A Report to the President
on

Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce:

Building the Foundation for a More Secure American Future

Transmitted by
The Secretary of Commerce
and
The Secretary of Homeland Security

Contents

Letter of Transmittal ii

Executive Summary 1

Vision for the Cybersecurity Workforce of the Future 4

Imperatives, Recommendations, and Actions 6

Appendix 1: The Charge and Approach 21

Appendix 2: State of the Cybersecurity Workforce 23

Appendix 3: Executive Order 13800 33

Appendix 4: Consolidated Lists of Recommendations and Actions 35

Appendix 5: Request for Information 44

Appendix 6: Webinar and Workshop 45

Appendix 7: National Initiative for Cybersecurity Education (NICE) Strategic Plan 46

Appendix 8: Abbreviations and Acronyms 49

Letter of Transmittal

Dear Mr. President,

We are pleased to transmit our report *Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce* to you in accordance with Executive Order 13800: *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.*

We have subtitled this report "*Building the Foundation for a More Secure American Future,*" recognizing the fundamental role our cybersecurity workforce plays. Operating in both the private and public sectors, cybersecurity practitioners and educators are vital to our national security—especially since other nations are paying greater attention to their cybersecurity workforce needs and the cybersecurity weaknesses of their adversaries.

Our report is based on analysis of available data and the information and views shared by businesses, educational organizations, training and certification providers, government agencies at multiple levels, and individuals. It also takes into account other assessments, including several called for by your Executive Order.

Findings and recommendations address both public and private sector needs. They are specific, forward thinking, and actionable.

These issues are foundational and the Nation must get it right. You have our commitment that we will use our authorities to address the country's cybersecurity workforce skills gaps now.

Wilbur Ross
Secretary of Commerce

Elaine Duke
Acting Secretary of Homeland Security

Transmitted November 16, 2017

Executive Summary

This report responds to the May 11, 2017, Executive Order on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. That order directs the Secretary of Commerce and the Secretary of Homeland Security to:

1) Assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and
2) Provide a report to the President with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors.

Other departments and agencies, industry, academia, and others in the private and public sectors contributed helpful information and views. Previous studies were reviewed to provide additional context.

Basic characteristics of the cybersecurity workforce[1] include:

- The majority of U.S. critical infrastructure is owned and operated by private companies, making its cybersecurity workforce vital.
- The federal government depends heavily on its cybersecurity workforce, supplemented by contractors.
- There are an estimated 299,000 active openings for cybersecurity-related jobs in the United States as of August 2017. Globally, projections suggest a cybersecurity workforce shortage of 1.8 million by 2022.
- Positions needing to be filled range from entry-level jobs attainable with minimal credentials to roles where successful performance is most knowledge-dependent and require advanced academic degrees, multiple certifications, and lengthy on-the-job technical, managerial, and business experience.
- In many instances, employers need workers with specialized knowledge or skills for specific sectors along with cybersecurity competencies.
- Competition for qualified cybersecurity workers is intense across all sectors.
- In comparison to the national workforce, minorities and women are underrepresented among those working in cybersecurity.
- Veterans represent an available and underutilized workforce supply.
- Pay for cybersecurity positions tends to be above the average levels for other positions in many parts of the economy, but in some areas—including the

[1] The cybersecurity workforce is defined in the NICE Cybersecurity Workforce Framework as "members of the workforce with roles and responsibilities that have an impact on an organization's ability to protect its data, systems, and operations." Also see p. 24, Defining the U.S. Cybersecurity Workforce.

federal government—cybersecurity pay is below the level needed to attract the necessary talent.

Key findings include:

- The United States needs immediate and sustained improvements in its cybersecurity workforce situation.
- Employers increasingly are concerned about the relevance of cybersecurity-related education programs in meeting the needs of their organizations.
- Expanding the pool of cybersecurity candidates by retraining those employed in non-cybersecurity fields and by increasing the participation of women, minorities, and veterans as well as students in primary through secondary school is needed and represents significant opportunities.
- There is an apparent shortage of knowledgeable and skilled cybersecurity teachers at the primary and secondary levels, faculty in higher education, and training instructors.
- Hiring considerations—including lengthy security clearance delays and onboarding processes—severely affect the sufficiency of the cybersecurity workforce.
- Comprehensive and reliable data about cybersecurity workforce position needs and education and training programs is lacking—even though the general context and urgency of the situation are obvious.

Key recommendations include:

- The Nation should set an ambitious vision and action plan-of-attack to "Prepare, grow, and sustain a national cybersecurity workforce that safeguards and promotes America's national security and economic prosperity."
- The federal government should lead in launching a high-profile national *Call to Action* to draw attention to and mobilize public and private sector resources to address cybersecurity workforce needs.
- The Administration should focus on, and recommend, long-term authorization and sufficient appropriations for, high-quality, effective cybersecurity education and workforce development programs in its budget proposals in order to grow and sustain the cybersecurity workforce.
- Federal departments and agencies must move quickly to address major needs relating to recruiting, developing, and retaining cybersecurity employees and continue to implement the Federal Cybersecurity Workforce Strategy and the Federal Cybersecurity Workforce Assessment Act of 2015 (FCWAA).
- The private and public sectors need to transform, elevate, and sustain the learning environment to grow a dynamic and diverse cybersecurity workforce by:
    - Emphasizing and expanding opportunities for retraining so that current employees as well as displaced workers and veterans can be reskilled to take on cybersecurity roles.

    - Building on and strengthening hands-on, experiential and work-based learning approaches—including apprenticeships, research experiences, co-op programs, and internships.
    - Using virtual training and assessment environments to augment the limited cadre of teachers and other educators and trainers and to improve assessment tools that match candidates with the skills and knowledge needed to succeed in the workforce and as lifelong learners.
    - Expanding the availability and expertise of teachers and faculty through incentives and policy changes.
    - Providing greater financial assistance and other incentives to reduce student debt or subsidize cybersecurity education and training costs.
- The private and public sectors need to align education and training with employers' cybersecurity workforce needs, improve coordination, and prepare individuals for lifelong careers by:
    - Encouraging educators, training providers, and employers to use the taxonomy and lexicon of the NICE Cybersecurity Workforce Framework as the reference for building workforce development strategies.
    - Developing model career paths for cybersecurity-related positions that can be used in the private and public sectors.
    - Developing interdisciplinary cybersecurity curriculum guidance that incorporates employers' cybersecurity needs.
    - Establishing at least one regional alliance or partnership for cybersecurity education and workforce in each state.
    - Establishing a clearinghouse of information on cybersecurity workforce development education, training, and workforce development programs and initiatives.
- The private and public sectors need to establish and leverage measures that demonstrate the effectiveness and impact of cybersecurity workforce investments. This includes:
    - Ensuring that all cybersecurity education and training programs have an associated set of robust metrics and evaluation mechanisms to track and determine success in terms of the quantity and quality of individuals educated, trained, and ready to fulfill cybersecurity tasks in the workplace.
    - Identifying and using tools to assess aptitude and skills related to cybersecurity positions in the workforce.

Actions are proposed to implement each of these recommendations. Carrying out these recommendations and related actions will ensure that the individuals who perform cybersecurity jobs—and the institutions that educate, train, and employ them—will be better prepared so that the Nation can lead the world in cybersecurity.

Vision for the Cybersecurity Workforce of the Future

> *"…the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace."*
>
> – Executive Order 13800, May 11, 2017

The Nation's private and public sector cybersecurity workforce is the foundation for our future success in protecting U.S. national security and economic prosperity and in maintaining a competitive advantage. Those who perform cybersecurity jobs—and the institutions that educate, train, and employ them—must be well prepared so that the Nation can lead the world in cybersecurity.

The country should declare and embrace a bold and ambitious vision for the future:

Prepare, grow, and sustain a national cybersecurity workforce that safeguards and promotes America's national security and economic prosperity.

Achieving this vision will demand stronger and better partnerships to forge, implement, and sustain strategies that will improve the education, training, recruitment, development, and retention of the U.S. cybersecurity workforce.

The United States will need to enable a cybersecurity workforce equipped with the knowledge, skills, and abilities to stay ahead of, and to cope with, evolving threats and vulnerabilities. Current cybersecurity practitioners must be adequately trained; others from nontraditional backgrounds need to be recruited; and greater numbers of students need the resources and paths required to pursue careers in cybersecurity. How well preeminent universities, faculty, and research efforts do in preparing students and workers will be vital to the country's success—as will the success of other educators, trainers, and employers.

A successful cybersecurity workforce strategy for the Nation should include an enhanced focus upon the value of diversity and inclusion and convert it into a potent resource that can be used to great advantage. Fostering and sustaining a diverse workforce will support the ability to find new talent to carry out this effort and to uncover novel ways to solve problems. Integrating cybersecurity concepts into our primary and secondary education curricula will generate early interest in cybersecurity in a manner that cuts across all sectors of American society. Among workforce-aged adults, veterans, women, minorities, and the economically disadvantaged should be aggressively recruited, without compromising required standards.

The United States must address the cybersecurity workforce as a constantly evolving ecosystem if the workforce is to be sustainable and effective. Those in entry-level positions—as well as those at the most advanced levels of cybersecurity research and education—must be able to move fluidly among positions that will keep them current and embody lifelong learning. *The Nation needs a larger, more mobile, and more capable cybersecurity workforce.*

Academia, training providers, and private sector employers must innovate, collaborate, and communicate more effectively. They must find new models for education and training to suit each generation of students and professionals.

The federal government also has important and expanding cybersecurity workforce-related leadership roles:

- Focusing the Nation's attention and voicing the urgent needs and opportunities to grow the U.S. cybersecurity workforce to meet national security needs and enhance economic prosperity;
- Drawing attention to and mobilizing the vital elements of the cybersecurity education, training, and workforce ecosystem;
- Setting the standard for excellence by supporting and promoting effective practices and solutions—including tools to assess individuals and programs, models that describe cybersecurity work roles and tasks, and cybersecurity-related educational curricula;
- Enabling the development of innovative cybersecurity education and training approaches and methods for validating proficiencies that are scalable and sustainable throughout the workforce and the ecosystem;
- Leading by example to demonstrate how to identify, prioritize, and manage the cybersecurity workforce; and
- Convening key players in both the private and public sectors to forge agreement and spur collective action with real impacts to cybersecurity; and

The federal government must lead in the effort to close U.S. cybersecurity workforce gaps—something that can be achieved only by changing the way the country views and practices cybersecurity. Meaningful change means constantly adopting new technologies and approaches while building upon those already deemed effective. The Nation has proven to be especially innovative and adaptable before and capable of mobilizing the public and private sectors to meet urgent national challenges—traits that will be essential to educating and developing the cybersecurity workforce for the future.

The following section identifies high-level imperatives and recommendations to help achieve the cybersecurity workforce vision for the future. Although the imperatives are intentionally directed toward government action, in many cases the imperatives support both the private and public sectors.

Imperatives, Recommendations, and Actions

Imperative 1:
Launch a national Call to Action to draw attention to and mobilize public and private sector resources to address cybersecurity workforce needs.

The seriousness of the Nation's cybersecurity workforce gaps merits a high-level initiative to raise awareness and create a sense of urgency about the importance of growing and sustaining a world-class cybersecurity workforce, ways to achieve that goal, and pathways to enter that workforce. Both short- and long-term efforts need much greater attention from senior government and industry leaders to individual employees, teachers, students and their parents, and private citizens.

❖ **Recommendation 1.1**

The Administration should convene senior leaders in business, education, and government to jointly develop and launch a high-profile *Call to Action* to achieve the Nation's vision of a cybersecurity workforce that safeguards and promotes America's national security and economic prosperity.

This wide-ranging initiative should:

- Fully engage thought leaders and policy makers, cybersecurity workers from all sectors, those with marketing expertise, educational technology developers and providers, and others in the private sector in addition to educators, students, and career advisors from primary through higher education;
- Include an emphasis on positive developments and outcomes and encourage increased investments;
- Cross generational boundaries to reach students as well as those in entry-, mid-, and advanced-levels in their careers, regardless of whether they are currently considering joining the cybersecurity workforce;
- Include underrepresented and disadvantaged populations;
- Build upon and promote recommendations in this report and the Strategic Plan of the National Initiative for Cybersecurity Education (NICE);[2] and
- Help make cybersecurity an *impactful, meaningful, and patriotic calling that is critical to enhancing national security*.

✓ **Action 1.1.1**

The Administration should actively engage senior Executive Branch and business and academic leaders in developing the *Call to Action*. This effort should include

[2] NICE is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. It is led by the U.S. Commerce Department's National Institute of Standards and Technology (NIST). See Appendix 7 and https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan.

leaders from the education and training communities, state and local as well as tribal government representatives, and private sector officials from critical infrastructure sectors and technology and cybersecurity-oriented companies. An action plan should be developed to implement this recommendation as well as Recommendations 1.2 and 1.3.

✓ **Action 1.1.2.**
Senior federal officials should encourage the private sector to broaden and deepen its support for cybersecurity education, training, and workforce efforts, including expanding and committing to long-term support for these activities. Special attention should be given to owners and operators of critical infrastructure sectors. Departments and agencies should identify the most effective private sector programs and the contributions of private companies and nonprofit organizations for positive attention.

Recommendation 1.2
Senior Administration officials should widely socialize the country's cybersecurity workforce challenges as a matter of national and economic security and commit their departments and agencies to creatively, aggressively, and visibly address this pressing need.

✓ **Action 1.2.1**
With the urgency of a national mobilization, federal department and agency heads should elevate attention to U.S. cybersecurity workforce needs and strategies in their communications with internal and external audiences and implement all relevant recommendations in this report.

❖ **Recommendation 1.3**
The Administration should include funding in the President's budget and work with Congress to provide long-term authorization and sufficient appropriations for **cybersecurity education and workforce development programs in order to sustain and expand current efforts. Priorities should be given to those that address cybersecurity workforce development in effective and innovative ways and those that support federal workforce initiatives**. Support for all levels of the education enterprise, from primary to secondary schools to the most advanced levels of higher education, should be eligible for expanded support. Successful programs rely on sustainable funding to allow them to be managed with a longer-term view and to adapt. Several programs are singled out in the recommendations that follow.

✓ **Action 1.3.1**
The Administration should develop a legislative proposal to amend the Cybersecurity Enhancement Act of 2014 to codify the National Security Agency/Department of Homeland Security (NSA/DHS) National Centers of Academic Excellence (CAE) in Cybersecurity program. In addition, the Administration should include funding in the President's budget for annual

authorization of appropriations for the NSA/DHS CAE program to systematically grow and sustain support of the institutions critical to growing the cybersecurity workforce of the future.[3]

✓ **Action 1.3.2**

The Office of Management and Budget (OMB) should utilize existing federal departments' and agencies' cybersecurity spending data to evaluate the effectiveness of resources to this initiative and increase or decrease resources, as appropriate, to the most effective and efficient government programs. To aid in that process, Imperative 4 includes recommendations to improve the availability and use of information about the effectiveness and efficiency of these programs.

✓ **Action 1.3.3**

To reduce confusion and ensure alignment, federal departments and agencies should strive to standardize around the use of a single definition of "cybersecurity workforce" based on the NICE Cybersecurity Workforce Framework (NICE Framework).

❖ **Recommendation 1.4**

Federal departments and agencies must move quickly to address major needs relating to *recruiting, developing, and retaining* cybersecurity employees as they continue to implement the Federal Cybersecurity Workforce Strategy[4] and the Federal Cybersecurity Workforce Assessment Act (FCWAA).[5] These actions must be given close attention by senior agency leaders to ensure that timelines are met.[6]

✓ **Action 1.4.1**

The Office of Personnel Management (OPM) with the support of the Chief Human Capital Officer (CHCO) Council and CIO Workforce Council, federal departments and agencies, should be provided more clearly defined and readily available guidance and resources to identify and quickly recruit cybersecurity talent. This could include, among other tools, standardized position descriptions, job analysis and assessment tools, and career path guidance based on the NICE Framework to identify opportunities to bring skilled staff into the cybersecurity workforce. Federal agencies must also better coordinate recruitment outreach across the government for federal cybersecurity workers and make better use of cybersecurity camps, competitions and challenges, games, contests, and other interactive opportunities.

---

[3] The NSA/DHS CAE program has grown from 186 colleges and universities in 2015 to over 230 in 2017. Designated CAE institutions exist in 46 U.S. states. The program has many initiatives under way, made possible by one-time funding provided in FY 2017, that will help to advance imperatives and recommendations in this report.

[4] http://www.ncsl.org/documents/statefed/Federal_Cybersecurity_WorkforceStrategy.pdf.

[5] The FCWAA was enacted as a part of the Consolidated Appropriations Act of 2016, Pub. L No. 114-113, Div. N, Title III, 129 Stat. 2242, 2975-77 (Dec. 18, 2015).

[6] GAO, *Federal Efforts Are Under Way That May Address Workforce Challenges*, GAO-17-533T (Washington, D.C.: April 4, 2017).

OPM should align classification standards with the current cybersecurity landscape and provide a library of positions descriptions that are made available to all departments and agencies.

✓ **Action 1.4.2**

OPM and federal departments and agencies should explore the use of direct hire or other authorities and salary incentives, to address recruiting difficulties and shortages of cybersecurity expertise. National Background Investigations Bureau, the Security Executive Agent (Office of the Director of National Intelligence), and Suitability Executive Agent (OPM), in partnership with federal departments and agencies, should speed up security clearances by bringing additional background investigators on board while continuing to automate background investigation processes, taking greater advantage of interim clearances, and examining and addressing challenges in applying reciprocal clearances across multiple agencies.

❖ **Recommendation 1.5**

The federal government should launch a vigorous effort to recruit cybersecurity workers from large and diverse pools of candidates who are underutilized or underrepresented in the cybersecurity workforce. This includes veterans, women, and minorities.[7]

✓ **Action 1.5.1**

OPM should lead federal departments and agencies in a government-wide outreach strategy to educate and raise awareness among students, recent graduates, current federal employees, and veterans transitioning to the civilian workforce through educational institutions, military installations, and other organizations. This effort includes reaching diverse talent pools, including women, minorities, and individuals with disabilities. It also includes providing technical assistance and guidance to federal cybersecurity recruitment teams to target talent with the skill set and experience needed to successfully fill cybersecurity positions.

✓ **Action 1.5.2**

Federal agencies should expand their use of recruitment tools including websites (such as www.cybercareers.gov), videos, and social media with additional functionality and enhanced branding to attract a richer and more diverse candidate pool and preview federal cybersecurity careers. They also should expand use of cybersecurity competitions, challenges, contests, and other interactive opportunities, as is the case with Action 1.4.1.

[7] The Department of Defense (DoD) employs a large number of veterans working in cybersecurity positions.

Imperative 2:
Transform, elevate, and sustain the learning environment to grow a dynamic and diverse cybersecurity workforce.

Learning environments for cybersecurity-related content span the educational system from primary through higher education and are also an important factor for training and certification providers. Learning also takes place online and in alternative venues such as virtual labs, Massive Open Online Courses (MOOCs), boot camps, summer camps, conferences, competitions, and in the workplace. Most importantly, education and training must translate into learning outcomes that allow individuals to demonstrate cybersecurity competencies and support lifelong careers.

The Nation must continue to build the knowledge and skills of those in the cybersecurity workforce so that they can address local and national needs. The United States also needs to expand the pool of talented individuals who are interested in entering or switching to a cybersecurity career, whether they are in primary or secondary school or are long-established employees who are candidates for retraining. Better cooperation and collaboration, including collecting and sharing information about successful approaches and curricula, is called for—as is being innovative in using modern teaching methods that leverage emerging learning platforms; this includes using virtual or cloud-based technologies, challenges, and competitions.

The United States cannot achieve a cybersecurity workforce vision of preeminence without increasing the levels of investment and support of its learning infrastructure, including teachers, faculty, researchers, and instructors. That involvement and support must come from both the public and private sectors and be available to students and workers at any point in their education or career.

These resources—including the time and effort of educators and students—are valuable and must be used wisely. Expanding the focus on, and commitment to, metrics and asking challenging questions to program managers and educators alike, can lead to better evaluation, prioritization, and selection of education and training programs. (See Imperative 4.)

❖ **Recommendation: 2.1**
Emphasize retraining programs so that current employees can be reskilled to take on cybersecurity roles.

✓ **Action 2.1.1**
Government at all levels and the private sector should consider assessing the cybersecurity-related aptitudes and abilities of employees who recently lost their jobs, will be laid off, or are planning to retire (including police, firefighters, and military) as part of a comprehensive recruitment scheme. Candidates for

cybersecurity-related education and training should be selected from individuals who demonstrate aptitude for cybersecurity work. (See Recommendation 4.2.)

✓ **Action 2.1.2**
The Interagency Council on Veterans Employment, co-chaired by the Secretaries of the Department of Labor (DOL) and Veterans Affairs (VA) with the OPM Director serving as vice chair and chief operating officer, should develop and implement plans to provide career guidance and identify education and training services that encourage veterans with cybersecurity experience to transition to federal positions.

✓ **Action 2.1.3**
Involve and incentivize NSA/DHS CAE-designated institutions or other local or regional educational or training providers to assist with employee education, training, and career awareness activities—including career fairs and career advising.

❖ **Recommendation: 2.2**
Government, the private sector, and academia should build on and strengthen hands-on, experiential, and work-based learning approaches—including apprenticeships, research experiences, co-op programs and internships—as part of their strategies for meeting cybersecurity workforce needs. This recommendation is consistent with Executive Order 13801, *Expanding Apprenticeships in America*.[8] The apprenticeship training model is based on real-world tasks, timelines, and experience; it is well suited to preparing the cybersecurity workforce. Internships also have proven successful, including in the STEM communities where they are providing science and engineering organizations with a more robust pipeline to build their workforce.

✓ **Action: 2.2.1**
Agencies should utilize additional hiring authorities and programs such as the Pathways Program (which includes internships, opportunities for recent graduates, and the President's Management Fellowship program) and apprenticeships to grow cybersecurity talent and offer opportunities to students and recent graduates to rapidly integrate participants into the federal workforce in a way similar to the recent authorization that DoD laboratories received for STEM employees.

✓ **Action 2.2.2**
DOL should build cybersecurity apprenticeships into applicable Employment & Training Administration-funded programs, and provide other agencies with advice and technical assistance for their apprenticeship programs.

[8] See https://www.whitehouse.gov/the-press-office/2017/06/15/presidential-executive-order-expanding-apprenticeships-america.

✓ **Action 2.2.3**
Colleges and universities—especially community colleges—should partner with their local, regional, and national business community to support apprenticeship programs; this includes expanding on the few college-level cybersecurity apprenticeship programs. These should focus on a select group of cybersecurity job categories, gain employer commitment to the concept, and launch and evaluate additional pilots to gain the needed experience before full-scale expansion.

❖ **Recommendation 2.3**
Private and public sector organizations should sponsor the use of virtual training and assessment environments to augment the limited cadre of teachers and assessment tools that match workforce needs. Gaming and simulations, such as cyber ranges and the NICE Challenge Project, are examples of such innovative environments.

✓ **Action 2.3.1**
All federal agencies involved in cybersecurity education and training should develop and deploy more training and talent assessment environments and programs—including challenges.[9] NSA, the National Science Foundation (NSF), and DHS should coordinate with NICE on a series of Grand Challenges to catalyze and incentivize entrepreneurial activity that would result in either government selection of a solution or contributions to a market where the best and most affordable products survive. Academic and private sector organizations should be invited to address priority needs for technological tools or capabilities, including career exploration applications, aptitude assessments, proficiency examinations, and job seeker-employer matching solutions.

✓ **Action 2.3.2**
Agencies should make greater use of cybersecurity competitions, including in professional development of those in the cybersecurity workforce.

❖ **Recommendation 2.4**
Expand the availability and expertise of teachers and faculty through a combination of incentives and policy changes.

✓ **Action 2.4.1**
The Administration should encourage employers and academic institutions to initiate or support programs attracting and allowing experienced cybersecurity workers to supplement existing curricula and improve effectiveness in delivering cybersecurity-related knowledge in primary through higher education, including

[9] See, for example, NSA's Day of Cyber career exploration tool; CyberStart's aptitude test; the NICE Challenge that could serve as a proficiency exam; and SkillSmart, which connects employers with job seekers based on skills.

regular classroom situations as well as mentoring and other environments.[10] Introducing cybersecurity practitioners into the teaching environment also can make the field more attractive to potential future members of the cybersecurity workforce.

✓ **Action 2.4.2**
Educational institutions and businesses should encourage qualified cybersecurity practitioners to serve as teachers, professors of practice, guest presenters, or adjunct faculty. This includes changes in policies relating to employee contracts and credentialing that would permit practitioners to teach alongside partner teachers, establishing guest instructor programs with industry, and adjusting requirements for teaching credentials.

✓ **Action 2.4.3**
Increase the capacity of the teaching workforce through intensive professional development for current teachers regardless of their formal background and current teaching focus. More schools should consider opportunities for team teaching with industry professionals and incentives for teacher preparation programs to incorporate cybersecurity into the curriculum of future educators.

✓ **Action 2.4.4**
The U.S. Department of Education (ED) should develop a national recognition program that identifies and acknowledges school districts, colleges and universities, employers, and individuals that are role models in enhancing the development of future cybersecurity workers. Senior Administration officials should visibly support this program.

✓ **Action 2.4.5**
Use federal cybersecurity education and training programs as a vehicle to recognize teachers and faculty who provide instruction in cybersecurity education, including "train the trainer" experiences.

❖ **Recommendation 2.5**
Strengthen the capacity for high schools to prepare students with the range of knowledge, skills, and abilities to enter into cybersecurity career and educational pathways by supporting the development of rigorous Career Technical Education (CTE) programs and education of the teaching workforce.

✓ **Action 2.5.1**
Support the development of an elite comprehensive career technical education program of study in cybersecurity through the existing Carl D. Perkins Career and

[10] NSA's MEPP, for example, allows agency employees to serve up to 140 hours annually in elementary, middle, and high schools as guest speakers, visiting teachers, and mentors.

Technical Education Act. The program should align with the NICE Framework; deliver rigorous academic, technical, and employability skills; and give credits that transfer directly to NSA/DHS CAE-designated institutions.

✓ **Action 2.5.2**
Increase the capacity of the CTE teacher workforce to incorporate cybersecurity instruction through intensive professional development and incentives for current teachers.

❖ **Recommendation 2.6**
Federal and state governments, as well as the private sector, should consider providing greater financial assistance and other incentives to reduce student debt or subsidize the cost of cybersecurity education or training.

✓ **Action 2.6.1**
The Administration should include in the President's proposed budget increased federal funding for the CyberCorps®: Scholarship for Service (SFS) program administered by NSF to dramatically increase the number of students studying cybersecurity and entering the federal cybersecurity workforce.

✓ **Action 2.6.2**
Modify student loan repayment programs to provide a direct financial incentive for individuals to take cybersecurity jobs in federal, state, local, or tribal governments or economically distressed regions. Cybersecurity-related faculty positions with public or private colleges or universities providing two-year, four-year, and graduate degrees in NICE Framework-recognized specialty areas also should be eligible for repayment.[11]

✓ **Action 2.6.3**
Provide additional federal or state tax incentives for cybersecurity-related education and training. Incentives could encompass employer tax breaks to support employee participation in training programs, including for-credit or noncredit academic courses to develop knowledge or skills that correspond to a NICE Framework work role.

❖ **Recommendation 2.7**
Expand government and private sector support for high-quality cybersecurity camps, boot camps, and similar programs designed to educate and train teachers or students.

[11] Federal agencies already have the authority to repay loans. However, this authority could be enhanced with legislation to allow higher maximum payments.

✓ **Action 2.7.1**
Develop a mechanism for providing need-based scholarships to students and teachers to participate in high-quality camps or professional development programs.

✓ **Action 2.7.2**
The Administration should propose in the President's budget increased and sustained funding for the GenCyber program through the NSA and NSF—to allow it to grow to 300 camps, covering all 50 states, by 2020. This would reach approximately 150,000 students per year (15,000 through direct participation and 135,000 indirectly through teacher participation).

Imperative 3:
Align education and training with the cybersecurity workforce needs of employers and prepare individuals for lifelong careers.

The *perceived* and *actual* cybersecurity workforce needs of employers in companies, government agencies, and other organizations need to be better aligned—and then education and training curricula should be matched with those workforce needs. The NICE Framework serves as the common lexicon that can improve communication in the ecosystem.

Some employers request specific education, experience, or certification requirements in cybersecurity job opportunity announcements that are misaligned with actual job responsibilities. Consequently, many positions remain unfilled—or may be filled by employees who possess the desired credentials but do not have the essential knowledge, skills, and abilities to perform the work. Employers are challenged to assess candidates' competencies rather than their formal education or training credentials. Finding ways to allow candidates who can demonstrate work experience as a complement to their formal education or training increases the pool of potential employees.

❖ **Recommendation 3.1**
The Executive Branch should strongly encourage educators, training providers, and employers to use the taxonomy and lexicon of the NICE Framework as the reference for building workforce development strategies.

✓ **Action 3.1.1**
To help codify cybersecurity roles throughout the U.S. workforce, NICE should more widely promote its Framework, which defines cybersecurity work roles, and collect and share information about how it is being used. That Framework should be updated regularly with even broader input; it must be dynamic and expanded to cover additional work roles.

✓ **Action 3.1.2**
NICE should educate and encourage employers to align cybersecurity tasks with corresponding Knowledge, Skills, and Abilities (KSAs) rather than use generalized job descriptions that incorporate outdated degree, certification, and experience requirements. OPM should also update qualification standards to incorporate position requirements such as degree levels, certifications, and experience.

✓ **Action 3.1.3**
Just as federal government departments and agencies are required to use the NICE Framework to identify and define work roles and tasks, federal contractors should be required to use the same lexicon for these purposes.

✓ **Action 3.1.4**
The Council of Governors, National Governors Association, and the National Association of State Chief Information Officers should encourage use of the taxonomy and lexicon of the NICE Framework by state, local, and tribal governments.

❖ **Recommendation 3.2**
Develop model career pathways for cybersecurity-related positions that can be used in the private and public sectors. These pathways should spell out education, training, and other experiences that align with employers' skill needs and prepare an individual to be successful in entering or advancing in a cybersecurity career.

✓ **Action 3.2.1**
The Interagency Working Group on Career Pathways, led by DOL, should partner with NICE, ED, Department of Commerce (DOC), OPM, and other public and private sector organizations to develop and raise awareness about model career pathways for cybersecurity-related positions.

✓ **Action 3.2.2**
DHS, in consultation with other federal government civilian agencies and the private sector, should lead the development of capability indicators required for entry-level, mid-level, and advanced-level work roles in the NICE Framework.

❖ **Recommendation 3.3**
The federal government should partner with the private sector and academia to develop interdisciplinary cybersecurity curriculum guidance that addresses the need for widely accepted and shareable cybersecurity curricula that incorporate employers' cybersecurity needs.

✓ **Action 3.3.1**
NICE, NSF, the NSA/DHS CAE program, and the NSA College of Cyber should continue to engage employers, academia, and professional societies to coordinate and establish cybersecurity curriculum guidance.

✓ **Action 3.3.2**
The Administration should propose sustained funding for the curriculum development initiative operated by the NSA College of Cyber based on one-time FY 2017 funding. This initiative is already funding development of a publicly available cybersecurity curriculum and online mechanism for promoting and sharing it—similar to Skills Commons,[12] a DOL digital library of Workforce Training Materials that includes cybersecurity content.

✓ **Action 3.3.3**
State and local governments and the private sector should integrate cybersecurity into existing STEM programs, especially computer science courses, and develop cybersecurity topics and examples for use in the broader primary school curricula; they should take advantage of the large number of programs already under way and the curricula already developed.[13]

❖ **Recommendation 3.4**
Establish cooperative agreements between NICE and at least one regional alliance or partnership for cybersecurity education and workforce in each state. These collaborative efforts should facilitate local and regional partnerships of employers, educational institutions, local governments, and community organizations to better meet the needs of local and regional industry and the workforce.

✓ **Action 3.4.1**
Develop sustainable mechanisms within communities to identify employer cybersecurity workforce needs based on the NICE Framework. The Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development[14] is an example of a collaborative private-public approach that is yielding early successes. Many locally based initiatives have begun to emerge and are having positive results, closely connecting education efforts with local employers' needs.

❖ **Recommendation 3.5**
The federal government should establish a clearinghouse of information on cybersecurity workforce development education, training, and development programs and initiatives. The clearinghouse, which would serve the public and

---

[12] See https://www.skillscommons.org/.
[13] Potential exemplary programs include the NICERC (National Integrated Cyber Education Center) curriculum funded by DHS, Microsoft's TEALS (Technology Education and Literacy in Schools) program, and efforts by Code.org.
[14] RAMPS is a federal program funded by the NICE Program Office at NIST. For more information, visit https://www.nist.gov/nice/regional-alliances-and-multistakeholder-partnerships-stimulate-ramps.

private sectors, should include knowledge from allies and the wider global community and address:

- New and existing government programs and initiatives, such as research, pilot programs and grants, for the purposes of collaboration, information sharing, and efficient resource management; and
- Private sector education and training offerings that will provide employers, students, and transitioning workers information on content, quality, cost, and the types of financial assistance available.

✓ **Action 3.5.1**

DOC should run the clearinghouse, administered by NICE in cooperation with NICE partner departments and agencies. These organizations currently share information and help to coordinate many cybersecurity education and training initiatives across the ecosystem. Special attention should be given to programs seeded with federal funding. The clearinghouse needs to be updated regularly.

❖ **Recommendation 3.6**

The federal government should lead efforts to improve the country's understanding of employers' specific cybersecurity workforce needs.

✓ **Action 3.6.1**

NICE should work with its grantees to expand the CyberSeek tool's capabilities by identifying where the greatest job demands are by sector or critical infrastructure and by identifying the level of the positions (i.e., entry/mid-level/advanced).

✓ **Action 3.6.2**

DHS should prepare a plan in conjunction with DOC, DOL, the Department of State, and the Office of the Director of National intelligence (ODNI) to regularly gather comparative information needed to better track and understand the Nation's dynamic cybersecurity workforce needs. Special attention should be given to critical infrastructure sectors as well as to the situation and progress being made by allies and competitors.

Imperative 4:
Establish and leverage measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

To reasonably assess the sufficiency of efforts to educate and train the American cybersecurity workforce, far better indicators and measurements of sufficiency are needed. These metrics should include more accurate information that will help to narrow the uncertainty about *numbers* and *types* of cybersecurity positions needing to be filled in the short-, mid-, and long-term, the situation for U.S. critical infrastructure sectors, and how the United States compares with global competitors. Information and feedback from employers about job applicants' readiness for their specific competency needs is sparse. Furthermore, some education and training

providers lack timely information about the specific Knowledge, Skills, and Abilities (KSAs) that employers need for their cybersecurity workers.

In many cases, those sponsoring cybersecurity education and workforce programs use insufficient metrics to indicate program effectiveness. Some may emphasize the quantity of students enrolled in a program irrespective to the overall outcome—such as those with successful job placement after completion. Gauging employers' satisfaction of how well these graduates perform is even more challenging. A variety of metrics could help determine a program's efficacy, including measures of effectiveness, quality, relevance, currency, practicality, global acceptance, and perceived and actual value to employers.[15] These measurements could then be applied to programs aimed at students not yet in the workforce, as well as entry-, mid-, or advanced-level employees.

Decision makers generally appear to lack the information required to choose the best courses of action about the value of investments in one approach or program versus another. In all cases, to better inform sponsors and shape policy, more and better information needs to be collected regarding the *inputs*, *outputs, outcomes, and impacts* of efforts.

❖ **Recommendation 4.1**

All programs related to cybersecurity workforce education or training should have an associated set of robust metrics and evaluation mechanisms to track and determine success in terms of the quantity and quality of individuals educated, trained, and ready to fulfill cybersecurity tasks in the workplace.

✓ **Action 4.1.1**

NICE should establish a clearinghouse that *identifies effectiveness metrics already used* by one or more organizations and that are deemed helpful by federal agencies. The clearinghouse should build on information contributed by the NSA/DHS CAE community[16] and others.

✓ **Action 4.1.2**

NICE should lead an effort to *develop a portfolio of reliable metrics* for measuring and evaluating cybersecurity workforce programs, including common performance measures included in the Workforce Innovation and Opportunity Act (WIOA). NICE should work with NSF and DOL to convene experts in government, academia, and business to identify how to measure the outputs and outcomes of cybersecurity workforce education and training programs, which should include: current metrics and their usefulness, the identification and prioritization of key gaps in metrics, and a recommended plan of action to address these gaps.

---

[15] SANS Institute. (2017). *Reply to Request for Information (RFI).* Retrieved from https://www.nist.gov/sites/default/files/documents/2017/08/02/sans_institute.pdf.

[16] The NSA/DHS CAE community is identifying effectiveness metrics as part of a one-time grant during FY 2017.

✓ **Action 4.1.3**

All organizations receiving federal funding to provide cybersecurity workforce education and training services should use a set of robust metrics and evaluation mechanisms to track and determine success in terms of the quantity and quality of individuals educated and trained.

❖ **Recommendation 4.2**

Federal agencies should work with educational institutions to identify and use currently available tools to assess aptitude and skills related to cybersecurity positions in the workforce. Priority improvements needed in assessment tools should be identified and addressed**.**

✓ **Action 4.2.1**

The Executive Branch should coordinate federal plans to develop centrally available and reliable tools to assess 1) aptitude for a cybersecurity career and 2) the technical readiness to demonstrate the possession of KSAs and the ability to perform specific tasks identified in the NICE Framework. NSA, NSF, DHS, and NICE should collaborate in these efforts and all federal departments and agencies should make maximum use of these assessment tools.

Appendix 1:
The Charge and Approach

The Charge

On May 11, 2017, President Trump issued an *Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.*[17] In part, the order states that it is the policy of the United States "to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace." Consequently, the Secretary of Commerce and the Secretary of Homeland Security are directed to:

1) Assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and

2) Provide a report to the President with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors.

This report defines the cybersecurity workforce as "members of the workforce with roles and responsibilities that have an impact on an organization's ability to protect its data, systems, and operations."[18] The terms "cybersecurity jobs" and "cybersecurity-related jobs" often are used interchangeably in reference to positions held by those who are part of this workforce.

The Approach

The Executive Order directed the Secretaries of Commerce and Homeland Security to conduct an assessment and prepare a report in consultation with the Secretary of Defense, the Secretary of Labor, the Secretary of Education, the Director of the Office of Personnel Management, and other federal agencies. These departments and agencies and other federal organizations constituted the study team.[19]

Industry, academia, and others in the private and public sectors informed the analysis and made recommendations. This was accomplished in three ways: via a webinar, a Request for Information (RFI) published in the *Federal Register,* and a workshop. More than 95 responses were received in response to the RFI[20] and

---

[17] See https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

[18] See Defining the Cybersecurity Workforce, p. 24 and the NICE Framework: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[19] Other departments and agencies involved in this study include the Department of Health and Human Services, the Department of Energy, the National Science Foundation, and the Federal Communications Commission.

[20] See Appendix 3.

approximately 125 individuals representing industry, academia, and government participated in the workshop.[21]

This report reflects the input received and considers the findings and recommendations from several prominent previous studies.

Assessment of Scope of Efforts to Educate and Train the Workforce
The assessment of scope of effort ("scope assessment") included all aspects of education and training of the workforce, along with related issues of recruitment, hiring, and retention.

Many previous studies have made it clear that every current and potential user of information technology has a role in cybersecurity. Better preparation of students and better awareness of the public about cybersecurity will help the country better secure its digital resources. For purposes of this report, the public's role is not included, except as members of the public enter or consider entering the cybersecurity workforce.

Assessment of Sufficiency of Efforts to Educate and Train the Workforce
In determining the sufficiency of the U.S. cybersecurity workforce ("sufficiency assessment"), this study considered current and future:

1) Cybersecurity job needs, including the knowledge, skills, and abilities (KSAs) as well as the competencies *required by employers* in both the private and public sectors;
2) *Ability of employers* to identify and employ those with cybersecurity KSAs or competencies to effectively meet their cybersecurity needs;
3) Capability of education and training providers—both in terms of quantity and quality—to meet the needs of *students and others* desiring to gain or advance their cybersecurity capabilities;
4) Degree to which the cybersecurity workforce currently meets the *Nation's* needs; and
5) Degree to which we can expect the cybersecurity workforce to meet the *Nation's future* needs based on current efforts.

In short, the sufficiency assessment addressed two main questions:

1) How is the Nation doing in meeting the needs of *students and employees*, *employers,* and the needs of the *Nation in terms of cybersecurity education, training, and readiness to carry out cybersecurity responsibilities*?
2) What could be done to better meet those needs and who needs to take action?

[21] See Appendix 4.

Appendix 2:
The State of the Cybersecurity Workforce

A. Cybersecurity Workforce Knowns and Unknowns

The assessment of the state of the cybersecurity workforce ("status assessment") sought quantitative and qualitative information on the state of the Nation's cybersecurity workforce and the underlying education and training system that prepares that workforce to function effectively.

A major finding of this assessment is that *reliable, quantitative information about the cybersecurity workforce is lacking.* There are too few measures regarding the numbers and kinds of cybersecurity-related positions needed and the effectiveness of education and training programs in preparing the cybersecurity workforce.

Contributing factors are:

1) The rapidly changing nature of cybersecurity-related work, including those jobs in which cybersecurity tasks make up only a portion of assigned responsibilities;
2) The slow adoption of a taxonomy and common lexicon to describe cybersecurity work consistently, presenting data analysis challenges when using job openings to measure the cybersecurity workforce and the needs of employers;
3) The decentralized nature of the U.S. education and training system; and
4) The absence of consensus on standardized cybersecurity curricula and evaluation methods.

Reliable information about the numbers and types of unfilled positions has been difficult to obtain.[22] In 2016, the National Initiative for Cybersecurity Education (NICE)[23] funded the *CyberSeek* website[24] to provide detailed, actionable data about supply and demand in the cybersecurity job market.[25] Based on that data, which is improved but still would benefit by more robust information, there are an estimated 299,000 active openings for cybersecurity-related jobs in the United States as of August 2017. Globally, projections suggest a cybersecurity workforce shortage of 1.8 million by 2022.[26]

The status assessment illustrates the need for more reliable data. This report identifies some of those most critical data needs and recommends several steps to

---

[22] Some survey data on cybersecurity jobs has been generated by local and regional organizations. For example, see https://sdccoe.org/wp-content/uploads/2015/01/CCOE EIS-2016-.pdf.
[23] NICE is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. It is led by the U.S. Commerce Department's National Institute of Standards and Technology (NIST).
[24] The National Initiative on Cybersecurity Education (NICE) provided a grant to CompTIA.
[25] See http://cyberseek.org/.
[26] (ISC)[2] *Response to NIST RFI* (2017). See https://www.nist.gov/sites/default/files/documents/2017/08/02/isc2.pdf.

address them. Despite the lack of comprehensive, robust data about important aspects of the cybersecurity workforce as well as education and training, the status assessment found that there is a real need for improvement in the U.S. cybersecurity workforce's development and that today's situation warrants both immediate and sustained attention. The following sections describe the Nation's cybersecurity workforce and education needs, including areas for which quantitative data are lacking.

B. Defining the U.S. Cybersecurity Workforce

The cybersecurity workforce is defined as "members of the workforce with roles and responsibilities that have an impact on an organization's ability to protect its data, systems, and operations."[27] For the purposes of this report, the cybersecurity workforce refers to those individuals performing the work roles contained in the NICE Cybersecurity Workforce Framework.[28]. Those who fill cybersecurity positions have varying backgrounds and skill levels, however, and their responsibilities vary widely depending on an organization's needs. Cybersecurity knowledge, skills, and abilities are applied not only by individuals operating and defending complex technical systems vital to organizations, but also by anyone in the organization who has a role that can reduce the organization's cybersecurity risk.

Who Manages and Who Makes Up the Cybersecurity Workforce?

The federal government depends heavily on its cybersecurity workforce, which issupplemented by contractors. The fact that so much of the U.S. critical infrastructure is owned and operated by the private sector makes it clear that the private sector's capabilities are vital and must be addressed to protect the country's digital infrastructure. Cybersecurity workforce issues are a national problem and need to be addressed by the public *and* private sectors, with the heavy involvement of education and training enterprises.

Positions needing to be filled range from entry-level jobs that can be performed by high school graduates who have received additional training through coursework, apprenticeships, or on-the-job experience, to the most knowledge-dependent, requiring advanced degrees coupled with lengthy on-the-job experience. Positions requiring the highest levels of education and training along with managerial and business experience appear to be the most difficult to fill, especially in the federal government.[29]

---

[27] See the NICE Framework: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[28] The NICE Cybersecurity Workforce Framework categorizes and describes cybersecurity work. The NICE Framework serves as a fundamental reference resource to support a workforce capable of meeting an organization's cybersecurity needs. It provides organizations with a common, consistent lexicon that categorizes and describes cybersecurity work. See http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[29] The RAND Corporation (2014). *Hackers Wanted: An Examination of the Cybersecurity Labor Market*. See https://www.rand.org/pubs/research_reports/RR430.html.

A study of U.S. cybersecurity jobs in 2015 revealed that approximately 84% of cybersecurity vacancies required either a bachelor's or master's degree; 83% required at least 3 years of experience (with an average of 5.4 years required); and 35% required a certification.[30] This reinforces a concern offered during the assessment about the apparent abundance of mid-level openings and suggests that creating more entry-level jobs would offer opportunities for acquiring and developing talent starting at that level. The data also suggest that employers should commit to hire their cybersecurity workforce based on skills rather than relying solely on either academic credentials or job experience.

One major gap in available data is the need to better understand the extent to which U.S. cybersecurity workforce needs can be addressed by "shared services providers" who are responsible for executing and handling specific information technology and cybersecurity tasks and can draw upon their own pool of experts; this would reduce the pressure on each organization to employ its own cybersecurity staff. Although use of shared services could be an obvious part of the cybersecurity workforce solution for any organization, there are only a few data sources readily available that report on these trends.

Determining Specialized Skills

In many instances, employers need workers with specialized competencies for specific sectors along with cybersecurity competencies. Combining these multiple requirements in a single position makes finding qualified candidates more difficult. At the same time, it points to an opportunity to meet cybersecurity-related workforce needs by providing cybersecurity-specific learning opportunities to those now in the workforce or those being educated or trained in entirely different fields.

The increasing emphasis that employers are placing on communication, teamwork, marketing, and other "soft" skills adds to the potential candidates for cybersecurity positions. The sufficiency assessment identified the need for more rigorous and reliable aptitude tests to identify those in today's workforce who can shift into cybersecurity roles. Current aptitude assessments are still evolving in quality, scope, and ready availability.

Maintaining a Competitive Advantage

Competition for qualified cybersecurity workers is intense across all sectors. This situation is as true for faculty positions as it is for the general cybersecurity workforce—a special challenge since the country relies heavily on its education system to develop future cybersecurity workers. This competition for talent is helping to drive increases in salaries and benefits, making cybersecurity positions

[30] Burning Glass Technologies (2015). *Job Market Intelligence: Cybersecurity Jobs*. See http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf.

overall more attractive.[31] However, this upward pressure also makes it more difficult for employers to afford and retain qualified workers.

Moreover, this workforce market competition can create tensions within organizations' human resource operations; there may be pressure to increase salaries, institute hiring and retention bonuses, or relax strict educational and experience requirements associated with cybersecurity positions. In many instances, human resource departments are also under pressure to decrease the time to hire for these positions, which can cause the assessment process to be shortchanged.

We need to grow the pool of qualified cybersecurity professionals; doing so will ease a too-competitive marketplace, in turn enabling employers to fill positions while slowing the pressure of salary increases and retention bonuses.

Diversity
In comparison to the national workforce, minorities and women are underrepresented among those working in cybersecurity. While this is true overall for the Science, Technology, Engineering, and Math (STEM) fields, it is especially evident in cybersecurity.[32] Lower participation rates can mean that organizations miss out on additional candidates who might have had the potential to succeed as well as the positive contributions of diverse teams. As one industry executive described the situation: "Mature cybersecurity teams require a mix of skills and diversity of thought—you must foster teamwork that's inclusive and integrates multidisciplinary and diverse perspectives."[33]

To increase the participation of minorities and women in cybersecurity, multiple initiatives have been launched by the federal government as well as by state, local, and private sector employers. These include several that appear to be especially successful. The need for more mentors and role models continually emerges in tech gender gap surveys.[34]

Compensation
Pay for cybersecurity positions tends to be above the average pay levels for other positions in many parts of the economy, including information technology positions

---

[31] Cybersecurity postings offer $6,459 increase in salary in comparison to their IT counterparts (Source: Burning Glass Technologies (2015). *Job Market Intelligence: Cybersecurity Jobs 2015* (2015).
[32] Chabrow, E. (2011) *Minorities Scarce in IT Security Field*. See http://www.bankinfosecurity.com /women-minorities-scarce-in-security-field-a-4143.
[33] Angela Messer, Booz Allen executive vice president. See https://www.iamcybersafe.org/news_women_cybersecurity/.
[34] Alan B. Watkins (2017). *Response to NIST Request for Information (RFI)*. See https://www.nist.gov /sites/default/files/documents/2017/08/02/nist_rfi_-_cybersecurity_workforce__response_by _abwatkins_2017-08-01.pdf.

in all sectors.[35] Still, in some areas—including the federal government—cybersecurity pay is below the level needed to attract the necessary talent.[36] In comparison with private sector employers, uniform and inflexible pay schedules that federal and state government agencies are required to use by law tend to inhibit their recruitment and retention of cybersecurity professionals.[37] Groups such as the Partnership for Public Service and others have called for more market- and performance-sensitive personnel systems for federal government agencies for many years.[38]

Another consideration complicating the situation is that smaller organizations to balance the kind of specific competencies that they seek with their desire for individuals who can carry out multiple cybersecurity work roles. Smaller organizations appear to be especially affected by the competitive marketplace for cybersecurity workers.[39]

C. Cybersecurity Workforce Education and Training

Generally, recent initiatives by government at all levels, the private sector, and academia have advanced the Nation's capabilities to better educate and train students and the workforce. There are multiple examples of successful education and training programs, including several capable of being scalable across the United States. Some efforts are already wide in scope and reaching large numbers of students at all levels.

We lack good data about the number of private sector institutions and programs providing cybersecurity-related education and training, the number of students taking advantage of and completing those programs, or their outcomes and impacts. There are few reliable data sources about the level of U.S. investment in cybersecurity education and training or how expenditures compare with other

---

[35] ibid, RAND Corporation, "Hackers Wanted." Also see The Center for Strategic and International Studies and Intel Security, *Hacking the Skills Shortage.* pp. 6-7. See https://www.csis.org/events/hacking-skills-shortage. Also see Burning Glass Technologies (2015). *Job Market Intelligence: Cybersecurity Jobs 2015* (2015).

[36] GAO, *Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority*, GAO-16-686 (Washington, D.C: Aug. 26, 2016).

[37] According to a 2015 NASCIO study, "Ninety-six (96) percent of state Chief Information Security Officers find 'state's salary rates and pay grade structures' as the factor that poses the biggest challenge to the state's ability to develop, support, and maintain a cybersecurity workforce." See https://www.nist.gov/sites/default/files/documents/2017/08/03/nascio_nist_rfi_cyber_workforce_august_2017.pdf).

[38] Partnership for Public Service, "Cyber In-Security II: Closing the Federal Talent Gap" report from April 2015 available for download at https://ourpublicservice.org/research/civil-service-reform.php.

[39] See https://biztechmagazine.com/article/2016/07/businesses-face-shortage-workers-cybersecurity-skills-survey-shows. Based on "Hacking the Skills Shortage." Also, remarks by Jason Volmut, President, CPURX, at workshop on cybersecurity workforce development on Wednesday, August 2, 2017.

countries.[40] Similarly, studies and data to document and assess whether the United States is spending enough are scarce.[41]

To gain a better understanding of the level of effort and to assist in future efforts to improve cybersecurity workforce education and training undertakings, the study team compiled a list of government and private sector cybersecurity programs at primary through secondary schools, career and technical education; two- and four-year colleges and universities as well as graduate offerings; apprenticeships; internships; cybersecurity camps and badges; cybersecurity challenges and other virtual education and training approaches; and retraining initiatives.

New and creative approaches are emerging regularly, including community-based, regional partnerships among academia, business, workforce development organizations, and economic development agencies to facilitate entry-level training and education of new cybersecurity workers.[42] These partnerships are providing access to a broader array of candidates into the workforce pipeline, as well as training and education for current cybersecurity workers. Cybersecurity competitions have been increasingly popular tools for attracting talented individuals to the field and have received added emphasis in federal law calling for federal agencies to support and promote these approaches.[43] They appear to hold promise for continuing professional development as well. A scan of the cybersecurity education and training landscape, which is a representative sample rather than a comprehensive list, will appear on the NICE website. This report recommends steps to address the lack of readily available, complete collections about cybersecurity education and training programs.

Measuring Effectiveness of Education and Training Programs
This study also revealed a lack of rigorous evaluative information about the effectiveness of cybersecurity education and training programs. That includes evaluating the success of programs aimed at training either those already in the workforce or those graduating from a two- or four-year post-secondary education in a nontechnical field but with analytical interests and capabilities. Virtual environments bring added value; measures to assess their relative effectiveness versus classroom education and training are also needed.

---

[40] Ibid. *Hacking the Skills Shortage, p.* 10, reports, "The US and UK rank highest in current investment in cybersecurity education…."
[41] Ibid. Based on responses from 200 U.S. decision makers who are involved in cybersecurity from organizations with at least 500 employees from within both public and private sectors, this study reports that more than 75 percent of U.S. respondents said, "My government is not investing enough in cybersecurity skills."
[42] For example, five regional pilots are in operation: Cin-Day Cyber in Ohio, HRCyber in the Tidewater Region of Virginia, Arizona Statewide Cyber Workforce Alliance in Phoenix, CyberPrep Program in Colorado Springs, and Partnership to Advance Cybersecurity Education and Training in Albany, New York.
[43] Cybersecurity Enhancement Act of 2014, Title III, §301, Cybersecurity Competitions and Challenges, 15 USC 7431, Public Law 113-274 (2014).

The measurement and evaluation of the job-related success of students who complete their education is sparse, even in high-profile and institutionalized programs. For example, the NSA/DHS National Centers of Academic Excellence in Cybersecurity (CAEs) provide little information about the number of students who graduate and find cybersecurity jobs; data are especially lacking about the quality of the students and their experiences when they move into the workplace.

Even though dozens—perhaps scores—of cybersecurity education programs are operating, study participants stated that there is a lack of efficient and effective sharing of the curriculum used in these efforts. Broad, flexible guidance and improved sharing about curricula—essentially, what is working—would support the development of cybersecurity programs at a range of institutions. Limited availability of data regarding program effectiveness makes better sharing about success rates and the quality of programs and students essential.

Supplying the Demand for Educators

A particularly important factor affecting the sufficiency of the cybersecurity workforce is the apparent shortage of knowledgeable and skilled teachers[44] at the primary and secondary levels, faculty in higher education, and training instructors. Although relevant data about the number of and reason for open positions are not readily available, supporting indicators include 1) heavy competition among colleges and universities; 2) strict requirements for faculty members to have terminal advanced degrees versus valuing work experience; and 3) the higher salaries available in nonteaching cybersecurity jobs.[45] This report makes several recommendations for increasing the supply of capable faculty.

Aligning Workforce Needs with Academic Requirements

Employers are expressing increasing concern about the relevance of certain cybersecurity-related education programs in meeting the real needs of their organization. For example, there is anecdotal evidence that employers have become overly reliant upon educational attainment as a proxy for KSAs rather than making employability judgments based upon competency-based assessments or evidence that prior work performance validates command of the relevant KSAs. That is consistent with findings in other countries. For certain work roles, a bachelor's degree in a cybersecurity field may or may not be the best indicator of an applicant's qualifications.[46] The study team found many concerns regarding the need to better

---

[44] "Lack of faculty in cybersecurity education programs who have real-world experience and can transfer applied knowledge to cybersecurity students" is cited as a special challenge. See: Georgetown University's response to the RFI at: https://www.nist.gov/sites/default/files/documents/2017/08/04/georgetown_university_school_of_continuing_studies.pdf

[45] For example, multiple speakers addressed this issue at the Workshop on Cybersecurity Workforce Development, Chicago, IL, August 2, 2017.

[46] One workshop participant reported that eight out of ten employers say that a 4-year degree does not adequately prepare people for cybersecurity jobs, yet eight out of ten job openings request that

align education requirements with employers' cybersecurity needs and how important it is for educational institutions to engage constantly with industry.[47] Recommendations to address this situation are included in this report. (See Imperative 3.)

Complicating the demands on the education enterprise are concerns that some cybersecurity programs offered by higher education institutions concentrate only on technical knowledge and skills. One university team responding to the RFI described the situation this way:

> "*…many of the cybersecurity educational programs offered by institutions of higher education focus solely on technical skills and knowledge. The need for such experience is real but often overshadow nontechnical skills required by employers*."

They point to the desirability of soft skills or employability skills, such as communications, team-building, analytical and strategic thinking, problem solving, risk management, and ethics.[48] This echoes similar concerns overseas. Concern also has been expressed that educators focus too much on theory and too little on practice.

At the same time, some educators reported that they found employers to be less than fully communicative about their needs in terms of numbers and types of positions they need to fill. That phenomenon apparently is not unique to the U.S.

Retraining

Expanding the pool of candidates for the cybersecurity workforce by retraining those currently employed in non-cybersecurity fields was identified as both a need and a large opportunity to fill vacant positions.[49] Retraining current workers, including those whose positions are more likely to be eliminated, carries obvious

---

level of education, suggesting a real disconnect.[46] Also see Burning Glass Report (2015). *Job Market Intelligence*. pp. 6. http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf.

[47] One recent survey indicated that nearly 65 percent of all entry-level cybersecurity applicants lacked the requisite skills to perform the tasks related to the jobs they were seeking. "State of Cybersecurity: Implications for 2016," p.12, An ISACA and RSA Conference Survey, 2016, http://www.isaca.org/cyber/Documents/state-ofcybersecurity_res_eng_0316.pdf.

[48] Georgetown University School of Continuing Studies (2017). pp.4-5. *Memorandum*. See https://www.nist.gov/sites/default/files/documents/2017/08/04/georgetown_university_school_of_continuing_studies.pdf.

[49] For example, multiple speakers addressed this issue at the Workshop on Cybersecurity Workforce Development, Chicago, IL, August 2, 2017. Also, see: Harvard Business Review, Marc van Zadelhoff, (May 4, 2017) https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

benefits for the organization, the individual, and the Nation. The scope assessment identified some examples of apparent retraining successes.[50]

Professionalization

Input provided for this assessment also suggests an interest in formalizing and institutionalizing cybersecurity as a profession—even as there is uncertainty about whether it is, in fact, a profession, a portfolio of work assigned to individuals or teams within an organization, or a discrete discipline of study.[51] There are concerns about whether professionalization would be constructive at this point. Comparisons with the medical and legal professions were offered, along with suggestions that more rigorous credentialing would help to firm up and improve the reliability of the cybersecurity workforce. Counter-suggestions were also put forward, reflecting concerns about locking in cybersecurity education and training requirements in what is an extraordinarily dynamic field. In response to those concerns, advocates for greater professionalization make the case that medical, legal, and other professions also are dynamic, and any standards established for the cybersecurity field can be changed over time to keep pace with technology.

Lack of Agreement on Industry Credentials

Several programs provide separate credentials or certifications related to individuals' qualifications in addition to those that provide more straightforward evidence that a particular course or training regimen was completed. These credentialing organizations offer assurances to employers about the specific capabilities of candidates or current employees. Nevertheless, there is some uncertainty among students, employees, and employers alike about how certifications relate to an individual's cybersecurity knowledge, skills, and abilities, in a specific position. That is especially true if credentials do not map well to a particular position—something that can occur quickly as technology and threats advance. Small- and medium-size businesses, in particular, may be struggling with understanding certifications and other credentialing. The study team was made aware of references to "credentialing confusion" and suggestions that a national rating system is needed. A listing of known certification programs is available from the Department of Homeland Security (DHS).[52]

Changes in Technology

---

[50] Cyber Innovation Center. (2017). *Cybersecurity Workforce Development: The Long Game: A Regional Model for the Nation*. pp. 9. Retrieved from https://www.nist.gov/sites/default/files/documents/2017/08/02/cyber_innovation_center.pdf Also see https://www.doleta.gov/TAACCCT/TAACCCT_One_Pagers_All.pdf; https://www.sans.org/cybertalent/immersion-academy; https://www.sans.org/ukcyberacademy/graduation; https://techhire.org/.

[51] Committee on Professionalizing the Nation's Cybersecurity Workforce: Criteria for Future Decision-Making; Computer Science and Telecommunications Board; Division on Engineering and Physical Sciences; National Research Council, 2013.

[52] Department of Homeland Security (2017). *Cybersecurity Certifications*. See https://niccs.us-cert.gov/featured-stories/cybersecurity-certifications.

Technology advances will inevitably change the jobs of those in the cybersecurity workforce as well as associated education and training programs. All cybersecurity practitioners and educators must stay current with the latest security-related advances, including new tools and vulnerabilities. Data analytics and artificial intelligence, for example, are fundamentally changing the portfolio of cybersecurity tools.[53] Although some reports predict that these advances could decrease the number of cybersecurity specialists needed,[54] it is generally deemed more likely that they will shift the nature of their work and education requirements or may actually grow, based on past experience.[55] Technology advances offer exciting possibilities for improving education tools and for extending the learning environment. This report includes a recommendation to develop and foster greater use of innovative technologies to improve cybersecurity education and training as well as assessment.

D. Hiring Practices

Beyond education and training, hiring considerations in both the private and public sectors affect the sufficiency of the U.S. cybersecurity workforce. Constraints in formal hiring systems in all parts of society contribute to a less efficient system.

For example, security clearances often are required for government and private sector cybersecurity positions based on a need to be eligible for access to classified national security and other sensitive information. Delays in gaining these clearances impede government and government contractor hiring. Some candidates may not be willing or able to wait for those clearances and will accept other job offers. The sensitive work environment may complicate efforts to bring in interns or apprentices, despite the valuable job training opportunities available in those organizations. Other prospective cybersecurity hires are very limited in what they can accomplish until clearances are finalized. Challenges in applying clearance reciprocity across government agencies are a barrier identified during the assessment, as is the potential for agencies to classify too much information or overstate the levels of classification that apply; in turn, that affects the level of the clearance required in positions needing access to that information.

Alignment of education and training requirements with hiring decisions is a major factor that affects the ability of those with cybersecurity backgrounds to find employment or perform well in the workplace, as noted above. A set of recommendations for better alignment is provided in this report.

---

[53] Accenture Federal Services, LLC (2017). *U.S. Department of Commerce Cybersecurity Workforce RFI*. See https://www.nist.gov/sites/default/files/documents/2017/08/03/accenture_response_cybersecurity_workforce_vf.pdf.

[54] ibid. *Hacking the Skills Shortage* (2016). pp. 6. See https://www.csis.org/events/hacking-skills-shortage.

[55] President's Commission on Enhancing National Cybersecurity (December 1, 2016) at: https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

Appendix 3:
Executive Order 13800
Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

Below is the section of the Executive Order relating to cybersecurity workforce development. Full text is available at:
https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to protect American innovation and values, it is hereby ordered as follows:
…..

Sec. 3. Cybersecurity for the Nation..
(a) Policy. To ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Further, the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace.
….

(d) Workforce Development. In order to ensure that the United States maintains a long-term cybersecurity advantage:

(i) The Secretary of Commerce and the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Secretary of Labor, the Secretary of Education, the Director of the Office of Personnel Management, and other agencies identified jointly by the Secretary of Commerce and the Secretary of Homeland Security, shall:

(A) jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and

(B) within 120 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors.

(ii) The Director of National Intelligence, in consultation with the heads of other agencies identified by the Director of National Intelligence, shall:

(A) review the workforce development efforts of potential foreign cyber peers in order to help identify foreign workforce development practices likely to affect long-term United States cybersecurity competitiveness; and

(B) within 60 days of the date of this order, provide a report to the President through the Assistant to the President for Homeland Security and Counterterrorism on the findings of the review carried out pursuant to subsection (d)(ii)(A) of this section.

(iii) The Secretary of Defense, in coordination with the Secretary of Commerce, the Secretary of Homeland Security, and the Director of National Intelligence, shall:

(A) assess the scope and sufficiency of United States efforts to ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities; and

(B) within 150 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations on the assessment carried out pursuant to subsection (d)(iii)(A) of this section.

(iv) The reports described in this subsection may be classified in full or in part, as appropriate.

….
DONALD J. TRUMP

THE WHITE HOUSE
May 11, 2017.

Appendix 4:
Consolidated List of Imperatives, Recommendations and Actions

Imperative 1	Launch a national Call to Action to draw attention to and mobilize public and private sector resources to address cybersecurity workforce needs.
Recommendation 1.1	The Administration should convene senior leaders in business, education, and government to jointly develop and launch a high-profile *Call to Action* to achieve the Nation's vision of a cybersecurity workforce that safeguards and promotes America's national security and economic prosperity.
Action 1.1.1	The Administration should actively engage senior Executive Branch and business and academic leaders in developing the *Call to Action*. An action plan should be developed to implement this recommendation as well as Recommendations 1.2 and 1.3.
Action 1.1.2	Senior federal officials should encourage the private sector to broaden and deepen its support for cybersecurity education, training, and workforce efforts, including expanding and committing to long-term support for these activities. Special attention should be given to owners and operators of critical infrastructure sectors.
Recommendation 1.2	Senior Administration officials should widely socialize the country's cybersecurity workforce challenges as a matter of national and economic security and commit their departments and agencies to creatively, aggressively, and visibly address this pressing need.
Action 1.2.1	With the urgency of a national mobilization, federal department and agency heads should elevate attention to U.S. cybersecurity workforce needs and strategies in their communications with internal and external audiences and implement all relevant recommendations in this report.
Recommendation 1.3	The Administration should include funding in the President's budget and work with Congress to provide long-term authorization and sufficient appropriations for cybersecurity education and workforce development programs in order to sustain and expand current efforts. Priorities should be given to those that address cybersecurity workforce development in effective and innovative ways and those that support federal workforce initiatives.
Action 1.3.1	The Administration should develop a legislative proposal to amend the Cybersecurity Enhancement Act of 2014 to codify the National Security Agency/Department of Homeland Security (NSA/DHS) National Centers of Academic Excellence (CAE) in Cybersecurity program. In addition, the Administration should include funding in the President's

	budget for annual authorization of appropriations for the NSA/DHS CAE program to systematically grow and sustain support of the institutions critical to growing the cybersecurity workforce of the future.
Action 1.3.2	The Office of Management and Budget (OMB) should utilize existing federal departments' and agencies' cyber spending data to evaluate the effectiveness of resources to this initiative and increase or decrease resources, as appropriate, to the most effective and efficient government programs.
Action 1.3.3	To reduce confusion and ensure alignment, federal departments and agencies should strive to standardize around the use of a single definition of "cybersecurity workforce" based on the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.
Recommendation 1.4	Federal departments and agencies must move quickly to address major needs relating to *recruiting, developing, and retaining* cybersecurity employees as they continue to implement the Federal Cybersecurity Workforce Strategy and the Federal Cybersecurity Workforce Assessment Act (FCWAA). These actions must be given close attention by senior agency leaders to ensure that timelines are met.
Action 1.4.1	Led by the Office of Personnel Management (OPM) with the support of the Chief Human Capital Officer (CHCO) Council and CIO Workforce Council, federal departments and agencies should be provided more clearly defined and readily available guidance and resources to identify and quickly recruit cybersecurity talent.
Action 1.4.2	OPM and federal departments and agencies should explore the use of direct hire or other authorities and salary incentives, to address recruiting difficulties and shortages of cybersecurity expertise. National Background Investigations Bureau, the Security Executive Agent (Office of the Director of National Intelligence), and Suitability Executive Agent (OPM), in partnership with federal departments and agencies, should speed up security clearances by bringing additional background investigators on board while continuing to automate background investigation processes, taking greater advantage of interim clearances, and examining and addressing challenges in applying reciprocal clearances across multiple agencies.
Recommendation 1.5	The federal government should launch a vigorous effort to recruit cybersecurity workers from large and diverse pools of candidates who are underutilized or underrepresented in the cybersecurity workforce. This includes veterans, women, and minorities.

Action 1.5.1	OPM should lead federal departments and agencies in a government-wide outreach strategy to educate and raise awareness among students, recent graduates, current federal employees, and veterans transitioning to the civilian workforce through educational institutions, military installations, and other organizations.
Action 1.5.2	Federal agencies should expand their use of recruitment tools including websites (such as www.cybercareers.gov), videos, and social media with additional functionality and enhanced branding to attract a richer and more diverse candidate pool and preview federal cybersecurity careers. They also should expand use of cybersecurity competitions, challenges, contests, and other interactive opportunities.
Imperative 2	**Transform, elevate, and sustain the learning environment to grow a dynamic and diverse cybersecurity workforce.**
Recommendation: 2.1	Emphasize retraining programs so that current employees can be reskilled to take on cybersecurity roles.
Action 2.1.1	Government at all levels and the private sector should consider assessing the cybersecurity-related aptitudes and abilities of employees who recently lost their jobs, will be laid off, or are planning to retire.
Action 2.1.2	The Interagency Council on Veterans Employment should develop and implement plans to provide career guidance and identify education and training services that encourage veterans with cybersecurity experience to transition to federal positions.
Action 2.1.3	Involve and incentivize NSA/DHS CAE-designated institutions or other local or regional educational or training providers to assist with employee education, training, and career awareness activities—including career fairs and career advising.
Recommendation: 2.2	Government, the private sector, and academia should build on and strengthen hands-on, experiential, and work-based learning approaches—including apprenticeships, research experiences, co-op programs and internships—as part of their strategies for meeting cybersecurity workforce needs.
Action 2.2.1	Agencies should utilize additional hiring authorities and programs such as the Pathways Program (which includes internships, opportunities for recent graduates, and the President's Management Fellowship program) and apprenticeships to grow cybersecurity talent and offer opportunities to students and recent graduates to rapidly integrate participants into the federal workforce in a way similar to the recent authorization that Department of Defense (DoD) laboratories received for STEM employees.

Action 2.2.2	The Department of Labor (DOL) should build cybersecurity apprenticeships into applicable Employment & Training Administration-funded programs, and provide other agencies with advice and technical assistance for their apprenticeship programs.
Action 2.2.3	Colleges and universities—especially community colleges—should partner with their local, regional, and national business community to support apprenticeship programs; this includes expanding on the few college-level cybersecurity apprenticeship programs.
Recommendation 2.3	Private and public sector organizations should sponsor the use of virtual training and assessment environments to augment the limited cadre of teachers and assessment tools that match workforce needs.
Action 2.3.1	All federal agencies involved in cybersecurity education and training should develop and deploy more training and talent assessment environments and programs—including challenges.
Action 2.3.2	Agencies should make greater use of cybersecurity competitions, including in professional development of those in the cybersecurity workforce.
Recommendation 2.4	Expand the availability and expertise of teachers and faculty through a combination of incentives and policy changes.
Action 2.4.1	The Administration should encourage employers and academic institutions to initiate or support programs attracting and allowing experienced cybersecurity workers to supplement existing curricula and improve effectiveness in delivering cybersecurity-related knowledge in primary through higher education, including regular classroom situations as well as mentoring and other environments.
Action 2.4.2	Educational institutions and businesses should encourage qualified cybersecurity practitioners to serve as teachers, professors of practice, guest presenters, or adjunct faculty.
Action 2.4.3	Increase the capacity of the teaching workforce through intensive professional development for current teachers regardless of their formal background and current teaching focus. More schools should consider opportunities for team teaching with industry professionals and incentives for teacher preparation programs to incorporate cybersecurity into the curriculum of future educators.
Action 2.4.4	The U.S. Department of Education (ED) should develop a national recognition program that identifies and acknowledges school districts, colleges and universities, employers, and individuals that are role models in enhancing the development of future cybersecurity workers.

Action 2.4.5	Use federal cybersecurity education and training programs as a vehicle to recognize teachers and faculty who provide instruction in cybersecurity education, including "train the trainer" experiences.
Recommendation 2.5	Strengthen the capacity for high schools to prepare students with the range of knowledge, skills, and abilities to enter into cybersecurity career and educational pathways by supporting the development of rigorous Career Technical Education (CTE) programs and education of the teaching workforce.
Action 2.5.1	Support the development of an elite comprehensive career technical education program of study in cybersecurity through the existing Carl D. Perkins Career and Technical Education Act. The program should align with the NICE Framework; deliver rigorous academic, technical, and employability skills; and give credits that transfer directly to NSA/DHS CAE-designated institutions.
Action 2.5.2	Increase the capacity of the CTE teacher workforce to incorporate cybersecurity instruction through intensive professional development and incentives for current teachers.
Recommendation 2.6	Federal and state governments, as well as the private sector, should consider providing greater financial assistance and other incentives to reduce student debt or subsidize the cost of cybersecurity education or training.
Action 2.6.1	The Administration should include in the President's proposed budget increased federal funding for the CyberCorps®: Scholarship for Service (SFS) program administered by NSF to dramatically increase the number of students studying cybersecurity and entering the federal cybersecurity workforce.
Action 2.6.2	Modify student loan repayment programs to provide a direct financial incentive for individuals to take cybersecurity jobs in federal, state, local, or tribal governments or economically distressed regions. Cybersecurity-related faculty positions with public or private colleges or universities providing two-year, four-year, and graduate degrees in NICE Framework-recognized specialty areas also should be eligible for repayment.
Action 2.6.3	Provide additional federal or state tax incentives for cybersecurity-related education and training.
Recommendation 2.7	Expand government and private sector support for high-quality cybersecurity camps, boot camps, and similar programs designed to educate and train teachers or students.

Action 2.7.1	Develop a mechanism for providing need-based scholarships to students and teachers to participate in high-quality camps or professional development programs.
Action 2.7.2	The Administration should propose in the President's budget increased and sustained funding for the GenCyber program through the NSA and National Science Foundation (NSF)—to allow it to grow to 300 camps, covering all 50 states, by 2020.
Imperative 3	**Align education and training with the cybersecurity workforce needs of employers and prepare individuals for lifelong careers.**
Recommendation 3.1	The Executive Branch should strongly encourage educators, training providers, and employers to use the taxonomy and lexicon of the NICE Framework as the reference for building workforce development strategies.
Action 3.1.1	To help codify cybersecurity roles throughout the U.S. workforce, NICE should more widely promote its Framework, which defines cybersecurity work roles, and collect and share information about how it is being used. That Framework should be updated regularly with even broader input; it must be dynamic and expanded to cover additional work roles.
Action 3.1.2	NICE should educate and encourage employers to align cybersecurity tasks with corresponding Knowledge, Skills, and Abilities (KSAs) rather than use generalized job descriptions that incorporate outdated degree, certification, and experience requirements. OPM should also update qualification standards to incorporate position requirements such as degree levels, certifications, and experience.
Action 3.1.3	Just as federal government departments and agencies are required to use the NICE Framework to identify and define work roles and tasks, federal contractors should be required to use the same lexicon for these purposes.
Action 3.1.4	The Council of Governors, National Governors Association, and the National Association of State Chief Information Officers should encourage use of the taxonomy and lexicon of the NICE Framework by state, local, and tribal governments.
Recommendation 3.2	Develop model career pathways for cybersecurity-related positions that can be used in the private and public sectors. These pathways should spell out education, training, and other experiences that align with employers' skill needs and prepare an individual to be successful in entering or advancing in a cybersecurity career.

Action 3.2.1	The Interagency Working Group on Career Pathways, led by DOL, should partner with NICE, ED, DOC, OPM, and other public and private sector organizations to develop and raise awareness about model career pathways for cybersecurity-related positions.
Action 3.2.2	DHS, in consultation with other federal government civilian agencies and the private sector, should lead the development of capability indicators required for entry-level, mid-level, and advanced-level work roles in the NICE Framework.
Recommendation 3.3	The federal government should partner with the private sector and academia to develop interdisciplinary cybersecurity curriculum guidance that addresses the need for widely accepted and shareable cybersecurity curricula that incorporate employers' cybersecurity needs.
Action 3.3.1	NICE, the National Science Foundation (NSF), the CAE program, and the NSA College of Cyber should continue to engage employers, academia, and professional societies to coordinate and establish cybersecurity curriculum guidance.
Action 3.3.2	The Administration should propose sustained funding for the curriculum development initiative operated by the NSA College of Cyber based on one-time FY 2017 funding.
Action 3.3.3	State and local governments and the private sector should integrate cybersecurity into existing STEM programs, especially computer science courses, and develop cybersecurity topics and examples for use in the broader primary school curricula; they should take advantage of the large number of programs already under way and the curricula already developed.
Recommendation 3.4	Establish cooperative agreements between NICE and at least one regional alliance or partnership for cybersecurity education and workforce in each state. These collaborative efforts should facilitate local and regional partnerships of employers, educational institutions, local governments, and community organizations to better meet the needs of local and regional industry and the workforce.
Action 3.4.1	Develop sustainable mechanisms within communities to identify employer cybersecurity workforce needs based on the NICE Framework.
Recommendation 3.5	The federal government should establish a clearinghouse of information on cybersecurity workforce development education, training, and development programs and initiatives.

Action 3.5.1	The Department of Commerce (DOC) should run the clearinghouse, administered by NICE in cooperation with NICE partner departments and agencies.
Recommendation 3.6	The federal government should lead efforts to improve the country's understanding of employers' specific cybersecurity workforce needs.
Action 3.6.1	NICE should work with its grantees to expand the CyberSeek tool's capabilities by identifying where the greatest job demands are by sector or critical infrastructure and by identifying the level of the positions (i.e., entry/mid-level/advanced).
Action 3.6.2	Action 3.6.2 DHS should prepare a plan in conjunction with DOC, DOL, the Department of Labor, and the Office of the Director of National intelligence (ODNI) to regularly gather comparative information needed to better track and understand the Nation's dynamic cybersecurity workforce needs.
Imperative 4:	*Establish and leverage measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.*
Recommendation 4.1	All programs related to cybersecurity workforce education or training should have an associated set of robust metrics and evaluation mechanisms to track and determine success in terms of the quantity and quality of individuals educated, trained, and ready to fulfill cybersecurity tasks in the workplace.
Action 4.1.1	NICE should establish a clearinghouse that *identifies effectiveness metrics already used* by one or more organizations and that are deemed helpful by federal agencies.
Action 4.1.2	NICE should lead an effort to *develop a portfolio of reliable metrics* for measuring and evaluating cybersecurity workforce programs, including common performance measures included in the Workforce Innovation and Opportunity Act (WIOA).
Action 4.1.3	All organizations receiving federal funding to provide cybersecurity workforce education and training services should use a set of robust metrics and evaluation mechanisms to track and determine success in terms of the quantity and quality of individuals educated and trained.
Recommendation 4.2	Federal agencies should work with educational institutions to identify and use currently available tools to assess aptitude and skills related to cybersecurity positions in the workforce. Priority improvements needed in assessment tools should be identified and addressed.

Action 4.2.1	The Executive Branch should coordinate federal plans to develop centrally available reliable tools to assess 1) aptitude for a cybersecurity career and 2) the technical readiness to demonstrate the possession of KSAs and the ability to perform specific tasks identified in the NICE Framework.

Appendix 5:
Request for Information

The National Institute of Standards and Technology (NIST) issued a Request for Information (RFI) in the *Federal Register* on July 12, 2017 to gather information to inform the federal assessment on the scope and sufficiency of efforts to educate and train the Nation's cybersecurity workforce and to develop recommendations for ways to support and improve that workforce in both the public and private sectors. Comments were due by August 2, 2017. All comments received were posted to the NICE website without change or redaction.

Sources of the 97 responses received were:

- 47% from academia;
- 30% from industry;
- 7% from government; and
- 5% from other organizations or individuals without a stated affiliation.[56]

Organizations ranged from private and public educational institutions, large and small companies, government at all levels, nonprofits, and regional collaboratives.

The RFI included eight questions related to the cybersecurity workforce. Respondents also were encouraged to share information and views on related issues. Many submitted or referenced additional materials containing information about cybersecurity-related workforce, education, and training issues.

The assessment team reviewed and analyzed each of the RFI responses for content. More than 575 unique comments were submitted by the 97 respondents; all were reviewed and considered for the assessment and report.

[56] Percentages do not add due to rounding.

Appendix 6:
Webinar and Workshop

Webinar:
The NICE Program Office hosted a webinar on June 5, 2017, to provide an overview of the cybersecurity workforce provisions of the Executive Order, present a summary of existing federal government legislation and programs for additional context, and describe plans to engage the community to collect input and receive feedback.

Over 300 individuals took part in the webinar. A recording of the webinar has been viewed more than 880 times since it took place. The presentation slides and recording are available at https://www.nist.gov/itl/applied-cybersecurity/nice/webinar.

Workshop:
The National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) held a workshop on cybersecurity workforce development on August 2, 2017, to assist in carrying out the study called for by Executive Order 13800.

More than 120 attendees took part in the workshop, which was hosted by the Illinois Institute of Technology in Chicago, IL. Separate panels focused on:

- Assessing Workforce Needs and Planning for the Future
- Growing the Cybersecurity Workforce Through Education and Training
- Recruiting and Hiring a Knowledgeable and Skilled Workforce
- Developing and Retaining a Globally-Competitive Workforce

Speakers included representatives of education and training institutions (ranging from K-12 schools and community colleges to universities), industry, federal agencies and local governments, and students.

Comments by panelists, including in response to participants' questions, informed the study and the report to the President. These comments supplemented responses to a Request for Information, and allowed the study team to probe more deeply into the key issues identified during the assessment.

An audio recording of the workshop is available at https://www.nist.gov/news-events/events/2017/08/workshop-cybersecurity-workforce-development.

Appendix 7:
National Initiative for Cybersecurity Education (NICE)
Strategic Plan

Vision: A digital economy enabled by a knowledgeable and skilled cybersecurity workforce.

Mission:
To energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development.

Values*:*

Seek Evidence – inform actions or decisions with data and pursue objective and reliable sources of information

Pursue Action – create concrete steps towards deliverable outcomes to achieve mission and goals

Challenge Assumptions – examine rationale for past and present education, training, and workforce approaches and apply critical analysis to future solutions

Drive Change – seek creative and innovative solutions that might disrupt or defy the status quo

Stimulate Innovation – inspire and experiment with new approaches to education, training, and skills development

Foster Communication – raise awareness of cybersecurity education and workforce issues and encourage openness to build trust

Facilitate Collaboration – combine the knowledge and skills of multiple stakeholders with multiple viewpoints to achieve the best outcomes

Share Resources – leverage, support, and raise awareness of community-developed approaches and solutions

Model Inclusion – encourage participation from stakeholders with diverse backgrounds and viewpoints

Measure Results – assess the effectiveness of results through both quantitative metrics and qualitative measures

Goal #1 Accelerate Learning and Skills Development
Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers

Objectives:

1.1 Stimulate the development of approaches and techniques that can more rapidly increase the supply of qualified cybersecurity workers
1.2 Advance programs that reduce the time and cost for obtaining knowledge, skills, and abilities for in-demand work roles
1.3 Engage displaced workers or underemployed individuals who are available and motivated to assume cybersecurity work roles
1.4 Experiment with the use of apprenticeships and cooperative education programs to provide an immediate workforce that can earn a salary while they learn the necessary skills
1.5 Explore methods to identify gaps in cybersecurity skills and raise awareness of training that addresses identified workforce needs

Goal #2 Nurture a Diverse Learning Community
Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce

Objectives:

2.1 Improve education programs, co-curricular experiences, and training and certifications
2.2 Encourage tools and techniques that effectively measure and validate individual aptitude, knowledge, skills, and abilities
2.3 Inspire cybersecurity career awareness with students in elementary school, stimulate cybersecurity career exploration in middle school, and enable cybersecurity career preparedness in high school
2.4 Grow creative and effective efforts to increase the number of women, minorities, veterans, persons with disabilities, and other underrepresented populations in the cybersecurity workforce
2.5 Facilitate the development and dissemination of academic pathways for cybersecurity careers

Goal #3 Guide Career Development and Workforce Planning
Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent

Objectives:

3.1 Identify and analyze data sources that support projecting present and future demand and supply of qualified cybersecurity workers
3.2 Publish and raise awareness of the National Cybersecurity Workforce Framework and encourage adoption
3.3 Facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs
3.4 Promote tools that assist human resource professionals and hiring managers with recruitment, hiring, development, and retention of cybersecurity professionals
3.5 Collaborate internationally to share best practices in cybersecurity career development and workforce planning

Appendix 8:
Abbreviations and Acronyms

CAE	Centers of Academic Excellence
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CTE	Career and Technical Education
DHS	Department of Homeland Security
DOC	Department of Commerce
DoD	Department of Defense
ED	Department of Education
DOL	Department of Labor
ETA	Department of Labor's Employment & Training Administration
FCWAA	Federal Cybersecurity Workforce Assessment Act of 2015
HR	Human Resources
ICC	Interagency Coordinating Council
ISACA	Information Systems Audit and Control Association (now, ISACA)
$(ISC)^2$	International Information System and Security Certification Consortium
KSAs	Knowledge, Skills, and Abilities
NICE	National Initiative for Cybersecurity Education
NICEWG	NICE Working Group
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSF	National Science Foundation
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPM	Office of Personnel Management
RAMPs	Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development
SFS	Scholarship for Service
STEM	Science, Technology, Engineering, and Mathematics