working Group on Cyber Skills and Awareness. More than 35 Federal departments and agencies in these groups have begun implementing the objectives in the NCWES.

Federal agencies pivot to skills-based hiring and talent development

As the Biden-Harris Administration continues to encourage employers to adopt skills-based approaches, it is also taking a major step to lead by example. On April 29, 2024, the National Cyber Director announced that the Administration is modernizing the Federal hiring process. OPM is leading the transition of the Information Technology (IT) Management series, called the 2210 series, to skills-based hiring principles and practices. The 2210 job series represents IT workers in every Federal agency and a majority of the Federal IT workforce, accounting for nearly 100,000 current Federal employees. Aligned with broader strategic hiring objectives, this modernization effort will include the use of Registered Apprenticeship programs.

Additionally, the Federal Government made a similar commitment to Federal contractors who work shoulder to shoulder with and support Federal employees every day, with an announcement from the Department of Energy on its effort to pivot toward skills-based hiring in IT and cyber contracts.

In 2023, OPM, in consultation with OMB and ONCD, developed a cyber workforce legislative package intended to bring equity across the Federal Government with improved hiring and pay flexibilities, including greater emphasis on skills-based hiring and increased incentives for high-demand cyber skills. The OPM package describes actions to increase skills-based hiring and talent development in Federal Government cyber roles. It outlines new authorities, personnel flexibilities, and requirements to align Federal cyber positions with the NICE Framework and the DoD Cyber Workforce Framework, where applicable. The proposed legislation is also intended to aid in transitioning to skills-based approaches from relying solely on minimum education requirements, and to support a holistic talent management strategy across the Federal Government.

To further support skills-based practices, ONCD is working with OMB to encourage wider adoption of Section 39.104 of the Federal Acquisition Regulation, which states that when information technology services are being acquired, solicitations must not describe any minimum experience or educational requirement for contracted personnel.

In addition to advancing skills-based practices, departments and agencies in the FCWWG have begun to identify barriers and opportunities to increase the efficiency of Federal hiring processes. Although modifying Federal process will span multiple years, solutions are already in development, including pooled hiring processes, harmonization of cyber workforce frameworks, increased participation in scholarship-for-service programs, and expansion of the National Center of Academic Excellence in Cybersecurity (NCAE-C) program.

Tech to Gov Working Group (TTGWG) lands cyber talent for the Federal Government

Launched and led by OPM in July 2023, TTGWG is a workstream of the FCWWG. On April 18, 2024, OPM held a second Tech to Gov fair, where more than 1,700 attendees registered, representing 50 states. Applicants participated in 1,746 one-on-one conversations with over 100 agency representatives. To date, the Tech to Gov initiative has resulted in 150 tentative job offers to

experienced cyber professionals to increase the strength of Federal cyber workforce. A fourth Tech to Gov fair is scheduled for fall of 2024.

Federal programs provide rigorous cyber learning opportunities

Prior to the release of the NCWES, Federal programs in cyber workforce and education, including the NCAE-C program, led by the National Security Agency (NSA); the CyberCorps®: Scholarship for Service (SFS) program, led by the National Science Foundation (NSF) and OPM; the Department of Defense (DoD) Cyber Service Academy (DoD CSA); the Cybersecurity Education and Training Assistance Program (CETAP), led by the Cybersecurity and Infrastructure Security Agency (CISA); and NICE, led by National Institute of Standards and Technology (NIST), were already reinforcing the importance of sustained Federal investments by establishing a foundation for cyber workforce and education program development to provide a pipeline of qualified cyber talent. ONCD meets with departments and agencies multiple times per week to coordinate related actions and reduce duplication of efforts.

Designation as an NCAE-C is a mark of distinction for colleges and universities that highlights a commitment to advancing the cybersecurity capabilities of the Nation. This prestigious recognition reflects the dedication of an NCAE-C to higher standards for rigorous academic instruction, ongoing faculty development, leadership in the cybersecurity field, alignment with cutting-edge technologies, and engagement in cyber workforce and education ecosystem efforts. The NCAE-C program goes beyond accreditation as it sets the gold standard for cybersecurity education that maps to the NICE Framework.

CISA manages the Federal Cyber Defense Skilling Academy, which provides full-time Federal employees an opportunity to focus on professional growth through an intense, full-time, three-month accelerated training program. The Federal Cyber Defense Skilling Academy currently offers courses to prepare for the positions of Cyber Defense Analyst, Cyber Defense Forensics Analyst, Cyber Defense Incident Responder, and Vulnerability Assessment Analyst.

CISA also launched a Neurodiverse Federal Workforce (NFW) Initiative in fiscal year 2024 to increase opportunities for neurodiverse individuals who are on the autism spectrum. The 15-month NFW Initiative will place interns in operations research analysis, IT management, and management and program analysis roles in CISA and will enable CISA to better support its neurodistinct employees. Information gathered through the NFW Initiative can be used by CISA and the broader community to implement similar initiatives and ultimately help respond to the need for skilled cyber workers.

Opportunities to develop national cyber workforce and education systems have also been identified in Federal economic investments such as those directed by the Bipartisan Infrastructure Law (BIL), Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act, American Rescue Plan Act (ARP), and Inflation Reduction Act (IRA), in addition to existing workforce development, economic development, and education programs.

★ ★ ★ ★ ★ ★

A list of Federal cyber workforce and education programs is included in Appendix B.

Cyber workforce and education programs emphasize cyber across disciplines

ONCD, together with its public and private sector partners, is leveraging Federal programs as part of a concerted approach to incorporate cyber content and skills across academic, occupational, and industrial disciplines. For example, to increase access to apprenticeships in fields such as cybersecurity, in 2023 the Department of Labor (DOL) awarded approximately $108 million through grants and contracts to expand Registered Apprenticeships in high-growth and in-demand industries. DOL, in coordination with ONCD and the Departments of Commerce, Homeland Security, and Defense and other federal agencies, conducted a cyber apprenticeship sprint. DOL also announced the availability of nearly $200 million in grants to continue to support public-private partnerships that expand, diversify, and strengthen Registered Apprenticeships in education, care, clean energy, IT, supply chain, other in-demand industries. These funding opportunities demonstrate the commitment of the Administration to strengthen the national workforce development infrastructure and connect people in all communities to good jobs in cyber.

In June 2024, ONCD participated in the Cyber Across Disciplines (CyAD) conference in Chicago, Illinois, which convened college and university faculty in cyber. The CyAD conference provided an opportunity to encourage the integration of cybersecurity across academic disciplines and industry sectors, as well as incorporating cybersecurity in computer science, artificial intelligence (AI), and emerging technology curricula in an effort to promote secure-by-design principles.

Cyber Clinics provide hands-on learning for students while serving local communities

NSA, through grants to NCAE-C institutions, launched Cyber Clinics in Nevada, Minnesota, Louisiana, and Virginia. Cyber Clinics support communities and small governments that would otherwise not have access to cyber risk assessment and planning assistance, and they provide an opportunity for over 200 students to develop competencies while in a supervised learning environment. The Cyber Clinics model has garnered more than $25 million in private sector investment that has enabled the opening of clinics at 45 more institutions.

Shared job postings and hiring pools reduce delays in recruiting Federal cyber talent

OPM is providing agencies with candidates who have ready-to-use hiring certificates to reduce delays in hiring qualified cyber talent. This year, OPM provided hiring lists for IT Product Manager, IT Specialist, IT Specialist (Data Management), and Program Analyst (Data Analytics) positions. Additionally, to support the AI talent surge, OPM launched a pooled hiring action for Data Scientists under the Government-wide direct hire authority. Recently, 181 qualified Data Scientist candidates were made available to agencies.

Outreach engagements lift best practices and connect local and regional stakeholders

Since the release of NCWES last year, ONCD has launched a national workforce road show to help amplify the Biden-Harris Administration's workforce growth priorities; highlight needs, solutions,

and progress; and engage and promote cyber workforce and education ecosystems of stakeholders across all industry sectors.

These events have been held in collaboration with partners such as Members of Congress, Governors, and mayors as well as private and public sector stakeholders to expand the cyber workforce in Arizona, Florida, Georgia, Illinois, Maryland, Michigan, Nevada, North Carolina, Ohio, Oklahoma, Pennsylvania, Tennessee, Texas, Virginia, and Washington.

Beyond the road show, ONCD has also participated in numerous events with academia, industry, employers, and community organizations to help change how communities approach cyber workforce development and education.

Federal departments respond to cyber workforce demands

The Federal departments and agencies actively participating in the implementation of the NCWES are producing deliverables that respond to the challenges facing cyber workforce and education. Together, the initiatives represent a comprehensive plan to begin addressing the most immediate needs in developing a skilled and resilient cyber workforce that is able to protect our nation, economy, and society while providing pathways into good-paying jobs.

The whole-of-government approach led by the Administration has resulted in numerous commitments and initiatives from the following departments and agencies to increase cyber hiring and talent development in the Federal Government and provide support for expanding the cyber workforce:

Cybersecurity & Infrastructure Security Agency (CISA)
Department of Commerce (DOC)
Department of Defense (DoD)
Department of Housing and Urban Development (HUD)
Department of Labor (DOL)
Department of State (DOS)
Department of Transportation (DOT)
Department of the Treasury (Treasury)
Department of Veterans Affairs (VA)
National Science Foundation (NSF)
National Security Agency (NSA)
Office of Personnel Management (OPM)
Office of the National Cyber Director (ONCD)
Small Business Administration (SBA)

A detailed list of commitments and initiatives led by Federal agencies is included in Appendix A. In addition to the agencies making specific commitments, all of the Federal agencies that are participating in the implementation of the NCWES are listed in Appendix C.

★ ★ ★ ★ ★ ★

Agencies expand educational pathways into the Federal Government

ONCD is collaborating with the Federal agencies administering key cyber workforce and education programs including NCAE-C, SFS, and the DoD CSA. Together with CISA, DoD, NIST, NSA, NSF, and OPM, ONCD is working to expand the pipeline to meet the demand for cyber workers in the Federal Government. Designation of a college or university as an NCAE-C establishes eligibility for additional resources, recognizes the rigor of the cyber curricula, and increases access for more students to enter cyber education programs.

For example, in fiscal year 2024, 104 colleges and universities participated in the SFS and DoD CSA programs. This figure represents a 6.1% increase in participating institutions over fiscal year 2023. Additionally, in fiscal year 2024, 50 institutions of higher education are expected to receive their initial NCAE-C designation and 80 will renew their designations, bringing the total number of NCAE-C institutions to nearly 500—a 13% increase from 440 participating schools in fiscal year 2023.

The SFS, DoD CSA, and NCAE-C programs play a major role in creating a pipeline for the Federal cyber workforce, and the Administration, through ONCD, intends to build on these successes. The full list of NCAE-C institutions is included in Appendix D.

The Administration elevates Federal cyber workforce efforts across the Government

The NCWES implementation is one part of the effort led by the Administration to enhance the capacity of the Federal cyber workforce to protect the Nation, economy, and society. ONCD is leading coordination across agencies to align and harmonize Federal investments and initiatives. The following efforts are broader than the cyber workforce, but their continued progress and success has bolstered cyber workforce enhancement and expansion.

The President's Management Agenda (PMA) has prioritized attracting and hiring the most qualified employees who reflect the diversity of our country and is striving to make every Federal job a good job, where all employees are engaged, supported, heard, and empowered. The Administration is reimagining the Federal workforce of the future, informed by national workforce trends, as it seeks to make the Government a model employer to deliver effectively on a broad range of agency missions. OPM recently released a workforce of the future playbook to support agencies in implementing key initiatives such as using pooled hiring, emphasizing skills-based hiring, attracting early career talent, fostering an inclusive work environment, and other approaches to strengthen the ability of agencies to recruit, hire, and retain a workforce with the skills need to fulfill their missions. To that end, OPM has initiated a skills-based hiring training course to train Federal hiring professionals on how to reframe recruitment and retention efforts in terms of the skills needed to successfully perform work roles rather than relying solely on college degrees.

Under the Trusted Workforce 2.0 initiative led by the Security, Suitability, and Credentialing Performance Accountability Council (PAC), the average amount of time needed to complete a security clearance background investigation has fallen from 411 to 155 days for a Top Secret and

173 to 53 days for a Secret clearance. Agencies have also been encouraged to clear personnel with clean records for onboarding on the basis of the highest-value background checks, known as a preliminary determination. The PAC is working to expand this practice by implementing ambitious targets of 45 days for Top Secret and 25 days for Secret clearances. In the second quarter of fiscal year 2024, over 27,000 new hires were cleared using preliminary determinations.

National Security Memorandum 3 (NSM-3) has driven an increase in paid internship, scholarship-for-service, and fellowship programs and an expansion of efforts to recruit and retain a diverse national security and foreign policy workforce from all segments of our society. These programs are paramount to strengthening the Federal cyber workforce.

The 2024 President's Cup Cybersecurity Competition drew competitors from more than 100 agencies across the Federal Government, including finalist teams and individuals from the Army, Navy, Air Force, Marines, DoD, NSA, and FBI. In its fifth iteration, the President's Cup Cybersecurity Competition saw an increase in participation over the previous competition, and it introduced a new Industrial Control Systems Escape Room that challenged and expanded the opportunities for success beyond those typically seen at cyber competitions. CISA invited the top five team finalists and the top three individual winners from each track to the awards ceremony held at the White House in May 2024. CISA and ONCD plan to continue conducting the awards ceremony at the White House to encourage more participation.

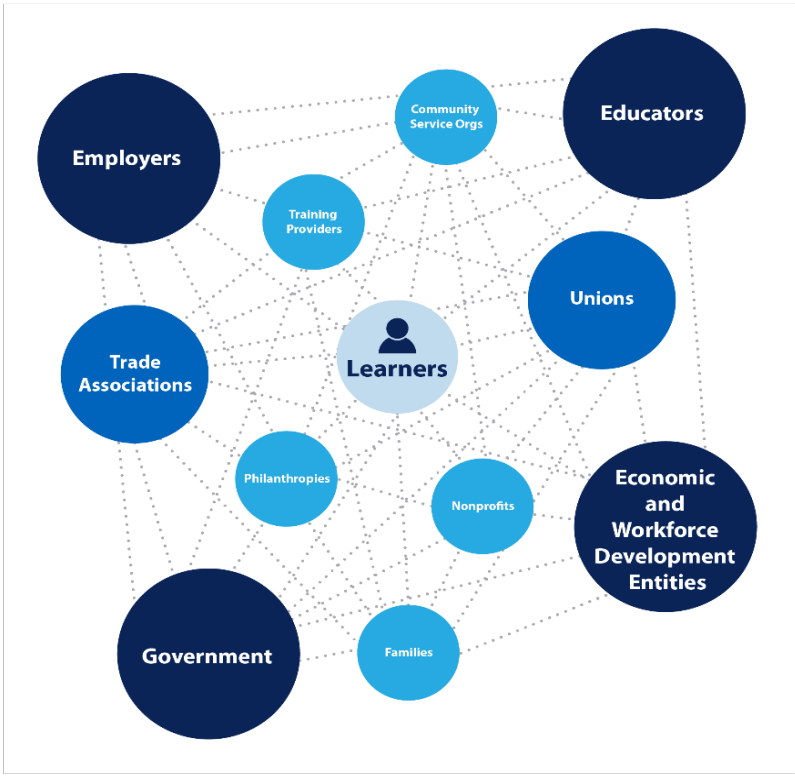
In fiscal year 2024, the Administration has been combining efforts from the NCWES and the President's Executive Order 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," to launch AI, Cyber, and Tech Hiring Surge initiatives. Departments and agencies have identified common talent needs and coordinated hiring actions for AI, cyber, and other in-demand technology roles in order to provide a pool of candidates for consideration by multiple employing agencies, saving time and cost for agencies, job applicants, and taxpayers.

To assist military-connected families, OPM has reinforced the use of flexible work arrangements that support the needs of military-connected families, including telework and remote work, administrative leave, and workforce retention tools such as the opportunity to request reassignment and relocation. Federal agencies can leverage Executive Order 14100, "Advancing Economic Security for Military and Veteran Spouses, Military Caregivers, and Survivors," to expand the reach of Federal cyber workforce recruitment efforts.

On March 6, 2024, President Biden issued Executive Order 14119, "Scaling and Expanding the Use of Registered Apprenticeships in Industries and the Federal Government and Promoting Labor-Management Forums," to meet employers' needs while investing in workers' skills, reducing employment barriers, and promoting job quality, equity, inclusion, and accessibility for the benefit of the Federal Government and the Nation. Federal agencies are leveraging this executive order to broaden avenues to good-paying cyber jobs and improve access to opportunities for workers underrepresented in the cyber workforce.

NON-FEDERAL GOVERNMENT ACTIONS

The ecosystem approach to cyber workforce and education proposed in the NCWES that no single stakeholder alone can achieve change at the scale required to meet today's urgent need to fill cyber career positions. Engagement of organizations beyond the cyber sector are critical if employer demand for skilled cyber workers is to be met. ONCD is developing a cyber workforce and education ecosystem playbook for publication in fall 2024 that will help stakeholders understand, create, and navigate their ecosystems. This playbook will draw on expertise from the private sector.



Example of a Cyber Workforce and Education Ecosystem

Together with departments and agencies, ONCD is coordinating Federal efforts to incubate and expand effective models in order to leverage the strengths of ecosystems to increase the quality and quantity of cyber professionals in the workforce.

As an introduction to this work, the NCWES provides examples of cyber workforce and education ecosystems across the country. Though their structure, governance, and leadership may vary, model cyber education and workforce development ecosystems should be focused on learners, such as students, job seekers, adults, and employees at the center of a network of active stakeholders—including employers, unions, educators, training providers, governments, nonprofit organizations, philanthropists, and civic organizations. Ecosystem stakeholders are united by a common vision of education and workforce development. This connection helps foster accessible, inclusive learning opportunities across education stages and career pathways. State, local, tribal, and territorial governments are important members of cyber workforce and education ecosystems. Successful ecosystems have sustainability and succession plans to ensure that funding and leadership can weather economic and political pressures.

★ ★ ★ ★ ★ ★

Employers and educators expand the cyber workforce nationwide

Stakeholder collaboration is critical to success. As the Federal Government stepped up to do its part, over 100 organizations—including philanthropies, technology companies, professional associations, and academic institutions—answered the call. They made voluntary commitments that included providing $95 million in investments, hiring 13,000 workers, and training one million individuals in cyber. These commitments are often spotlighted at ONCD outreach events across the country.

The following are examples of some stakeholder commitments; Appendix A gives a more detailed list. A version that is continually updated can be found on the White House website, https://whitehouse.gov/cyberworkforce.

- Over $100 million to support cybersecurity workforce development, education, tools, and services.
- High school students can take up to 30 credits of university-level computer science coursework as dual-credit through a statewide program to assist rural populations in public, private, and tribal schools, as well as those who are home-schooled.
- Over 50,000 students engaged in gamified learning, with up to 5,000 receiving training and certification scholarships, and more than $9.2 million in training and certification scholarships to 500+ individuals to drive increased participation in cybersecurity training across the nation.
- Up to 200 small water utilities are receiving cybersecurity training to help secure the nation's water infrastructure from cyber threats, improve their cybersecurity risk management, and enhance their ability to respond to and recover from a cybersecurity incident.
- Free cyber training for human resources (HR) professionals to better understand the nuances of hiring cyber workers.
- $5 million to support and expand cybersecurity and open-source security ecosystems, including work to ensure that the next generation is informed and motivated to engage across these technologies.
- Training in foundational cyber skills to be provided to 5 million girls by 2025, along with access to free cybersecurity education, training, and resources for up to 10 million micro, small, and medium-sized businesses by 2025.

★ ★ ★ ★ ★ ★

FUTURE OUTLOOK

The Biden-Harris Administration will continue to drive change in the public and private sectors through engagement and collaboration. Filling the hundreds of thousands of cyber job vacancies across America is a national security imperative and a top priority to help prepare our country to lead in the digital economy.

Through the FCWWG, ONCD will work with Federal departments and agencies to reach their hiring goals for the Federal cyber workforce in fiscal years 2024 and 2025. This effort relies on the continued improvement of data on the Federal cyber workforce.

ONCD, in collaboration with OPM and the FCWWG, will facilitate a hiring surge to fill open Federal cyber positions in fiscal year 2024 and conduct cyber sprints to generate job offers. Over the next year, as the Federal Government works to expand the use of skills-based hiring and talent development for Federal cyber positions and contracts, previously underutilized members of the national cyber workforce will have on-ramps to the good-paying Federal cyber jobs that are needed to help secure the nation's defenses and infrastructure and to help support Federal programs.

The NCWCG and its working groups will connect with constituents across the country to amplify the value of cyber workforce and education ecosystems and identify stakeholders willing to make additional voluntary commitments in fiscal years 2024 and 2025. Ecosystems and models that elevate opportunities for learners will be highlighted, and assistance for community champions seeking to spark, support, or scale an ecosystem will be included in a cyber workforce and education ecosystem guide to be compiled by ONCD.

As part of its strategic outreach, the Administration will work with stakeholders to conduct cyber career fairs, with particular focus on populations underrepresented in the cyber workforce—including women, people of color, veterans, transitioning service members, military spouses, members of rural communities, and individuals with disabilities.

Collectively, the initiatives and activities that the Federal Government is pursing in the next two years are intended to respond to the critical need for cyber workers; increase skills-based hiring, talent development, and education nationwide; address barriers faced by Federal and non-Federal stakeholders; proactively analyze and monitor the changing labor demand for cyber skills; and continue to advance our cyber posture, national security, economy, and society.

ONCD will monitor and report on the progress of the actions that are aligned to objectives in the NCWES to develop a qualified and diverse cyber workforce, meet the demand for cyber workers in the Federal Government, encourage skills-based approaches to cyber workforce development, and transform education systems to increase access to cyber learning opportunities.

To strengthen the Federal cyber workforce, Federal departments and agencies will work to increase adoption of skills-based hiring and assessment in the Federal Government and make improvements

in recruitment, hiring, retention, and talent development processes. This effort includes expanding work-based learning on-ramps into Federal employment, increasing the use of flexible and innovative Federal hiring and pay practices, and improving training programs for Federal HR professionals.

The Administration will be working with Federal departments and agencies to identify cyber workforce development and education program best practices, update online resources, and elevate cyber careers through a coordinated national call to action.

Initiatives in fiscal year 2024 will also seek to expand learning opportunities in foundational cyber skills and increase the capacity of K-12 systems and institutions of higher education to teach rigorous cybersecurity content. To boost the participation of students and educators in cyber scholarship programs, Federal departments and agencies will work with academia to expand concurrent credit transfer and articulation opportunities for academic credit, further integrate cyber across academic disciplines, and increase the availability of low-cost and no-cost cyber training and education curricula.

Together with private sector stakeholders, the Administration will encourage the use of skills-based approaches by employers and increase work-based learning opportunities.

The Administration will leverage the collective strength of all Federal departments and agencies to increase participation and promote the value of veterans, separating service members, and military spouses in the cyber workforce.

The whole-of-nation approach presented in the NCWES will require the combined efforts of every cyber workforce and education ecosystem stakeholder to enable all Americans to benefit from the enormous potential of our interconnected future.

★ ★ ★ ★ ★ ★

APPENDIX A

Cyber Workforce and Education Commitments

The whole-of-nation strategy outlined in the National Cyber Workforce and Education Strategy (NCWES) cannot be achieved without the participation of stakeholders in the private sector and academia. Stakeholders demonstrate their participation in the form of commitments. The commitments listed below reflect the actions taken to support the initial implementation of the NCWES. The most current version of this list, updated as new commitments are received, can be found online at https://whitehouse.gov/cyberworkforce.

Federal Departments and Agencies

College of Information and Cyberspace (CIC) at National Defense University (NDU)

Beginning in fall 2024, admissions eligibility to the CIC at NDU will expand to include senior noncommissioned officers (NCOs) serving in the U.S. military on Active Duty or in the National Guard. Offerings will feature tuition-free cyber workforce programs, including a part-time master of science (M.S.) degree and various graduate certificates.

Cybersecurity & Infrastructure Security Agency (CISA)

Each October, CISA's Cybersecurity Awareness Month offers a focused opportunity to engage the public, businesses, and other national and international organizations, providing essential cybersecurity tips and other information as well as tools, occasions for public engagement, and more for audiences at all levels. In 2022, Cybersecurity Awareness Month garnered more than 1,400 media mentions and included more than 120 CISA-wide speaking engagements (from CISA leadership), six regional trips, 111 social media posts with more than one million impressions, 7,300 downloads of the Partner Amplification Toolkit, and 108,000 page views of the 2022 landing page. Throughout the year, CISA encourages diversity in the current and future cyber workforce, exposes young people to careers in cybersecurity, and bridges the current cyber gap experienced by women in cybersecurity and tech through partnerships with groups such as Girl Scouts of the USA, Girls Who Code, and Women in CyberSecurity (WiCyS). CISA also manages a Federal Cyber Defense Skilling Academy to help civilian Federal employees develop cyber defense skills through training in the baseline knowledge, skills, and abilities of a Cyber Defense Analyst (CDA).

Department of Commerce (DOC)

Through the National Institute of Standards and Technology (NIST), the National Initiative for Cybersecurity Education (now NICE) program is charged with energizing, promoting, and coordinating a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development. It launched the Cybersecurity Career Ambassador Program to create a network of "ambassadors" to prepare, grow, and sustain the

cybersecurity workforce. The Ambassador Program supports the NICE Strategic Plan by helping to build cybersecurity career awareness and expanding a national workforce that is both knowledgeable and skilled in cybersecurity. Over the next year, the Ambassador Program aims to identify over 200 ambassadors across the United States.

Department of Commerce (DOC)

NICE will award up to $3.6 million for Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) cybersecurity education and workforce development projects. The Notice of Funding Opportunity for RAMPS is open to organizations that will bring together employers and educators to develop a skilled workforce to meet industry needs within a local or regional economy. NIST may fund up to 18 RAMPS awards. Additionally, in cooperation with Katzcy, a digital marketing firm, NIST supports the U.S. Cyber Games to recruit, train, and develop the team representing the United States in international cybersecurity competitions. This program engages with over 2,000 individuals in the yearly U.S. Cyber Open and annually trains over 150 students though months-long U.S. Cyber Combine and Pipeline programs.

Department of Commerce (DOC)

The National Telecommunications and Information Administration (NTIA) highlighted the work of the Connecting Minority Communities program, which is part of the Biden-Harris Administration's Internet for All initiative that will connect everyone in America with affordable, reliable high-speed internet. The program specifically directs $268 million from the Consolidated Appropriations Act of 2021 for expanding high-speed internet access and connectivity to Historically Black Colleges and Universities (HBCUs), Tribal Colleges and Universities (TCUs), and Minority-Serving Institutions (MSIs) for the purchase of broadband internet access and eligible equipment, or to hire and train information technology personnel.

Department of Defense (DoD)

The DoD Cyber Service Academy (DoD CSA), formerly the DoD Cyber Scholarship Program, provided scholarship offers to more than 165 Americans in 2024 and aims to maintain a 17% increase per year. These scholarships assist the U.S. Government in promoting higher education in all cyber disciplines, enhance DoD's ability to recruit and retain cyber specialists, increase the number of military and civilian personnel in DoD with cyber expertise, and ultimately enhance the Nation's cyber posture. The program is a result of commitments from DoD and Congress to support higher education as a means to prepare the DoD workforce to combat threats against the Department's critical information system and networks.

Department of Housing and Urban Development (HUD)

HUD joined the Cybersecurity Talent Initiative in July 2023 and joined with the Partnership for Public Service to enhance the early career talent pipeline and recruitment effort. HUD's Office of the Chief Information Security Officer (OCISO) is collaborating across all HUD Program Offices to get at least 50 placements in the next fiscal year. This initiative will offer participants a cybersecurity

and information technology pathway into HUD by removing as many socioeconomic barriers as possible. Participants will be provided opportunities to gain Federal employment and hands-on job experience in an immersive environment while learning about HUD's mission, operations, and culture.

Department of Labor (DOL)

The Department of Labor announced $66.9 million in formula and competitive grants to 46 states and territories under the State Apprenticeship Expansion program to develop and scale registered apprenticeship programs in cybersecurity and other critical sectors. Seven of these states and territories identified cybersecurity as one of their targeted sectors. DOL also made a competitive award to Utah to support the expansion of Registered Apprenticeship Programs for cybersecurity and other sectors. In addition, the Department announced an agreement with several Registered Apprenticeship industry intermediaries that will focus on launching, promoting, and expanding Registered Apprenticeship programs in cybersecurity.

Department of Labor (DOL)

DOL announced the availability of nearly $200 million in grants to support public-private partnerships that expand, diversify, and strengthen Registered Apprenticeships in education, care, clean energy, information technology (IT), supply chain, and other in-demand industries. The funding opportunity includes $95 million of competitive grants through the second round of the Biden-Harris Administration's Apprenticeship Building America Grant Program and $100 million in the second round of State Apprenticeship Expansion Formula Grants. The announced funding opportunities continue the Department of Labor's commitment to providing all of America's workers with access to training and career preparation that leads to good jobs with family-sustaining wages. These grants serve as another avenue toward strengthening the Nation's workforce development infrastructure to connect people from all communities to the good jobs being created by President Biden's Investing in America agenda.

Department of State (DOS)

The Department of State is using special hiring authority granted by the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (P.L. 117-263, Sec. 9502) to accelerate hiring for up to 25 personnel into cyber positions within the Bureau of Cyberspace and Digital Policy (CDP). In furtherance of the Secretary's Modernization Agenda, CDP has partnered with the Department's Foreign Service Institute to train more than 200 employees in the Cyber and Digital Policy Tradecraft course by the end of 2024, thereby enabling placement of a trained cyber/digital officer engaged on these issues at every overseas mission.

Department of Transportation (DOT)

In service of its mission to support and continually improve national transportation infrastructure within the modern, digital environment, DOT is committed to attracting, developing, and retaining

cybersecurity and information technology talent. This effort includes leveraging the diverse backgrounds and accrued experience of veterans and their families. The DOT Office of the Chief Information Officer is using two recruitment programs, the Partnership for Public Service's Cybersecurity Talent Initiative and the Pathways Internship Program, which provide both on-site and virtual opportunities for training and mentorship that prepare participants for lifetime careers in the IT industry. In FY24, DOT commits to increase its paid internship slots from 3 to 12; it continues to enable participants to identify a cybersecurity and information technology pathway, and to convert eligible interns into full time employees.

Department of the Treasury (Treasury)

Treasury is partnering with Google on a new skills-based hiring and cloud certificate training program, designed to identity and attract cyber talent. Focused on cloud security, the program includes custom-built courses that reflect cyber workforce demands at Treasury and other Federal departments and agencies. The courses will also be available to current Treasury employees, equipping the Treasury workforce with key cybersecurity skills.

Department of Veterans Affairs (VA)

VA announced a Cybersecurity Apprenticeship Program for Veterans: a two-year developmental program within the VA Cybersecurity Operations Center (CSOC) to provide a unique, hands-on learning and development experience for cybersecurity apprentices and to encourage a career in the Federal cybersecurity workforce. Program apprentices will develop cyber knowledge and experience through mentoring, on-the-job training, and leading-edge training courses. The program is a Registered Apprenticeship with the Department of Labor and will begin recruiting and onboarding its first cybersecurity apprenticeship cohort in Q3 FY24. The first cohort will consist of approximately 5 transitioning veterans coming from tech-specific Military Occupational Specialties (MOS), with the hopes of increasing capacity to 10. In addition, VA authorized a special salary rate (SSR) for its technology and cybersecurity personnel in the 2210-Information Technology, 1550-Computer Science, and 0854-Computer Engineering occupational series. This is an important step toward closing the growing gap between industry and Federal Government salary rates for technology and cybersecurity roles. The SSR represents an average increase of 17% in basic pay for members of VA's highly skilled technical workforce who are dedicated to providing veterans and their families with the world-class benefits they have earned.

National Centers of Academic Excellence in Cybersecurity (NCAE-C)

There are currently 450 institutions designated by the NSA as National Centers of Academic Excellence in Cybersecurity (NCAE-C). The NCAE-C program was created in 1999, and in 2024 the National Security Agency (NSA) will be furthering its commitment to high-quality cybersecurity education by increasing the number of Minority-Serving Institutions designated as NCAE-Cs by 10, including at least one HBCU.

★ ★ ★ ★ ★ ★

National Science Foundation (NSF)

NSF is investing over $53M in CyberCorps®: Scholarship for Service (SFS) awards over the next four years. These awards are intended to support the development of a robust and resilient cybersecurity workforce by addressing the unique challenges around recruiting and retaining cybersecurity professionals for careers serving local, state, Federal, or tribal governments. Awards have been made to Florida Atlantic University, University of Delaware, University of Nevada Las Vegas, Brigham Young University, Loyola University of Chicago, Boise State University, George Washington University, University of Alabama Huntsville, California State Polytechnic University at Pomona, Rochester Institute of Technology, University of Arizona, University of Maryland–College Park, and Norwich University.

National Science Foundation (NSF)

NSF announced $1.5 million in supplemental funding to support, identify, and implement strategies that have been shown to be effective in attracting, retaining, and graduating students in cybersecurity advanced degree programs who identify as women, Black, African American, Latino(a), Hispanic, or Indigenous. In addition, NSF announced the Jump Start in Cyber Program for Students at Historically Black Colleges and Universities (HBCUs) and Predominately Black Institutions (PBIs), a no-cost, six-week cybersecurity program targeting undergraduate students who attend HBCUs and PBIs.

National Science Foundation (NSF)

NSF is looking to invest in the Bridge to Cyber initiative to provide an estimated 500 individuals with no background in cybersecurity, including those from populations historically marginalized in tech/cyber, the opportunities to earn advanced degrees in cybersecurity.

National Security Agency (NSA)

In the fall of 2023, National Center of Academic Excellence in Cybersecurity (NCAE-C) grants will launch a pilot initiative of four new Cyber Clinics to open in Nevada, Minnesota, Louisiana, and Virginia. The Cyber Clinics will support communities and small governments that would otherwise not have access to cyber risk assessment and planning assistance and will provide an opportunity for over 200 students to develop competencies while in a supervised learning environment. NSA also expects by the end of 2024 to increase the number of NCAE-C institutions to 460, which will serve a projected 174,000 students annually. NSA also sponsors GenCyber summer camps each year, with a goal of at least 100 camps across the country, serving 2,800 students and 600 teachers.

Office of Personnel Management (OPM)

OPM collaborated with Federal agencies, the Chief Human Capital Officers (CHCO) Council Recruitment and Outreach Working Group, and external stakeholder groups to host a third Tech to Gov Job Fair on April 18, 2024, with a fourth fair planned for the fall of 2024. Further, OPM is conducting an occupational study to establish or update one or more occupational series covering

★ ★ ★ ★ ★ ★

Federal Government positions in the fields of software development, software engineering, data science, and data management. OPM will explore digital careers work in the Federal Government to determine workforce needs and policy requirements supporting a Federal digital careers workforce. This study will identify the nature and scope of digital careers work and the skills needed to perform such work Government-wide. The results of the study will affect how Federal agencies attract, hire, and retain digital career professionals Government-wide. OPM's Tech to Gov Working Group is also partnering with the U.S. Digital Service to support tech hiring across Government and to cultivate a pipeline of skilled tech talent recruitment representatives, regardless of their job series.

Office of the National Cyber Director (ONCD)

ONCD is committed to increased recruiting and outreach to underrepresented communities, such as women, people of color, and people with disabilities, to highlight internship opportunities in the Federal Government. ONCD has traveled across the country and met with members of communities underrepresented in the cyber workforce to emphasize the need for skilled cyber workers from all backgrounds. ONCD will identify unique outreach channels with a focus on reaching underrepresented communities and will create dedicated recruitment materials by the intern application season of summer 2024.

Small Business Administration (SBA)

SBA pledged to incorporate cybersecurity content into outreach and engagement programs, including those that support Black entrepreneurs and small businesses. These engagement programs include SBA's alliance with the National Pan-Hellenic Council, SBA Community Navigators, SBA Cybersecurity for Small Business Pilot grant program, and the SBA Cyber Summit, which launched in October 2023.

Non-Federal Organizations

ISC2

ISC2 (the International Information System Security Certification Consortium), an organization that provides training and certifications for cybersecurity professionals, will provide a minimum of 25,000 individuals working in advanced manufacturing with its foundational "Certified in Cybersecurity" certification exam and free training to help address the sector's critical cybersecurity skills gap. ISC2 will also introduce a series of 10 virtual forums over the next two years to explore solutions to the cybersecurity workforce challenges impacting the nation's advanced manufacturing sector.

★ ★ ★ ★ ★ ★

ISC2

ISC2 achieved a significant milestone in its current pledge for one million individuals to receive ISC2's new "Certified in Cybersecurity" certification. To date, over 265,000 people have enrolled, and more than 27,000 individuals achieved this entry-level certification in less than 10 months.

Accenture

Accenture is a global professional services company committed to reducing traditional barriers to employment and finding ways to increase pathways into cybersecurity roles. Accenture and Immersive Labs are partnering to fill one million entry-level jobs in the next decade by providing a free, robust cybersecurity platform that not only trains participants but also engages them in reality-based exercises to improve their skills, which unlocks jobs with hiring organizations within the platform. Recognizing the need for all people to have cyber skills regardless of their roles, Accenture will provide cybersecurity training to more than 700,000 of its people in the next year. Accenture has met its goal to fill 20% of entry-level roles from its apprenticeship program and is on track to achieve its 2025 goal of a gender-balanced workforce.

Access Living

Access Living is committed to launching an Independent Living Technology Program to address the gap in digital skills in the disability community, with the goal of reaching 150 disabled participants by the end of 2024. Participants will identify an independent living goal to achieve by using technology, such as looking for work, going through job training, or accessing information and services. They will then attend Access Living's disability-centered technology training course and receive one-on-one support. Upon completion of the program, participants who need it will be given their own laptop or tablet and a year of free internet access. Funding for this program is in part from a Federal grant. Access Living is also committed to expanding its consulting and training services to include a team of certified digital accessibility specialists, all of whom have disabilities themselves. The team aims to improve internet and digital product accessibility not just for Access Living's clients but overall, by centering lived experience with disability in its consultation, evaluation, and remediation of websites, portals, apps, and other digital content and interfaces to ensure that they meet or exceed accessibility standards.

Advocacy Blueprints

Advocacy Blueprints announced the creation of the Cyber Policy Leadership Institute for racially diverse undergraduate and graduate students, with a particular focus on HBCU, MSI, and TCU students. The leadership institute aims to provide students with opportunities to learn about and engage on U.S. and international cybersecurity public policy. The institute will help students and the entire cyber community begin to view policies through a racial equity lens to create solutions that address the evolving cyber threats, while empowering participation from historically underserved

and underrepresented communities. Over the coming months, Advocacy Blueprints will announce recruitment plans, programming, and additional partners.

American University (AU)

AU is committed to strengthening the cybersecurity workforce by continuing to expand access to hands-on cybersecurity training opportunities to all students, regardless of discipline. Through the newly launched Shahal M. Khan Institute for Cyber and Economic Security, and in collaboration with its global technology partner Cyber Range Solutions, AU is transforming cyber education by grounding technical cyber exercises in the context of national security and economic policy. In addition, AU announced its commitment to helping to equip every American with foundational cyber skills.

Aspen Institute

The Aspen Institute's Cybersecurity Program made three commitments that coincided with the release of the National Cybersecurity Workforce and Education Strategy: (1) for cybersecurity education—Aspen will work with American University on a summary of openly availably Government-issued cybersecurity resources; (2) for cybersecurity workforce development—Aspen plans to publish a guidebook on best practices for cybersecurity employee development and retention; and (3) for digital literacy—it will host the Aspen Cyber Summit in November in New York City and online to energize practitioners, students, and the public about cybersecurity issues, policy, opportunities, and more.

Augusta University

Augusta University will leverage a $1 million Regional Innovation Engines Development award from the National Science Foundation to catalyze local academic and industry partnerships around a growing regional cyber workforce; this effort will include supporting expanded training and internship opportunities and transitioning research to practice to foster the creation of new businesses, especially minority- and veteran-owned businesses.

BattleBots

BattleBots is announcing the creation of the Bot Builders Foundation, which will develop and lead the National BattleBots Collegiate and High School Championship. This competition will engage hundreds of students nationwide, commencing in 2024. BattleBots also affirms its special commitment to empowering the local Las Vegas community through initiatives aimed at inspiring and engaging traditionally underrepresented youth in science, technology, engineering, and mathematics (STEM) disciplines. These endeavors will include educational field trips and impactful school visits, with the intention of reaching and positively influencing the lives of over 500 students during the upcoming academic year.

★ ★ ★ ★ ★ ★

BCR Cyber

BCR Cyber, a leading provider of cybersecurity training, testing, certification, and job placement services, has trained, certified, and placed over 2,000 entry-level information technology (IT)/cyber workers with state, local, and industry partners using funding from the Maryland Department of Labor's Employment Advanced Right Now (EARN) grant program. Over the next two years, BCR Cyber commits to train and place an additional 3,000 individuals. BCR also aims to replicate the Maryland EARN model and expand nationally, focusing its initial expansion efforts on Virginia.

Black Cybersecurity Association (BCA)

BCA, a nonprofit organization founded by an HBCU graduate dedicated to facilitating underrepresented minority entry into the U.S. cybersecurity field through training, professional development, and networking, commits to securing gainful employment for 300 African American citizens in calendar year 2024. BCA strives to increase diversity in cybersecurity and works with multiple HBCUs, including Howard University and Morgan State University, as a part of its education and workforce development efforts. BCA plans to expand to additional HBCUs, including schools in Virginia.

Black Tech Street

Microsoft and Black Tech Street have announced an unprecedented long-term alliance for Historic Greenwood, the neighborhood in Tulsa, Oklahoma, nicknamed "Black Wall Street" by Booker T. Washington because of its abundance of affluent Black entrepreneurs. Dubbed "The Digital Transformation of Black Wall Street to Black Tech Street," this long-term alliance aims to restore Greenwood's position as a national hub for Black talent and innovation, with an initial focus on cyber.

Boeing

At Boeing, a leading global aerospace company, the digital revolution has created new demands for technical skills to align with the digital future of work. The Boeing Technical Apprenticeship Program (BTAP) is an accelerated, on-the-job, earn-as-you-learn Registered Apprenticeship development program for those interested in gaining new job-ready technical skills for emerging and in-demand roles. BTAP participants receive paid, relevant work experience and are mentored by industry leaders while acquiring valued skills and on-the-job experiences. After a successful pilot program led to more than 10 high-quality and diverse employees hired across several states, BTAP launched a second cohort in July 2023 and is planning to expand the next round of apprenticeships to directly support Boeing as well as industry partners, preparing employees for jobs in Information Systems Security, Architecture and Cloud Security, Incident Response, and/or Product Security Engineering.

★ ★ ★ ★ ★ ★

Boise State

Boise State University's Institute for Pervasive Cybersecurity commits to expand its "Cyberdome" competency-based cyber education platform to include 8 additional rural K-12 districts across the state, for a total of 12 districts, in alignment with the National Cyber Workforce and Education Strategy. The Cyberdome platform enables 40 Idaho students per year to gain critical cyber competencies before joining the workforce. Employers around the state have commented positively on the students who have already gone through this program. Also, as part of a statewide initiative, the Institute of Pervasive Cybersecurity will work with K-12 school districts to create for students an ecosystem of cyber support and critically needed pathways to cybersecurity careers. This work is expected to engage over 100 students throughout Idaho and introduce them to cybersecurity as a STEM career option. It is also expected to create an ecosystem of capabilities throughout Idaho for all of its citizens. In addition, the Institute for Pervasive Cybersecurity is collaborating with the Idaho Department of Finance to develop statewide cybersecurity and cyber-fraud training for Idaho's senior communities. Further, Boise State and Idaho's Department of Finance are partnering to create focused Digital Diplomacy and Financial Technology Innovation & Cybersecurity certificates to support the state's growing cyber ecosystem.

Capitol Technology University

Capitol Technology University, housed between Washington, DC, and Baltimore, commits to and announces a new initiative to meet the national need for qualified and trained cyber educators by adding to its broad array of cyber education opportunities. Beginning in January 2024, this initiative includes the launch of two new programs: (1) the Doctor of Education (Ed.D.) in Cyber Science and the Master of Education (M.Ed.) in Cyber Science, with 12 students expected to be enrolled between 2024 and 2025, and (2) the creation of a new senior university leadership role focused on implementing an ecosystem approach toward cyber education. This initiative is expected to make Capitol a hub of educating cyber educators that can address the need for such professionals, especially within high schools and community colleges.

Check Point

Check Point Software has committed to training one million individuals in cybersecurity skills by 2028 through its MIND Cyber Security Training Program, which offers free training kits to all educational organizations in the United States. In addition, the MIND Cyber Security Training Program will include training for instructors and teachers through the SecureAcademy program.

Cisco

To ensure that U.S. organizations receive the certification-driven, skills-based training they need to develop their cybersecurity teams and achieve cybersecurity readiness, Cisco has committed to training 200,000 people with cybersecurity skills in the United States by July 2025 through the Cisco Networking Academy. Cisco has also announced new Multicloud Certifications focused on connectivity and security to ensure that IT professionals have the skills to protect companies from

future cyberattacks. In addition to providing security products and solutions, Cisco is addressing the critical need to close the cybersecurity skills gap at all levels by offering a continuum of learning through Cisco Networking Academy and Cisco U. Further, Cisco recently released a new Ethical Hacker course to prepare individuals for cyber offensive roles such as Ethical Hacker and Penetration Tester. For tech professionals who want to reskill or upskill, Cisco Learning & Certifications, including the Cisco U. platform, prepares learners for professional-level certifications up to expert-level bootcamps and role-based skills training. Cisco offers an industry-leading portfolio of technology innovations, with networking, security, collaboration, cloud management, and more.

College of Lake County (CLC)

CLC, in Grayslake, IL, commits to using funds received through a Federal grant to convene a group of 50 manufacturing employers and grow the manufacturing sector by expanding education and training, including cyber skill development, in the second-largest manufacturing county in the state of Illinois. CLC also commits to expanding its Advanced Technology Center (ATC), dedicated to Industry 4.0 training and education, to incorporate critical, complementary workforce needs such as cybersecurity, data analytics, mechatronics, and robotics.

Community College of Allegheny County (CCAC)

CCAC expects to train at least 50 students in advanced manufacturing, building automation systems, and cybersecurity programs in the next year at its recently opened Center for Education, Innovation, and Training, which was completed using funding from President Biden's American Rescue Plan.

CompTIA

CompTIA, a globally recognized advocate and voice for the tech community with industry-leading certifications and courses, launched the CompTIA Cybersecurity Trustmark program in March 2023. This program consists of 177 industry-accepted security safeguards pulled from six global frameworks. Already, there are over 800 managed service providers (MSPs) from 27 countries in the program, and CompTIA is committed to expanding that number to 1,400 by the end of 2024. Additionally, CompTIA Spark, the social impact nonprofit supported by CompTIA, is utilizing free in-school curriculum and other innovative programs to expand the knowledge of possible tech careers among middle school students. With a goal of serving one million students by 2030, CompTIA Spark is helping to build a future pipeline of diverse talent by offering programming that ranges from tech fundamentals to the latest in cybersecurity and other cutting-edge, emerging technologies.

ConSol USA

ConSol USA has innovated a demand-led, "ecosystem of ecosystems" model that engages underutilized talent (such as non-degreed individuals, veterans, women, and people of color) in underserved communities, in line with the imperatives of the National Cyber Workforce and

Education Strategy. ConSol USA has executed initial agreements, and is negotiating with other organizations, reaching a range of academic stakeholders including the University of Texas at San Antonio, George Washington University, and the University of California at Davis. ConSol USA is also engaged with USAA to reach military personnel, veterans, and their families. Through these efforts, ConSol USA is committed to directly hire and deploy a minimum of 11,000 cyber technologists nationally by 2027.

Craig Newmark Philanthropies

Craig Newmark Philanthropies pledged to increase its commitment from $50 million to $100 million to support a broad coalition of organizations dedicated to educating and protecting Americans amid escalating cybersecurity threats. Newmark has donated more than $60 million dollars to organizations focused on raising public awareness of threats and online security choices, in addition to the creation of online tools and digital infrastructure that help secure the country's networks. Newmark's donations will continue to advance nonprofit cybersecurity and education organizations such as BlackGirlsHack, the National Cybersecurity Association's #SeeYourselfInCyber HBCU Tour, National Black Journalists Association, Black Girls Code, and Girl Scouts.

Craig Newmark Philanthropies

Craig Newmark Philanthropies will provide an update on its $100 million commitment towards its Cyber Civil Defense Initiative. In 2023, it doubled its $50 million commitment to cybersecurity causes. It has also issued 11 grants totaling over $12 million to nonprofit organizations with programs that are well-aligned to many of the workforce strategy's key objectives, including cyber capacity building; applied learning opportunities; diversity, equity, and inclusion; digital literacy; and more. This funding builds on the $48+ million Craig Newmark Philanthropies has already delivered to organizations focused on cybersecurity workforce development, education, tools, and services.

CrowdStrike

CrowdStrike will fill 300+ internship positions, fund ten $10,000 scholarships, expand upon its successful SkillBridge apprenticeship program, and continue to offer its "return-to-work" program focused on caregivers by Q1 2025. CrowdStrike is also committed to making training materials and resources more broadly accessible to help upskill users. Further, CrowdStrike continues the development of the Next Generation Leaders Program initially announced at ONCD's roundtable "The State of Cybersecurity in the Black Community" earlier this year, with an anticipated launch during the spring academic semester.

CrowdStrike

Drew Bagley, Vice President & Counsel, Privacy & Cyber Policy–CrowdStrike, has committed to launching a joint initiative with key partners that will empower and create career opportunities for the Nation's next generation of cybersecurity policy professionals through impactful programming

and education connecting minority students and young professionals in the Black community with today's cybersecurity leaders.

Cyber Readiness Institute (CRI)

In August 2023, CRI and Center on Cyber and Technology Innovation (CCTI) will launch the Phased Critical Infrastructure Pilot: Resiliency for Water Utilities, providing up to 200 small water utilities with basic cybersecurity training and promoting a culture of cyber readiness. Microsoft is sponsoring this initiative to help address the challenge of securing the Nation's water infrastructure from cyber threats. The pilot is based on the CRI's Cyber Readiness Program, which is designed to assist small and medium-sized businesses improve their cybersecurity risk management and their ability to respond and recover from a cybersecurity incident. CRI and CCTI will also use the initiative to create a better understanding of the level of cyber readiness across water utilities

Cyber.org

CYBER.ORG supports the National Cyber Workforce and Education Strategy by focusing on K-12 cybersecurity education as the foundation for building success. In the next five years, across all 50 states, CYBER.ORG commits to (1) develop 1,300 cybersecurity lessons, activities, competitions, games, and career resources; (2) engage with 50,000 educators and caregivers and provide cybersecurity content to teach students; (3) reach over 6 million students through teachers and caregivers; and (4) host 1,250 cybersecurity training events affecting 32,500 educators and caregivers. CYBER.ORG, with support from school districts, the state department of education, and elected officials, will have a significant impact in the state of Nevada. Over the next year, CYBER.ORG will host or participate in three events in Nevada: DEFCON, BlackGirlsHack Squad Con, and the Society for Information Technology and Teacher Education Conference.

Cybersafe Foundation

Cybersafe Foundation will develop a cybersecurity ecosystem playbook specifically designed for the African continent based on the vision laid out in the National Cybersecurity Cyber Workforce and Education Strategy and the 2023 National Cybersecurity Strategy. The playbook will promote diversity and inclusion and will include lessons learned and best practices that support cyber workforce development. Cybersafe intends to use it to create opportunities for women and girls to excel in the cybersecurity field.

Cybersecurity Manufacturing Innovation Institute (CyManII)

CyManII has committed to developing and launching a new education and training program for advanced manufacturing professions that will reskill up to 10,000 students through an Introduction to ICS (Industrial Control System) Cybersecurity training for the manufacturing sector. This commitment supports the National Cyber Workforce and Education Strategy, in addition to the Apprenticeship Sprint.

★ ★ ★ ★ ★ ★

CyberSkills2Work.org

CyberSkills2Work, a nationally scalable program based at the University of West Florida and supported by a coalition of 10 National Centers of Academic Excellence–designated higher education institutions across the country, commits to adding 1,520 cybersecurity professionals to the Nation's cyber workforce over the next two years. The program also commits to expanding its support from Active Duty and transitioning military personnel to first responders, military spouses, women, underrepresented minorities, and Government personnel. The program will offer 22 additional training pathways that prepare learners for 16 cybersecurity work roles and 17 industry certifications. A $2.5 million NSA expansion grant funds this effort.

Dakota State University)DSU)

DSU, in Sioux Falls, SD, is enabling high school students in South Dakota to take as many as 30 credits of university-level computer science coursework as dual credit through the Governor's Cyber Academy program. Given that South Dakota's population is largely rural, the courses will be offered online and at high schools across the state to serve students at public, private, and tribal schools as well as those who are home-schooled. DSU anticipates that 40 students will enroll in the Academy this fall, with the goal of 250 students annually by 2027. In addition, 83 South Dakota small businesses, including minority-owned, veteran-owned, rural, and urban businesses, have enrolled in CyberSafe SD, a cybersecurity initiative sponsored by the U.S. Small Business Administration designed to empower small businesses to safeguard against cyber threats. The businesses range from boutique single-person businesses to larger 300-employee businesses from sectors that include manufacturing, health care, law, telecommunications, agriculture, education, entertainment, biotech, construction, retail, and tourism. Last, DSU is participating in CyberSkils2Work, which focuses on training military personnel and first responders in the domains of open-source intelligence and dark web investigations. The program has achieved remarkable success, surpassing projected enrollment by training over 300 learners to date, and it anticipates training 200 more participants this coming academic year. Its impact and effectiveness have been widely recognized, and as a result it has secured additional funds to cater to the growing demand for such critical training.

Dragos

Dragos, an industrial cybersecurity company, commits to furthering its investment in America's cyber workforce within the utilities sector through the expansion of its newly launched Community Defense Program. It commits to reaching over 5,000 new underresourced U.S.-based utility providers in 2024–25, equating to approximately $250 million in total benefits offered. The program provides free access to Dragos Academy's ICS/OT (operational technology) cybersecurity training, the Dragos Platform, and other assets that will arm the utility provider's cyber workforce with the tools needed for success.

★ ★ ★ ★ ★ ★

DruvStar

DruvStar has committed to providing paid internships to five University of Nevada, Las Vegas (UNLV) students a year. This internship will enable those students to receive hands-on cyber work experience and financial assistance when attending cybersecurity conferences such as DEFCON. These interns will also receive DruvStar training on common cyberattack patterns and on artificial intelligence technologies.

Eaton

Eaton—an intelligent power management company whose work cuts across advanced manufacturing, clean energy, and infrastructure—will offer paid co-op and internship opportunities with hands-on training in cybersecurity, and will invest $100,000 over the next three years in the Carnegie Mellon University (CMU) CyLab Security and Privacy Institute to support multidisciplinary cybersecurity research and education, building on its existing $350,000 investment.

Edwards Performance Solutions (Edwards)

Edwards, a Maryland-based woman-owned small business, remains integrally involved in Maryland organizations that champion cyber education/jobs and legislation, including the Cybersecurity Association of Maryland, Inc., and the Community College of Baltimore County Cybersecurity Advisory Board. As the only organization fully certified to support the Cybersecurity Maturity Model Certification (CMMC)—a unified standard for implementing cybersecurity across the defense industrial base—Edwards commits to nearly doubling the professionals trained in 2024, enabling more than 1,000 professionals to become CMMC-certified. Additionally, Edwards commits to hiring more than 10 junior cybersecurity consultants, using Edwards senior cyber subject matter experts (SMEs) for coaching and mentoring, while leveraging the Maryland EARN Program to enhance their skills through free, ongoing education.

Evolved Cyber, LLC

Evolved Cyber, a provider of cybersecurity services for businesses, is launching the MSP Cybersecurity Exchange (MSPCyberX), a collaborative community uniting managed service providers (MSPs) and cybersecurity compliance experts. Functioning as a continuously updated repository, MSPCyberX will organize compliance information by industry to offer an educational hub for its member MSPs. Recognizing that MSPs support an estimated 75%–80% of U.S. small to medium-sized businesses, MSPCyberX will focus on educating and supporting MSPs in compliance, fortifying a critical piece of the Nation's cybersecurity. MSPCyberX has committed to launch in February 2024 with a goal of over 100 MSPs on board by the end of 2024.

Fortinet

Fortinet is announcing its new Security Awareness Curriculum for K-12 students to help close the cyber skills gap and develop the cyber aware workforce of the future. Resources—crafted by former educators—include a comprehensive teacher's guide and classroom resources such as videos,

handouts, and lesson plans. This initiative became available at no cost to school districts and systems across the United States beginning in the fall of 2023. This effort will help educate students to become the cyber problem-solvers of the future and ensure that they are well-equipped to safely navigate the digital world. This curriculum can help over 55 million K-12 students across the country, including more than 500,000 students in Nevada, apply cybersecurity skills at school, home, and everywhere they go.

General Dynamics Information Technology (GDIT)

GDIT is committed to training the cyber workforce of the future to support the missions of the U.S. defense, intelligence, and civilian Government agencies. Specifically, in 2024 GDIT will both facilitate cybersecurity education for 20,000 employees and upskill over 1,000 employees with cyber certifications and learning courses. Further, GDIT will continue to invest in building local innovation ecosystems in St. Louis, New Orleans, and other cities by engaging nonprofits, academia, small businesses, and emerging technology companies to fuel the expansion and diversification of the cyber workforce.

Girl Security

Girl Security will unveil a new portfolio called All Secure, which includes the first comprehensive national security curriculum designed for dual enrollment for high schools and community colleges. As part of All Secure, Girl Security also launched the Workforce Futures Alliance, which will bring youth alongside industry leaders to design strategies and outputs to develop the security workforce talent to its fullest potential. Over the next three years, the organization will expand current programming and implement new programs designed to activate 1,500 new mentees, 1,200 workforce fellows, and 10 million U.S. learners through a targeted engagement strategy with more than 20,000 dual-enrollment high schools and 935 community colleges nationwide.

Google

In collaboration with the Consortium of Cybersecurity Clinics, Google.org has committed more than $20 million to help thousands of students receive hands-on experience in cybersecurity. This funding will support the creation and expansion of cybersecurity clinics at 20 higher education institutions across the United States; it follows the launch of the Google Cybersecurity Certificate focused on preparing people for entry-level jobs in cybersecurity. For cyber clinics across the country, Google.org commits to providing expert Googlers as volunteers to serve as student mentors in collaboration with the Consortium of Cybersecurity Clinics and select universities. In addition to volunteers, those attending the cyber clinics will receive access to the Google Cybersecurity Certificate, Google Titan security keys, and student mentorship opportunities from Google at no cost.

★ ★ ★ ★ ★ ★

Gula Tech Foundation

The Gula Tech Foundation has demonstrated a multiyear commitment to the recruitment and training of America's cyber workforce. By referring to the industry as the "Data Care" industry and providing critical support, expertise, and networks, the Gula Tech Foundation has enabled dozens of nonprofit organizations to employ appropriate cyber knowledge and skills, particularly those that seek to diversify the cyber workforce, with over $6 million in grants. In 2024, the Gula Tech Foundation is committing an additional investment of $2 million for cyber workforce developments focused on expanding access to apprenticeships.

HBCU Prep School

Claudia Walker—educator and author of "ABCs of HBCUs"—has committed to developing a cybersecurity-focused book for kids. The book series is called "The ABCs of Cybersecurity" and will teach children and their guardians about digital citizenship, how to stay safe online, and different career paths in the field of cybersecurity. Leaders from Black Girls in Cyber, Blacks in Cyber, and #ShareTheMicInCyber will partner and support content development.

HP

HP is increasing its free Future of Work Academy (FOWA) for community and technical colleges to nearly 100 institutions and over 500 students from across the country, including community colleges in Nevada. FOWA equips students with career readiness through an interactive symposium, an innovation incubator, and a career accelerator. In addition, students will have increased opportunities with top tech firms recruiting for full-time positions and internships.

IBM

IBM is committed to help skill 150,000 people in cybersecurity by the end of 2024. To help achieve this goal, and to contribute to a more diverse U.S. cyber workforce, IBM is partnering with 20 HBCUs to co-establish Cybersecurity Leadership Centers. Through these partnerships and programs, such as IBM SkillsBuild, IBM has provided more than 119,500 learners with cybersecurity training and will continue to build on its progress after reaching its goal.

ICS Village, SANS Institute, Siemens Energy

ICS Village (a nonprofit organization to advance security awareness and education of industrial control systems (ICS)), SANS Institute (a global cybersecurity training, workforce development, certification, and education provider), Siemens Energy (a Siemens business that supports companies and countries to reduce emissions across the energy landscape for a more sustainable energy system), and their partners plan to launch the Cybersecurity & Industrial Infrastructure Security Apprenticeship Program (CIISAp) as a Registered Apprenticeship to develop the next generation of cyber defenders protecting the digitally connected systems such as energy assets, wastewater treatment facilities, advanced manufacturing, and transportation systems. The initial goal is to fill the pipeline with 100 candidates, with a focus on veterans and transitioning military members. This

four-year program would enable apprentices to apply their technical industrial cybersecurity education with moderate computer skills, and gain the hands-on experience and knowledge needed to fill existing cybersecurity vacancies that currently pay above $90,000 per year. Apprentices would gain job experience at a rotation of employers while receiving technical training, as well as completing hands-on exercises and industry certifications.

iKeepSafe

iKeepSafe will host online trainings for educators reaching 400 educators each month over the next year, utilizing the online training content found at no cost on the iKeepSafe website—Data Privacy in Education—an iKeepSafe Educator Training Course. This training will provide educators at all levels—teachers, administration, and support staff—with the information necessary to understand their role in helping to keep students and student data safe in an increasingly online learning environment.

Information Technology Senior Management Forum (ITSMF)

ITSMF aims to raise the number of Black Chief Information Security Officers (CISOs) by 10% by 2026 and increase the cybersecurity workforce pipeline by the same percentage. The impact of ITSMF's efforts results in industry innovation, growth, and thought leadership through increased representation of talented Black professionals in cyber and risk management at senior levels.

Katzcy

Katzcy PlayCyber, a woman-owned small business based in the DC, Maryland, and Virginia region, is committed to fostering a more diverse, skilled, and resilient national cyber workforce by creating a Cyber ESport league that reaches thousands of professionals in 2024. Katzcy PlayCyber's Wicked6 Global Women's Hack and Chat was held virtually on March 29, 2024, and included a unique 24-hour hack and chat featuring six cyber games for some 2,000 women to hone their cyber skills. Throughout 2024, Katzcy PlayCyber will extend the US Cyber Games program with the commissioning of an all-women's US Cyber Team in order to call more women and girls to cyber through gaming. Through these commitments, Katzcy PlayCyber expects to reach over 10,000 individuals in 2024.

Kubota

Kubota, an equipment manufacturing firm, will use earn-and-learn opportunities, such as paid internships, and partnerships with technical schools, high schools, and universities on certificate, diploma, degree programs, and adult education across every area of its business, including to create a cyber-resilient workforce to secure Kubota's advanced manufacturing systems. Kubota made $457 million in facility investments in the past year and announced plans to fill over 1,300 new jobs in Georgia and Kansas.

★ ★ ★ ★ ★ ★

Lightcast/Cyberseek

Lightcast will provide quarterly data announcements on the size of the cyber talent needs, providing a more comprehensive, up-to-date picture of the cyber labor market. Lightcast will also develop a skills-based hiring toolkit for employers to help companies implement skills-based hiring best practices in developing their cyber workforce. In addition, Lightcast is on track to get up to 900,000 unique users on the Cyberseek website this year.

MassBay

MassBay Community college plans to announce an increase in the number of cybersecurity professors, enabling an expected increase in MassBay cybersecurity enrollment by more than 40 students, and strengthening its cybersecurity program through the addition of a cyber range. Learners (on an annual basis) will include 45 students from a consortium of colleges, 60 high school students, and 135 employees from businesses, municipalities, school systems, and nonprofit organizations from the Greater Boston region. NSF grant funding will assist the school in increasing the diversity of the cybersecurity workforce. The school is also applying for funding to build a Cybersecurity Center, which will include the range, a Security Operations Center, and abundant space where college and high school students and employees from businesses, municipalities, school systems, and nonprofit groups from the Greater Boston region can strengthen their cybersecurity skills.

MasterCard

Mastercard is doubling down on its long-standing efforts to build the cyber workforce and drive security for our shared digital ecosystem. Mastercard will align its cybersecurity roles to the Career Navigation structure conforming to the NICE Framework to simplify career growth and develop a robust skill set across many cybersecurity domains. To support its own talent development, Mastercard will also create upskilling pathways for junior professionals mapped to this same structure by 2024.

Additionally, Mastercard will strengthen its support for equipping American girls with foundational cyber skills through its commitment to educate 5 million students by 2025 with its flagship STEM education program, Girls4Tech™. Mastercard will also support access to free cybersecurity education, trainings, and resources for up to 10 million micro, small, and medium-sized businesses by 2025. The security of these businesses is critical and these resources, combined with its ongoing substantial investment, will help protect their ecosystem and our Nation's economy.

Microsoft

Microsoft is partnering with Last Mile Education Fund, Whatcom Community College, and the American Association of Community Colleges to achieve its goal of helping to skill and recruit into the cybersecurity workforce 250,000 people by 2025. To date, this effort has supported over 379 community colleges in 48 of the 50 states (nearly a third of all community colleges in the United

States). This includes $1,177,000 in direct scholarship support to 2,378 students, $93,000 in additional voucher assistance, 50 faculty supported through capacity-building community of practice, 28 academic/workforce professionals trained, and support of more than 60 cybersecurity classes in the 2023–24 school year, with content from curriculum partners CYBER.ORG and CodeHS.

MxD

MxD is a Chicago-based national advanced manufacturing institute that includes nearly 300 partners from industry, academia, nonprofit organizations, and Government to help manufacturers improve their operations and drive productivity improvements. MxD, in collaboration with the University of Maryland, Baltimore County, created the Cybersecurity for Manufacturing Operational Technology (CyMOT) program to increase the security of U.S. manufacturers from cyberattacks by providing role-based training to the next generation of cybersecurity workers in manufacturing. The 60-hour live-instruction course series targets roles in AI engineering and cybersecurity and has been utilized by MxD partners, including Boeing, Dow, and Rolls-Royce, to provide more than 175 current and future workers with skills unique to securing the manufacturing floor. The CyMOT course series is tailored to meet the needs of each student, including current manufacturing workers looking to upskill and future workers still learning the basics. MxD commits to use the CyMOT curriculum and other courses to train, certify, and provide employment opportunities to underserved students at community colleges and HBCUs across the United States.

National Cyber Group (NCG)

NCG builds and delivers effective cyber security vocational training curricula by training in a hands-on environment through a hybrid of classroom and apprenticeships in a live, working Security Operations Center. NCG is committed to training 10,000 new entrants to the cyber security field by 2025. NCG engages and recruits students who reflect our Nation and is committed to supporting a diverse and highly skilled cyber workforce. NCG supports veterans directly by offering cyber training scholarships so they may continue to serve in national security as they transition to the civilian cyber workforce.

National Cyber Scholarship Foundation (NCFS)

In the 2023–24 school year, NCSF provided gamified cyber learning to more than 800 students in Nevada from over 65 schools. Through public-private partnerships, it anticipates that over 80 students will receive more than $270,000 in scholarships to obtain industry training and certifications from the SANS Institute. Additionally, NCSF seeks to collaborate with leaders in Las Vegas and Reno to establish a state task force in Nevada to amplify the impact of cyber education programs across the state.

★ ★ ★ ★ ★ ★

National Cybersecurity Alliance (NCA)

NCA has committed to expanding opportunities for Black Americans in the cybersecurity industry through the upcoming HBCU Scholarship Program. Established in partnership with One In Tech, an ISACA Foundation, the initiative will support individuals currently underrepresented in the industry by ensuring equitable access and advancement in cybersecurity and tech careers. The new program will expand upon NCA's recently launched HBCU Career Program, which aims to equip students with the skills necessary to navigate the search process for positions in security, privacy, and risk.

National Cybersecurity Alliance (NCA)

NCA is kicking off the second year of the HBCUs Cybersecurity Career Program, "See Yourself In Cyber." "See Yourself In Cyber" aims to change the narrative around cybersecurity careers by showing students that there is a role in security for everyone and multiple pathways to a successful career. NCA is committed to raising awareness about cybersecurity careers and increasing opportunities for underrepresented students. In its first year, the program connected over 1,000 students with recruiters and professionals at on-campus events across nine schools, and 142 students have been paired with cybersecurity mentors. This fall, NCA will hold events at five HBCUs in September and November. Each event will feature both public and private sector employers, guest speakers, and recruiters, as well as local law enforcement departments, to show students the variety of career paths offered in cyber and opportunities available in their own communities.

National Cybersecurity Alliance (NCA)

NCA is committed to building the resilience of the small and medium-sized business (SMB) community in the face of increasing cyber risk. The NCA is launching its first cohort of the Cybersecure My Business education program, a program that focuses on training the owners and leaders of SMBs on how to manage cyber risk as a function of their business. This program launched in late February 2024 as a live, instructor-led, and virtual course paired with practical actions completed by participants between weekly training sessions. As a part of this commitment, the NCA pledges to reach over 100 businesses throughout 2024 and will gather metrics on the specific actions taken by the SMBs completing the course.

Northern Illinois Workforce Coalition (NIWC) Cybersecurity Career Pathway

NIWC, a regional consortium of 11 community colleges connected to local workforce boards, commits to develop an IT training program to prepare individuals for entry to cybersecurity certificate and degree programs from which graduates have the appropriate knowledge to thrive in this sector. The approach intends to remove barriers, accelerate entry into highly specialized cybersecurity careers, and create greater access to a diverse talent pool for the IT industry.

★ ★ ★ ★ ★ ★

NPower

NPower is a workforce development nonprofit. The organization commits to embedding cyber skills across all of its courses, primarily reaching young adults and military-affiliated individuals. NPower's curriculum routinely includes digital literacy to advance skills in cloud computing, cybersecurity, software development, and network infrastructure. NPower also commits to training over 6,000 individuals during the next three years and offering multiple on- and off-ramps to continued learning and full-time employment, including through apprenticeships.

Ohio Cyber Range Institute–Regional Programming Center (OCRI-RPC) Ecosystem

The OCRI-RPC Ecosystem is committed to expanding its skills-based training on a secure cyber range to all 88 counties in Ohio. Housed at and administered by the University of Cincinnati on behalf of the state, the OCRI-RPC Ecosystem knits together 24 other Ohio universities, colleges, and nonprofit organizations through a regional programming center system to deliver cyber range services to cybersecurity professionals and students across Ohio. To date, the OCRI-RPC Ecosystem has supported over 20,000 distinct Ohio-based users through 314 K-12 classes and 668 higher education courses, and has delivered 105 cyber camps, exercises, and bootcamps, the latter involving 1,000 citizens seeking industry-recognized cybersecurity credentials.

Okta

Okta, an identity and access management company, is committed to building a robust, diverse, and highly trained cybersecurity workforce for the future. In support of this commitment, Okta is investing in a $1.6 million philanthropic fund for organizations that are creating inclusive pathways to technology careers for underrepresented communities. Second, Okta is providing 5,000 educational grants to professionals not currently employed who are looking to make a career transition to cybersecurity by improving their skills. These grants will focus on military spouses, veterans, and tech workers.

Omidyar Network

Omidyar Network is a self-styled "philanthropic investment firm," composed of a foundation and an impact investment firm. It has committed $5 million dollars to support and expand cybersecurity and open-source security ecosystems, including work to ensure that the next generation is informed and activated to engage across these technologies.

Palo Alto Networks

Palo Alto Networks kicked off its 2023–24 Secure the Future competition, which challenges 100 students enrolled in community and four-year colleges and universities throughout the country to identify and address cyber threats in vulnerable industries. To date, Palo Alto Networks has hired seven participants from the competition. The top three finalists are awarded cash prizes of $10,000, $5,000, and $2,500, respectively. The company also invests in educating and training a new cohort of early talent professionals and interns as members of its Systems Engineering (SE) Academy. It is one

of several accelerated onboarding programs offered by Palo Alto Networks to help develop and diversify the cyber workforce and arm recent college graduates with hands-on labs and facilitated training with industry experts. As full-time members of the Palo Alto Networks workforce, program participants help organizations optimize their security posture. Palo Alto Networks recently welcomed a new cohort of systems engineers and is actively recruiting for 2024.

Parkway West Career and Technical Center

Parkway West Career and Technical Center committed to train 80 students per year in a cybersecurity Registered Apprenticeship program, connecting them to cybersecurity jobs in the region.

Pearson

Pearson VUE is committed to helping address the need for qualified cyber professionals in the workforce through its global network of 5,500 test and training centers. Pearson VUE has announced it will offer its IT Specialist in Cybersecurity training resources and certification exams at no charge to all learners in its network of learning and assessment centers across Pennsylvania and Ohio. Initially focusing on Pennsylvania and Ohio, Pearson's commitment will also support U.S. military installations worldwide, enabling participating centers to train and prepare more qualified individuals to cyber careers.

Peraton

Peraton, a technology company that provides space, intelligence, cyber, and defense capabilities for Government entities, is committed to doubling its apprenticeships and hiring more than 200 interns in 2024. This program will entail placing students on tasks with an emphasis on developing the next generation's cyber workforce. Internships will focus on cybersecurity skills, engineering, software development, database management, and security threat analysis, with an aim to providing a path to careers in a dynamic technological environment. In addition, Peraton will expand its community college partnerships on cybersecurity and establish a program in 2024 to assist young and mid-career professionals to transition to cyber careers.

San Diego Cyber Center of Excellence (CCOE)

San Diego CCOE assists employers seeking to audit and address their organizations' cybersecurity postures. With funding from California's CADENCE grant, CCOE is partnering with the City of San Diego Regional Cyber Lab, Cal Poly in San Luis Obispo, and Amazon Web Services to create "My e-CISO," a generative AI application that grades an organization's current cyber posture and provides recommendations for actionable steps for improvement. CCOE and the San Diego Regional Cyber Lab commit by the end of 2024 to assist more than 200 underresourced organizations in the Southern California region to better understand their cybersecurity posture and needs with the "My e-CISO" tool.

★ ★ ★ ★ ★ ★

SANS Institute

Over the past year, SANS and the National Cyber Scholarship Foundation (NCSF) expanded their partnership for CyberStart America and Cyber FastTrack, programs to inspire high school and college students across the United States to develop foundational cyber skills. In CyberStart, students utilize a transformative cyber education platform to solve challenges tied to real-world scenarios and build their core skills and knowledge, discovering a passion for cybersecurity in the process. For 2023–24, SANS and NCSF plan to engage over 50,000 students in gamified learning, with up to 5,000 receiving training and certification scholarships. Also, working with its nonprofit, Government, and private sector partners, SANS plans to broaden, diversify, and strengthen the national cyber workforce through reskilling for career changers. These reskilling programs will provide over $9.2 million in training and certification scholarships to 500+ individuals, driving increased diversity, equity, inclusion, and accessibility in cybersecurity across the Nation.

SAP

SAP—the world's largest enterprise software provider—will further its commitment to help close the cybersecurity skills gap by expanding its Global Security Early Talent program. This two-year program is designed for high-performing early career professionals, with little to no professional experience, who have a basic understanding of information technology and security topics. The program builds on the ambitious goal of SAP's digital skills initiative to upskill two million learners worldwide with technology skills by the end of 2025.

Society for Human Resource Management (SHRM)

SHRM is the foremost expert, convener, and thought leader on issues impacting today's evolving workplaces. With nearly 325,000 members in 165 countries, SHRM affects the lives of more than 235 million workers and families globally. SHRM has committed to offering free cyber training content for HR professionals and aims to provide the training to at least 15,000 users, projecting that these users would lead to the hiring of up to 75,000 cyber professionals.

Task Force Movement (TFM)

TFM will be awarding cybersecurity scholarships to transitioning service members/veterans and/or military spouses. TFM will fund 50 award recipients in the next year to pursue quality certification courses for career pathway entry into the cybersecurity ecosystem, with plans to expand the program in future years. TFM will also align the award recipients with employer partners who are committed to hiring the award recipients upon completion of the course.

Task Force Movement (TFM)

TFM prepares transitioning service members; veterans, including disabled veterans; and military families with the tools they need to engage in cybersecurity career pathways via scholarships and public-private partnerships. In addition to the 50 scholarships that TFM previously announced it will award over the next year, TFM is committing to expand this effort to directly support state and local

leaders in implementing their own Task Force Movement programs, starting with two states in the first year.

TeamWorx Security

TeamWorx Security, a defense, cyber, and critical infrastructure professional services and technology support company, is committed to growing the cyber community through training and upskilling 1,000 nontechnical personnel by 2026 across the U.S. military, Government, and critical infrastructure labor force. Additionally, TeamWorx Security is continuing to support internship positions across high school, college, and DoD SkillBridge candidates. Through training and technology, it is purposefully reducing the complexity of cyber to make it more accessible to a diverse workforce. TeamWorx Security's cloud-based cyber workforce collaboration platform, Hive-IQ, will be used to onboard an additional 5,000+ cyber professionals by 2026 across the military, Government, and critical infrastructure labor force.

Technology Advancement Center (TAC)

TAC is committed to providing key operational technology (OT) infrastructure cybersecurity training through nonprofit programs and conferences. Events such as Hack the Port, Hack the Hospital, and Hack the Railroad, to name a few, are designed to provide real-world learning to college students, military professionals, and other U.S. Government cyber professionals using actual products and services in the field. TAC's platform has already trained thousands of students in real-life scenarios and is expanding over the next two years to host an anticipated eight conferences and reach over 10,000 students and professionals.

ThriveDX

ThriveDX is committed to increasing employment and training opportunities for underrepresented and underserved communities in the cybersecurity field. In partnership with BlackGirlsHack, ThriveDX has formed and launched a cybersecurity scholars program concurrently with the launch of the National Cybersecurity Workforce and Education Strategy. This ThriveDX scholars program provides 25 learners from BlackGirlsHack with full-tuition scholarships to participate in the ThriveDX Cybersecurity Professional Certificate Training Program. The program includes skills-based training, wraparound services, career support, and job placement. In addition, ThriveDX is announcing that it will extend its existing collaboration with the local community of Nevada through its partnership with UNLV's Division of Educational Outreach. ThriveDX has committed to awarding 25 additional full-tuition scholarships to lifelong learners in underserved, underresourced, and U.S. military veteran communities in Nevada.

Trellix

Trellix is committed to hiring 300 interns over the next two years. Trellix will also leverage the career growth platform Gotara to advance the careers of 50 of Trellix's high-performing women and is

committed to offering roles to 12 employees via the Hispanic Alliance for Career Enhancement (HACE).

University of Nevada, Las Vegas (UNLV)

UNLV has received funding from the Federal Government for cybersecurity education, enabling it to bring on 50 students per year as paid interns at its Free Cyber Clinic. In this way, students will receive hands-on cyber experience from small business clients, training for the Security+ and Certified Ethical Hacker certifications plus exam fee support, and support for attending cybersecurity conferences such as DEFCON.

University of Pittsburgh

The University of Pittsburgh Institute for Cyber Law, Policy, and Security will help build a strong pipeline of cybersecurity professionals by training over 500 high school students in cybersecurity basics, ethics, and career opportunities by 2028.

VetSec, Inc.

VetSec, a nonprofit that provides low and no-cost training, education, employment, and transition assistance to Active-Duty service members, reservists, veterans, and members of the National Guard seeking cyber careers, is committed to providing educational pathways to meaningful employment to over 10,000 people by the end of 2025, and to 25,000 by 2028. In addition to this direct commitment, VetSec provides a lifelong community for military veterans in information technology (IT) and cyber. It is dedicated to supporting its members throughout their careers and life journeys.

VISA

The credit card company Visa, a world leader in digital payment technology, has launched the Visa Payments Learning Program to diversify entry paths into the workforce with an initial focus on payments cybersecurity. Through its learning courses and certifications, Visa seeks to upskill underutilized talent, such as returning-to-workforce, early-in-career, second career, and military talent—thereby broadening the industry's talent marketplace. Visa's initial introductory Payments Cybersecurity training courses and certifications will be offered to three groups: students via partner institutions, Visa clients, and Visa employees, apprentices and interns. Visa has welcomed an initial cohort of apprentices, who have undergone 16 weeks of specialist training and have recently embarked on a one-year apprenticeship. Visa also plans to develop intermediate and advanced level courses and certifications in 2024, and ultimately provide educational pathways both to local communities and to the broader payments industry.

Walmart

Walmart, committed to increased HBCU cyber investment; continued support of science, technology, engineering, arts, and mathematics (STEAM) organizations focused on the Black community; and long-term investment in partnerships to advance cyber awareness and training

across the Black and BIPOC (Black, Indigenous, and People of Color) communities, including with nonprofit organizations such as Black Girls in Cyber, BlackGirlsHack, Blacks in Cyber, Information Technology Senior Management Forum (ITSMF), and Cyversity. Walmart also announced the removal of the college degree requirement for information security positions, regardless of seniority, a change that will help improve opportunity for all.

Western Governors University (WGU)

WGU is committed to developing a skilled and robust national cybersecurity workforce. WGU currently serves almost 500 Nevada-based learners in its cybersecurity programs, and it projects that it will accept and enroll over 550 additional students direct from Nevada into its cybersecurity degree programs over the next 12 months. Currently over half of the current cybersecurity student population from Nevada represents a traditionally underserved population, with a significant portion identifying as a first-generation student, and WGU is committed to continuing this trend. During the next six to nine months, WGU will make digital credential wallets available to its students to identify and showcase their skills, align its program to a variety of occupations, and support students applying for jobs with employers who are seeking skilled talent. WGU will also will continue its competency-based education approach with an emphasis on hands-on experience and problem-solving abilities.

Women in Cybersecurity (WiCyS)

WiCyS is committed to mobilizing its network to underscore the importance of diverse and highly skilled cybersecurity professionals to support the National Cyber Workforce and Education Strategy through four commitments: (1) create cybersecurity career accessibility and opportunities for upskilling and reskilling underrepresented groups; (2) continue the WiCyS Security Training Scholarship program by working with a multi-organization approach to invest in the talent pipeline; (3) mobilize U.S. regions through WiCyS's 60 professional affiliates and 220 student chapters with increased opportunity via conferences, events, and hosted engagements; and (4) build a cybersecurity ecosystem through industry engagement. Through these commitments, WiCyS expects to reach more than 10,000 individuals.

★ ★ ★ ★ ★ ★

APPENDIX B

Federal Cyber Workforce and Education Programs

*An asterisk indicates a Government-affiliated program that may receive funding from the Federal Government.

Education and Training

Cybersecurity and Infrastructure Security Agency

- Cyber Defense Education and Training (CDET)
- Non-Traditional Training Grant (NTTP)
- National Initiative for Cybersecurity Careers and Studies (NICCS)
- Cybersecurity Apprenticeship Program for Veterans
- NICCS-Federal Virtual Training Environment (FedVTE)

Department of Commerce

- NIST
  - NICE Strategic Plan (2021–25)
  - NICE Interagency Coordinating Council
  - NICE Community Coordinating Council, Working Groups, and Communities of Interest
  - Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development
  - Cyberseek.org*
  - National K12 Cybersecurity Education Conference*
  - NICE Conference and Expo*
  - National Cybersecurity Career Ambassadors Program
  - Cybersecurity Career Week
  - NICE Framework and Resource Center
  - US Cyber Games*
  - Free or Low-Cost Cybersecurity Resources
  - Cybersecurity Apprenticeship Finder
- Economic Development Administration (EDA)
  - Regional Technology and Innovation Hub Program
  - Science, Technology, Engineering, and Math (STEM) Talent Challenge
- NTIA
  - Tribal Broadband Connectivity Program

Department of Defense (DoD)

- DoD Cyber Workforce Framework (DCWF) Resource Center
- Defense Civilian Training Corp (DCTC)
- Military Service Academies
- Senior Reserve Officer Training Corps (SROTC)
- Naval Postgraduate School
- National Defense University (NDU)
- College of Information and Cyberspace (CIC)

Senior Military Colleges (SMC)
Joint Special Operations University (JSOU)
Virtual Institutes for Cyber and Electromagnetic Spectrum Research and Employ (VICEROY)
The Air Force Institute of Technology (AFIT)
Cybersecurity Talent Initiative (CTI)*
CXO (Chief Executive Officers) Fellows Program with OMB
Center for Development of Security Excellence (CDSE)
Department of the Navy HBCU and Minority Institutions Program
DoD Cyber Service Academy (DoD CSA), formerly DoD Cyber Scholarship Program
Technology for Advanced Manufacturing Projects (STAMP)
DoD STEM
DoD STEM Community College Consortium
STEM Careers in Cyber
Cyber Patriot*
Army Educational Outreach Program (AEOP)
- College Qualified Leaders (CQL)*
- ECYBERMISSION*
- High School Apprenticeship Program (HSAP)*
- Research and Engineering Apprenticeship Program (REAP)*
- Undergraduate Research Apprenticeship Program (URAP)*

Air Force Research Laboratory (AFRL)/Air Force Office of Scientific Research (AFOSR)
- Center of Excellence (COE) Program

Air Force Research Laboratory (AFRL) Scholars Program*
Air Force Visiting Scientist Program
Consortium Research Fellows Program (CRFP)*
National Defense University–College of Information and Cyberspace

Department of Education

Graduate Assistance in Areas of National Need
Minority Science and Engineering Improvement Program
Presidential Cybersecurity Educator Award
Career and Technical Education (CTE)–Cyber Net

Department of Energy (DOE)

Cyber Fire Foundry*
CyberForce Competition
U.S. Department of Energy (DOE) Cyber Defense Competition
DOE STEM
BSSW Fellowship Program
Center for Global Security Research Student Intern Program
Cybersecurity Summer Institute
OMNI Technology Alliance Internship Program

Department of Homeland Security

The Secretary's Honors Program (SHP) Cyber Student Volunteer Initiative (CSVI)
Tribal Cybersecurity Grant Program

Department of Labor

Cybersecurity Apprenticeships
Apprenticeship Sprint

Youth Apprenticeships
National Apprenticeship Week
Youth Apprenticeship Week
Apprenticeship Standards Builder
Apprenticeships.Gov
Cybersecurity Competency Model*

Department of State

Bureau of Cyberspace and Digital Policy and Foreign Service Institute's Cyber and Digital Policy Tradecraft Course

Department of the Treasury

Skills-Based Cyber Hiring and Training Program

Department of Veterans Affairs (VA)

VA Cybersecurity Apprenticeship Program for Veterans
VA-Office of Information and Technology (OIT) Career Development Portal
Veteran Employment Through Technology Education Courses (VET TEC)
Technical Career Field (TCF) Trainee Program
Accelerated Payments for High-Technology Programs

Federal Bureau of Investigation

Cyber Investigator Certification Program (CICP)*
CISO Academy

National Science Foundation

National Cybersecurity Training and Education Center
Secure and Trustworthy Cyberspace
Advanced Technological Education (ATE) Community College Focus

National Security Agency

National Centers of Academic Excellence in Cybersecurity (NCAE-C) Program
National Security Agency (NSA) Student Programs
National Security Agency's GENCYBER Program
Center of Academic Excellence (CAE)-Cyber Operations Summer Intern Program
Cooperative Education Program (NSA) Hawaii
Cooperative Education Program (NSA) STEM
Cryptanalysis and Signals Analysis Summer Program (CASA SP)
Cyber Summer Program (CSP)
WIN Cyber
Cyber Kids Day
NSA Codebreaker Challenge
NSA-funded CyberSkills2Work Program*
NSA Cybersecurity Exercise (NCX)
NSA Careers Portal

USAID

Innovative Workforce Activity Grant Program

★ ★ ★ ★ ★ ★

Scholarships

Department of Defense

DoD Cyber Service Academy (DoD CSA), formerly DoD Cyber Scholarship Program
DoD SMART Scholarship-for-Service Program
DoD Cyber Scholarship Program
Science, Mathematics, and Research for Transformation (SMART)

Department of Education

Graduate Assistance in Areas of National Need

Department of State

American Association for the Advancement of Science (AAAS) Science and Technology Policy Fellowship Program*

National Science Foundation

CyberCorps®: Scholarship for Service (SFS)

Public Service – Military

Air Force

Cyber Science Program
Cyber Direct Commissioning

Army

Reserve Pilot Project

Department of Defense

DoD Cyber Excepted Service (CES)

National Security Agency (NSA)

NSA Experiential Tour (NET)

Public Service – Federal Civilian

Cybersecurity and Infrastructure Security Agency (CISA)

Intelligence and Cybersecurity Diversity Fellowship Program (ICDF)
Cybersecurity Talent Initiative (CTI)*
President's Cup Cybersecurity Competition
Federal Skilling

Department of Defense

Workforce Innovation Directorate (WID)

Department of Energy

CyberForce Program
Office of the Chief Information Officer (OCIO) Cybersecurity Education Program
Tracer FIRE*

Department of Health and Human Services

Centers for Medicare & Medicaid Services (CMS)
CMS CyberVets Program

Department of Homeland Security

Cybersecurity Talent Management System (CTMS)
Strategic Talent, Recruitment, Inclusion, Diversity and Engagement (STRIDE)
DoD/DHS/CISA/VA
Interagency Federal Cyber Career Pathways

Department of Justice

Cyber Fellowship Program

Federal Bureau of Investigation

Accelerated Cyber Training Program (ACTP)
Cyber Executive Training Program (CETP)
Computer Scientist Field Operations Training (CSFOT) Program
Data Science Curriculum: Onboarding Series (DSCOS)
Data Analytics Support Hub (DASH)

General Services Administration

Digital Corps

Office of Personnel Management

Tech to Gov
Cybercareer.gov
The Presidential Management Fellows (PMF) Program
Federal Rotational Cyber Workforce Program
STEM Portal on USAJobs

National Security Agency

National Security Agency (NSA) Development Programs

APPENDIX C

Federal Agencies Participating in NCWES Implementation

- Department of Agriculture
- Department of Commerce
  - Economic Development Administration
  - National Institute for Science and Technology
  - National Telecommunications and Information Administration
- Department of Defense
- Department of Education
- Department of Energy
- Department of Health and Human Services
- Department of Homeland Security
  - Cybersecurity and Infrastructure Security Agency
- Department of Housing and Urban Development
- Department of Interior
- Department of Justice
  - Federal Bureau of Investigation
- Department of Labor
- Department of State
- Department of Transportation
  - Federal Aviation Administration
- Department of the Treasury
- Department of Veteran's Affairs
- Environmental Protection Agency
- General Services Administration
  - U.S. Digital Corps
- National Security Agency
- National Science Foundation
- Nuclear Regulatory Commission
- Office of the Director of National Intelligence
- Social Security Administration
- U.S. Agency for International Development
- Executive Office of the President
  - Domestic Policy Council
  - Office of Management and Budget
  - Office of National Cyber Director
  - Office of Personnel Management
  - Office of Science and Technology Policy
  - National Economic Council
  - National Security Council

★ ★ ★ ★ ★ ★

APPENDIX D

National Centers of Academic Excellence in Cybersecurity

Achieving designation as a National Center of Academic Excellence in Cybersecurity (NCAE-C) is a mark of distinction that highlights an institution's commitment to advancing the cybersecurity capabilities of the Nation. This prestigious recognition reflects the dedication of an NCAE-C to rigorous academic standards, ongoing faculty development, leadership in the cybersecurity field, alignment with cutting-edge technologies, and engagement in cyber workforce and education ecosystem efforts. The NCAE-C program is managed by the National Security Agency's (NSA's) National Cryptologic School and supported by key Federal agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Institute of Standards and Technology (NIST), and National Science Foundation (NSF), as well as the Department of Defense (DoD) Chief Information Officer (DoD-CIO). NCAE-C institutions set the gold standard for cybersecurity education and are fostering the robust and skilled cybersecurity workforce that is essential for national security.

Institutions participating in the CyberCorps®: Scholarship for Service program of April 2024 are labeled with "SFS" in the list below. More information on the CyberCorps®: Scholarship for Service program can be found at https://sfs.opm.gov. Institutions participating in the DoD Cyber Service Academy (DoD CSA) program are indicated with "CSA."

Minority-Serving Institution Abbreviations

AANAPISI – Asian American and Native American Pacific Islander-Serving Institution
ANNH – Alaska Native–Serving and Native Hawaiian–Serving Institution
HBCU – Historically Black College and University
HSI – Hispanic-Serving Institution
NASNTI – Native American–Serving Non-Tribal Institution
PBI – Predominantly Black Institution
TCCU – American Indian Tribally Controlled College and University

Alabama

Athens State University
Auburn University — SFS
Calhoun Community College
Enterprise State Community College
Jefferson State Community College
Stillman College — HBCU
Talladega College — HBCU
Tuskegee University — HBCU, PBI, SFS
University of Alabama — SFS
University of Alabama at Birmingham — SFS
University of Alabama in Huntsville — SFS, CSA
University of South Alabama — SFS
Wallace State Community College

★ ★ ★ ★ ★ ★

Arizona

Arizona State University — HSI, SFS
Cochise College — HSI
Embry-Riddle Aeronautical University, Prescott Campus
Estrella Mountain Community College — HSI
Glendale Community College — HSI
Grand Canyon University — CSA
Pima Community College — HSI
University of Advancing Technology
University of Arizona — HSI, SFS, CSA

Arkansas

Northwest Arkansas Community College — PBI
University of Arkansas — SFS
University of Arkansas at Little Rock

California

California State Polytechnic University, Pomona — AANAPISI, HSI, SFS
California State University, San Marcos — AANAPISI, HSI
California State University, Sacramento — AANAPISI, SFS, HSI
California State University, San Bernardino — HSI, SFS
Coastline Community College — AANAPISI, HSI
Cosumnes River College — AANAPISI, HSI
Cypress College — AANAPISI, HSI
Fullerton College — AANAPISI, HSI
Long Beach City College — HSI
Moorpark College — HSI
National University — HSI, CSA
Naval Postgraduate School — SFS
Ohlone College — AANAPISI
Riverside City College — HSI
Saddleback College — AANAPISI, HSI
Sierra College
University of California, Irvine — AANAPISI, HSI, PBI
University of San Diego

Colorado

Arapahoe Community College
Colorado Mesa University
Colorado School of Mines
Colorado State University
Colorado State University–Pueblo — HSI
Colorado Technical University
Metropolitan State University of Denver — HSI, CSA
Pikes Peak Community College

★ ★ ★ ★ ★ ★

Pueblo Community College — HSI
Regis University — HSI
United States Air Force Academy
University of Colorado Denver — AANAPISI, HSI
University of Colorado, Colorado Springs — SFS, CSA
University of Denver
Western Colorado University

Connecticut

Central Connecticut State University
Quinnipiac University
Sacred Heart University
United States Coast Guard Academy
University of Connecticut — AANAPISI
University of New Haven — SFS, CSA

Delaware

University of Delaware — SFS
Wilmington University — HSI

District of Columbia

George Washington University — SFS
Georgetown University — HSI, SFS
Howard University — HBCU
National Defense University — HSI

Florida

Daytona State College
Eastern Florida State College
Embry-Riddle Aeronautical University, Daytona Beach — SFS, CSA
Florida Agricultural and Mechanical University (Florida A&M) — HBCU
Florida Atlantic University — HSI, SFS
Florida Institute of Technology
Florida International University — HSI, SFS
Florida Memorial University — HBCU
Florida State University — SFS, CSA
Indian River State College — HSI
Jacksonville University
Miami Dade College — HSI
Nova Southeastern University — AANAPISI, HSI, CSA
Palm Beach State College — HSI
Pensacola State College
Saint Leo University
St. Petersburg College — NASNTI
Tallahassee Community College — HSI
University of Central Florida — HSI, SFS

University of Florida — SFS
University of North Florida
University of South Florida — SFS
University of Tampa
University of West Florida — SFS, CSA
Valencia College — HSI

Georgia

Augusta Technical College — PBI
Augusta University —SFS, CSA
Central Georgia Technical College — PBI
College of Coastal Georgia
Columbus State University
Georgia Institute of Technology — HSI, SFS only
Georgia Southern University
Georgia State University — AANAPISI, PBI, SFS
Gwinnett Technical College
Kennesaw State University
Middle Georgia State University
University of Georgia
University of North Georgia — CSA

Hawaii

Leeward Community College — AANAPISI, ANNH
University of Hawaii, Kapiolani Community College — AANAPISI, ANNH
University of Hawaii, Manoa — AANAPISI, ANNH, SFS
University of Hawaii, Maui College — AANAPISI, ANNH
University of Hawaii, West Oahu — AANAPISI, ANNH

Idaho

Boise State University — SFS, CSA
College of Eastern Idaho
College of Western Idaho
Idaho State University — SFS
University of Idaho — SFS

Illinois

Bradley University
College of DuPage
DePaul University — AANAPISI
DeVry University
Illinois Institute of Technology
Illinois State University
John A Logan College
Loyola University Chicago — SFS
Moraine Valley Community College — HSI

★ ★ ★ ★ ★ ★

Rock Valley College
Roosevelt University — HSI
University of Illinois, Springfield
University of Illinois, Urbana-Champaign — SFS
Western Illinois University

Indiana

Indiana Institute of Technology
Indiana State University
Indiana University — SFS
Indiana University–Purdue University Indianapolis (SFS only)
Ivy Tech Community College
Purdue University
Purdue University Global
Purdue University Northwest — HSI, CSA
Vincennes University

Iowa

Des Moines Area Community College
Eastern Iowa Community College
Iowa State University — AANAPISI, PBI, CSA

Kansas

Butler Community College
Fort Hays State University
Johnson County Community College
Kansas State University — SFS
University of Kansas — SFS
Wichita State University — HSI, SFS

Kentucky

Bluegrass Community and Technical College
Murray State University
Northern Kentucky University
Owensboro Community and Technical College
University of Louisville, Kentucky — PBI, SFS
University of the Cumberlands

Louisiana

Bossier Parish Community College — PBI
Louisiana State University — SFS
Louisiana Tech University — SFS, CSA
University of New Orleans

★ ★ ★ ★ ★ ★

Maine

Southern Maine Community College
University of Maine, Augusta
University of Southern Maine

Maryland

Anne Arundel Community College
Baltimore City Community College
Bowie State University — HBCU
Capitol Technology University — CSA
Cecil College
College of Southern Maryland
Community College of Baltimore County
Hagerstown Community College
Harford Community College
Hood College
Howard Community College — AANAPISI
Johns Hopkins University — SFS, CSA
Montgomery College — AANAPISI, HSI
Morgan State University — HBCU, SFS
Prince George's Community College — PBI
SANS Technology Institute
Towson University — SFS, CSA
United States Naval Academy
University of Maryland — SFS
University of Maryland, Baltimore County — AANAPISI, SFS
University of Maryland Global Campus — CSA

Massachusetts

Assumption University
Bay Path University
Boston University
Northeastern University — SFS, CSA
Simmons University
University of Massachusetts, Dartmouth — SFS
University of Massachusetts, Lowell — AANAPISI
Worcester Polytechnic Institute — SFS, CSA

Michigan

Baker College
Central Michigan University
Davenport University
Delta College
Eastern Michigan University
Ferris State University

★ ★ ★ ★ ★ ★

Grand Rapids Community College
Grand Valley State University
Henry Ford College
Lansing Community College
Macomb Community College
Michigan Technological University — SFS
Northern Michigan University
Oakland University – SFS
University of Detroit, Mercy
Walsh College
Washtenaw Community College — SFS

Minnesota

Alexandria Technical and Community College
Capella University
Century College — AANAPISI
Hennepin Technical College
Metro State University — AANAPISI
St. Cloud State University
St. Cloud Technical, Community College
Walden University

Mississippi

Hinds Community College — HBCU, PBI
Mississippi Gulf Coast Community College
Mississippi State University — SFS, CSA
University of Southern Mississippi

Missouri

Maryville University
Metropolitan Community College, Kansas City
Missouri University of Science and Technology
Southeast Missouri State University
St. Louis Community College
University of Central Missouri
University of Missouri, Columbia — SFS
University of Missouri, Kansas City
University of Missouri, St. Louis
Webster University

Montana

Gallatin College Montana State University
Great Falls College Montana State University
Missoula College

★ ★ ★ ★ ★ ★

Nebraska

Bellevue University
Metropolitan Community College
Northeast Community College
University of Nebraska, Omaha

Nevada

College of Southern Nevada — AANAPISI, HSI
University of Nevada, Las Vegas — AANAPISI, SFS, HSI
University of Nevada, Reno — SFS

New Hampshire

Dartmouth College
Southern New Hampshire University
University of New Hampshire

New Jersey

Brookdale Community College
County College of Morris
Fairleigh Dickinson University — HSI
Hudson County Community College — HSI
Kean University — HSI
New Jersey City University — HSI
New Jersey Institute of Technology — AANAPISI, HSI, SFS
Rowan College, Burlington County
Rowan College, South Jersey — HSI
Rutgers, The State University of New Jersey — HSI
Stevens Institute of Technology — SFS, CSA

New Mexico

Eastern New Mexico University, Ruidoso Branch Community College — HSI
New Mexico Tech (New Mexico Institute of Mining and Technology) — SFS, HSI
University of New Mexico — SFS, HSI

New York

Binghamton University (SUNY at Binghamton) — SFS
City University of New York — HSI, AANAPISI
College of Westchester
Excelsior University
Fordham University — SFS
Mercy University — HSI
Mohawk Valley Community College
New York Institute of Technology — AANAPISI, CSA
New York University — SFS
Pace University — SFS, CSA

★ ★ ★ ★ ★ ★

Rochester Institute of Technology — SFS, CSA
Rockland Community College — HSI
St. John's University — AANAPISI
State University of New York, Albany
State University of New York, Buffalo — SFS
State University of New York, Canton
Suffolk County Community College — HSI
Syracuse University
Touro University
United States Military Academy, West Point
Utica University
Westchester Community College — HSI

North Carolina

Alamance Community College
Blue Ridge Community College
East Carolina University
Fayetteville Technical Community College
Forsyth Technical Community College
Gaston College
Guilford Technical Community College
Montreat College — CSA
North Carolina A&T State University — SFS, HBCU
North Carolina Central University — HBCU
North Carolina State University — SFS, CSA
Pitt Community College
Richmond Community College
Stanly Community College
University of North Carolina, Charlotte — SFS
University of North Carolina, Pembroke — NASNTI
University of North Carolina, Wilmington
Wake Technical Community College
Wayne Community College
Wilkes Community College

North Dakota

Bismarck State College
Minot State University
North Dakota State University
Turtle Mountain Community College — TCCU
University of North Dakota

Ohio

Air Force Institute of Technology
Cedarville University — CSA
Clark State College

★ ★ ★ ★ ★ ★

Columbus State Community College
Franklin University
Kent State University
Lakeland Community College
Sinclair Community College — SFS
Stark State College
Terra State Community College
Tiffin University
University of Cincinnati — SFS
University of Dayton
University of Findlay
Wright State University
Xavier University

Oklahoma

Oklahoma Christian University
Oklahoma City Community College
Rose State College
University of Tulsa — CSA

Oregon

Chemeketa Community College — HSI
Klamath Community College
Mt. Hood Community College
Oregon State University
Portland Community College
Portland State University — AANAPISI

Pennsylvania

Bloomsburg University of Pennsylvania
Carnegie Mellon University — SFS, CSA
Drexel University — SFS
East Stroudsburg University — CSA
Harrisburg University of Science and Technology
Indiana University of Pennsylvania — CSA
Lehigh Carbon Community College — HSI
Messiah University
Mount Aloysius College
Northampton Community College
Pennsylvania Highlands Community College
Pennsylvania State University — SFS, CSA
Pittsburgh Technical College
Robert Morris University — SFS, CSA
Saint Francis University
Saint Vincent College
Temple University

★ ★ ★ ★ ★ ★

University of Pittsburgh
Valley Forge Military College
West Chester University of Pennsylvania

Puerto Rico

Polytechnic University of Puerto Rico — HSI, SFS, CSA
University of Puerto Rico — HSI

Rhode Island

Community College of Rhode Island — HSI
Johnson & Wales University — PBI
New England Institute of Technology
Roger Williams University
University of Rhode Island — SFS

South Carolina

Anderson University
The Citadel — SFS, CSA
Clemson University
South Carolina State University — HBCU
Trident Technical College
University of South Carolina — CSA
University of South Carolina–Aiken

South Dakota

Dakota State University — SFS, CSA
Western Dakota Technical College — NASNTI

Tennessee

Jackson State Community College
LeMoyne-Owen College — HBCU
Roane State Community College
Tennessee Tech University — SFS, CSA
University of Memphis — SFS
University of Tennessee, Chattanooga — SFS
Vanderbilt University
Volunteer State Community College

Texas

Baylor University
Collin College
El Paso Community College — HSI
Hill College
Houston Community College — AANAPISI, HSI
McLennan Community College — HSI

★ ★ ★ ★ ★ ★

Northeast Lakeview College — HSI
Our Lady of the Lake University — HSI
Palo Alto College — HSI
Sam Houston State University — HSI, SFS
San Antonio College — HSI
Southern Methodist University
St. Mary's University — HSI
St. Philip's College — HBCU, CSA
Tarrant County College District — HSI
Texas A&M University — AANAPISI, HSI, SFS, CSA
Texas A&M University, Corpus Christi — HSI
Texas A&M University, San Antonio — HSI
Texas State Technical College — HSI
University of Dallas — HSI
University of Houston — AANAPISI, HSI
University of North Texas — HSI
University of Texas, Dallas — SFS, HSI, CSA
University of Texas, El Paso — SFS, HSI
University of Texas, San Antonio — HSI, SFS, CSA
University of the Incarnate Word — HSI

Utah

Brigham Young University -- SFS, CSA
Southern Utah University
Weber State University
Western Governors University — CSA

Vermont

Champlain College
Norwich University — SFS, CSA

Virginia

ECPI University
George Mason University — AANAPISI, CSA
Germanna Community College
Hampton University — HBCU, SFS
James Madison University — CSA
Laurel Ridge Community College
Liberty University — CSA
Marymount University — SFS, CSA
Mountain Empire Community College
New River Community College
Norfolk State University — HBCU, SFS, CSA
Northern Virginia Community College — AANAPISI, HSI
Old Dominion University — SFS, CSA
Radford University

★ ★ ★ ★ ★ ★

Regent University
Southwest Virginia Community College
Strayer University
University of Virginia
Virginia Commonwealth University — AANAPISI
Virginia Peninsula Community College
Virginia Polytechnic Institute and State University — AANAPISI, SFS, CSA
Virginia State University — HBCU
Virginia Western Community College

Washington

City University of Seattle — CSA
Columbia Basin College — HSI
Eastern Washington University — CSA
Green River College — AANAPISI
Highline College
South Puget Sound Community College
Spokane Falls Community College
University of Washington — AANAPISI, SFS
Western Washington University
Whatcom Community College — SFS

West Virginia

American Public University System
Blue Ridge Community and Technical College
Marshall University — CSA
West Virginia University — CSA

Wisconsin

Chippewa Valley Technical College
Marquette University — SFS
Northwood Technical College
University of Wisconsin, Stout
University of Wisconsin, Whitewater
Waukesha County Technical College