NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Testimony of

Rodney Petersen
Director of NICE and Interim Chief of the Applied Cybersecurity Division
National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House Committee on Homeland Security

On

"Finding 500,000: Addressing America's Cybersecurity Workforce Gap"

June 26, 2024

Chairman Green, Ranking Member Thompson, and Members of the Committee, I am Rodney Petersen, Director of the National Initiative for Cybersecurity Education (NICE) Program Office at the National Institute of Standards and Technology (NIST) in the Department of Commerce. I am pleased to testify before you today on behalf of the NICE program and to illuminate our vision to *prepare, grow, and sustain a cybersecurity workforce that safeguards and promotes American's national security and economic prosperity*.

I want to briefly share three stories:

Devonie Nelson is a Junior Cybersecurity Engineer who started her journey into the cybersecurity field while a single Mom with significant personal and financial challenges. After graduating with a biology degree, she experienced a series of personal and career challenges as a young adult. She eventually enrolled in a Security Management master's degree program with a concentration in cybersecurity. Along the way, she discovered a philanthropic organization that enabled her to persist in her educational journey and eventually acquire a cybersecurity position at a healthcare company. Now, she has dedicated herself to sharing with others her experiences and the opportunities available to eliminate some of the initial hurdles faced when entering the cybersecurity field, especially as a minority first-generation student.

Jimmy Minhinnett was a truck driver who is now an Information Security Associate with a company in the financial services sector. Although he understood the impact of technology at a young age thanks to his father who worked in IT, life circumstances took him in a different direction. He left high school before completing his diploma and for the next 10 years worked hard, physically demanding shifts as a commercial truck driver. As a result of the impact of the pandemic on the trucking industry – combined with grieving the death of his father – he decided to pursue a new career and that led to the discovery of a cybersecurity certificate program that he completed on weekends while continuing to work. After acquiring that credential, he received a good job that changed his life.

Shane Wallace is the product of a military family, and he enlisted in the Army as a combat medic in 2014. Through his military service, he demonstrated a relentless commitment to excellence, concurrently pursuing a degree in Healthcare Administration. His assignments spanned the globe, where he held various leadership roles, overseeing complex logistics operations and spearheading crucial medical initiatives. As he transitioned from military service in 2023, his passion for technology led him to pursue and graduate from a training program for transitioning veterans where he developed a competency in cloud computing that led to an eventual role as a Junior Engineer with a private sector employer.

These are just three examples of individuals who have pursued a cybersecurity career through alternative pathways – and their stories help to address the focus of this hearing on how to find workers to address America's cybersecurity workforce gap. They shared their

stories earlier this month at the annual NICE Conference & Expo,[1] which was held in Dallas. However, their stories represent a growing number of Americans who are getting into good-paying, meaningful careers in cybersecurity through the many different education or training pathways available to them.

NICE's mission is to *energize, promote, and coordinate a robust community working together to create an integrated ecosystem of cybersecurity education, training, and workforce development*. This mission aligns with the Administration's broader efforts in modernizing Federal hiring and strengthening the Federal workforce. As part of this NIST is also supporting broader workforce efforts including but not limited to the President's Management Agenda, the National Cyber Workforce and Education Strategy implementation, the National Security Memoradum-3 "Memorandum on Revitalizing America's Foreign Policy and National Security Workforce, Institutions, and Partnerships" and the AI Executive Order. The NICE Program Office also actively promotes and supports the Department of Commerce Principles on Highly Effective Workforce Investments[2] and the Department of Commerce and Department of Labor's Good Jobs Principles[3]. Today's testimony will focus on signature programs led by NIST beginning with the NICE Workforce Framework for Cybersecurity (or NICE Framework).

Federal Coordination and Coherence

As part of the administration-wide effort to connect Americans to Good Jobs in cyber, NICE coordinates with the White House of Office of National Cyber Director (ONCD), Office of Management and Budget, and through the National Cyber Workforce Coordination Group to integrate and align its work with the President's Management Agenda, National Cyber Workforce and Education Strategy (NCWES) implementation, Registered Apprenticeship EO, and Workforce Hub Efforts. For example, NICE is co-chair of the Working Group on Cyber Skills and Awareness as well as the Working Group on Cyber Workforce and Education.

NICE Workforce Framework for Cybersecurity (NICE Framework)

The NICE Framework[4] provides a common taxonomy or lexicon for describing cybersecurity work. It is used by employers to assess their workforce needs and to shape workforce development, including writing job descriptions that are more consistent and effective across organizations and sectors. The NICE Framework is also used by education and training providers to develop content and provide learning experiences to ensure that students or learners can develop skills and acquire credentials that attest to their capabilities. It is also used by learners, including students, job-seekers, and employees, to identify the skills and credentials necessary to enter and advance in high quality jobs in the cybersecurity career. The NICE Program Office released version 1.0.0 of the NICE

---

[1] https://niceconference.org/

[2] https://www.commerce.gov/issues/workforce-development

[3] https://www.dol.gov/general/good-jobs/principles

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Framework components in March, which represents a comprehensive update to the core content of the NICE Framework (NIST Special Publication 800-181r1). The recently updated NICE Framework includes 52 Work Roles across seven categories, 11 new Competency Areas, and over 2,220 Task, Knowledge, and Skill Statements.

CyberSeek: Interactive Cybersecurity Jobs Heatmap and Career Pathway Tool
Another signature program of NICE is our partnership with CompTIA and Lightcast, which has resulted in the production of CyberSeek. The CyberSeek.org[5] website is a tool that can help learners discover cybersecurity careers and policymakers, such as yourself, discover the dynamics of workforce supply and demand across the United States as well as in states or major metropolitan areas. Lightcast also developed the Quarterly Cybersecurity Talent Report as a commitment to support the NCWES from ONCD. It leverages and expands upon data Lightcast provides to CyberSeek.org. The updates to CyberSeek and the Cybersecurity Talent Report earlier this month revealed that, for the past 12 months in the U.S., there were 469,930 cybersecurity job postings, 1,239,018 existing cybersecurity workers, and 85 skilled cybersecurity workers for every 100 demanded by employers. While these numbers suggest modest improvements and indicate that we are making headway, there is still a talent gap of 225,000 cybersecurity workers needed to meet employer demand. In the DC metropolitan area alone, there are 66,775 cybersecurity jobs available and 36,908 across the entire state of Texas.[6]

NICE Strategic Plan (2021-2025)
The NICE Strategic Plan[7] and corresponding implementation plan is another signature program of NICE and establishes our vision, mission, and values. It also sets forth five goals with corresponding objectives.

Promote the Discovery of Cybersecurity Careers and Multiple Pathways
The first goal is to *Promote the Discovery of Cybersecurity Careers and Multiple Pathways*. As you heard earlier, the learning pathways to a career in cybersecurity can vary from learning experiences in high school or college leading to an academic degree to training programs or bootcamps that result in an industry-recognized certification to a Registered Apprenticeship or other earn and learn experience that culminates in a certificate of completion. However, providing multiple learning pathways is not enough if learners do not understand the variety of types of careers that are available in cybersecurity. That is why during the third week of October each year, as part of Cybersecurity Awareness Month, we hold a Cybersecurity Career Week,[8] that is a campaign to promote the discovery of cybersecurity careers and share resources that increase understanding and engagement in the multiple learning pathways and credentials that lead to careers in cybersecurity. The week is typically kicked-off with a Capitol Hill event hosted by the House Cybersecurity

[5] https://www.cyberseek.org/
[6] https://www.cyberseek.org/heatmap.html
[7] https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan
[8] https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-week

Caucus and Senate Cybersecurity Caucus and other events throughout the week including the US Cyber Team Draft Day[9], webinars, social media campaigns, and workplace events to showcase careers in cybersecurity.

Transform Learning to Build and Sustain a Skilled and Diverse Workforce

The second goal is to *Transform Learning to Build and Sustain a Skilled and Diverse Workforce*. There are many opportunities for innovation in the learning process that will increase the likelihood that job-seekers are job-ready to enter employment. Examples include more hands-on learning experiences and the use of performance-based assessments that measure competencies and capabilities to perform NICE Framework tasks. In an era when "skills-based approaches" is the mantra of employers and educators, we need to improve the quality and transparency of available credentials that serve to demonstrate and validate the competencies of a learner. We also need to advocate multidisciplinary approaches that integrate cybersecurity across disciplines, recognizing that a basic level of cybersecurity knowledge and skills are increasingly necessary in almost every career field and in every sector of the economy. The Cybersecurity Across Disciplines Conference[10] is an example of an event that brings together community and technical college faculty from diverse disciplines to explore the intersection of cybersecurity within their specific educational program areas and the critical infrastructure sectors they serve, including but not limited to manufacturing, healthcare, retail, engineering, and finance. And, building on the NICE value to Model Inclusion, this strategic plan goal emphasizes advocating and enabling engagement of stakeholders from diverse backgrounds and experiences.

Modernize the Talent Management Process to Address Cybersecurity Skills Gaps

The third goal is to Modernize the Talent Management Process to Address Cybersecurity Skills Gaps. It fundamentally seeks to enhance the capabilities of organizations and sectors to more effectively recruit, hire, develop, and retain the talent needed to manage cybersecurity-related risks. Building on other foundational NIST publications, such as the Risk Management Framework and Cybersecurity Framework[11], this goal helps organizations to focus on the "people" and workplace skills needed in their organizations who work alongside "technologies" or "processes" to manage cybersecurity risks. A few examples of reforms that are needed include: establishing more entry-level positions and opportunities that provide avenues for growth and advancement; aligning qualification requirements according to proficiency levels to reflect the competencies and capabilities needed to perform tasks in the NICE Framework; encouraging ongoing development and training of employees, including rotational and exchange programs, to foster and retain talent with diverse skills and experiences; and reskilling the unemployed, underemployed, incumbent workforce, and transitioning veterans or military spouses to prepare them for good jobs in cybersecurity.

---

[9] https://www.uscybergames.com/draft-day

[10] https://www.ncyte.net/about-ncyte/events/cyad-summit-cybersecurity-across-disciplines

[11] https://www.nist.gov/cyberframework

Expand Use of the NICE Workforce Framework for Cybersecurity (NICE Framework)
The fourth goal seeks to *Expand Use of the NICE Workforce Framework for Cybersecurity or NICE Framework*. This goal starts with increasing awareness of the benefits of the NICE Framework to employers, educators, and training providers. This goal goes on to ensure that the NICE Framework is aligned to other NIST resources, including the NIST Cybersecurity Framework, the NIST Privacy Framework[12], and other cybersecurity, privacy, and risk management publications or guidance. We are also keenly aware that tasks in the NICE Framework will be increasingly performed by automated techniques and will need to update knowledge and skill statements to incorporate appropriate and ethical use of artificial intelligence in the completion of cybersecurity tasks. Our international partners, especially developing nations, are increasingly looking to NIST resources, including the NICE Framework, as a model for their national efforts. That is why NICE recently partnered with the State Department to bring individuals representing over 20 countries to the NICE Conference & Expo earlier this month to learn more about their cybersecurity workforce development efforts and share how the NICE Framework is being widely used across the United States.

Drive Research on Effective Practices for Cybersecurity Workforce Development
The final goal in the NICE Strategic Plan seeks to Drive Research on Effective Practices for Cybersecurity Workforce Development. That is why each month, during our NICE Community Coordinating Council Meeting, we feature recent reports or research results that spotlight the most effective and proven practices. Similarly, we use research results to inform programs and curriculum design, foster continuous learning opportunities, impact learner success, and ensure equitable access. Again, supporting the NICE values to Challenge Assumptions, Stimulate Innovation, Act Based on Evidence, and Evaluate and Improve, we are working together as a community to pursue objective and reliable sources of information and using data to inform actions or decisions.

Foster Communication, Facilitate Collaboration, and Share and Leverage Resources
Let me conclude by just highlighting a few other ways in which NICE fulfills its mission – through its convening power and the development and dissemination of resources. On a monthly basis, NICE, convenes an interagency coordinating council of representatives from across federal government departments and agencies and the executive office of the president to coordinate and collaborate on national cybersecurity education and workforce development initiatives. We also convene a NICE Community Coordinating Council that is co-chaired by a leader from academia and industry. The Council includes working groups that correspond to each of the NICE Framework goals and communities of interest on topics such as cybersecurity apprenticeships, competitions, diversity and inclusion, K12 cybersecurity education, and more.

[12] https://www.nist.gov/privacy-framework

To promote and energize a robust community working together, NICE hosts several key events[13] each year, including the Annual NICE Conference and Expo, the Regional Initiative for Cybersecurity Education and Training Conference for the Americas, a NICE K12 Cybersecurity Education Conference, Cybersecurity Career Week, and a monthly NICE Webinar Series. These events bring together stakeholders to increase awareness and understanding, showcase effective practices and solutions, and expand our horizons by focusing on emerging and future trends. We also produce and share several resources[14], most of them developed with input from the broader community, including the NICE Framework Resource Center, the NICE Cybersecurity Apprenticeship Finder, one-pagers on topics such as Cybersecurity Workforce Demand, and a listing of Free and Low Cost Online Cybersecurity Learning Content.

Summary

In conclusion, the recent NICE Conference & Expo held in Dallas was our 15th annual conference and served to celebrate the establishment of NICE in 2008 by the Comprehensive National Cybersecurity Initiative. Over the past 15 years, we've seen considerable growth and progress towards fulfilling our mission to create an integrated system of cybersecurity education, training, and workforce development. However, the present and future promises to introduce new challenges and opportunities, and we must remain vigilant to continuously prepare, grow, and sustain the cybersecurity workforce that the public and private sector will need to safeguard our national security and promote America's economic prosperity.

Thank you for the opportunity to testify today on NIST's Cybersecurity Workforce activities, and I look forward to answering any questions.

[13] https://www.nist.gov/itl/applied-cybersecurity/nice/events

[14] https://www.nist.gov/itl/applied-cybersecurity/nice/resources