Testimony of

Rodney Petersen

Director, National Initiative for Cybersecurity Education (NICE)
National Institute of Standards and Technology
U.S. Department of Commerce

Before the

Subcommittee on Research and Technology of the
Committee on Science, Space, and Technology
United States House of Representatives

More Hires, Fewer Hacks: Developing the U.S. Cybersecurity Workforce

February 11, 2020

Introduction
Chairwoman Stevens, Ranking Member Baird, and Members of the Subcommittee, I am Rodney Petersen, Director of the National Initiative for Cybersecurity Education (NICE) program at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss NIST's National Initiative for Cybersecurity Education (NICE) program, the role NICE plays in interagency coordination for cybersecurity workforce pipeline issues and the challenges the federal government faces in recruiting and retaining skilled cybersecurity professionals.

NICE
Home to five Nobel Prizes, with programs focused on national priorities such as advanced communications, artificial intelligence, quantum science, advanced manufacturing and biosciences, NIST's mission promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In support of this mission, the National Initiative for Cybersecurity Education (NICE), is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development aimed at energizing and promoting a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with its partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity workers helping to keep our Nation secure.

2019 marked a year of milestones for the cybersecurity education and workforce development movement in the United States. In November, the 10th annual NICE Conference and Expo was held in Phoenix, Arizona. In December, NICE held the 5th annual NICE K-12 Cybersecurity Education Conference in Anaheim, California. Throughout 2019, NICE recognized the accomplishments resulting from 20 years of the National Centers of Academic Excellence in Cybersecurity. These milestones during 2019 allowed the NICE program to celebrate the work that has been accomplished to date and look forward to the future – the next 5 years, decade, or 20 years – to aspire to even greater improvements and innovations. While many consider the cybersecurity workforce gap a challenge, the NIST partnership looks at it as an opportunity and the NICE community is laser focused on addressing education and workforce problems with innovative solutions.

Consultative Process
The NICE Interagency Coordinating Council (ICC) convenes federal government partners of NICE for consultation, communication, and coordination of policy initiatives and strategic directions related to cybersecurity education, training, and workforce development. The meetings provide an opportunity for the NIST-led NICE Program Office, to communicate program updates with key partners in the federal government and to learn about other federal government

activities in support of NICE. The group also identifies and discusses policy issues and provides input into the strategic directions for NICE.

The NICE Working Group has been established to provide a mechanism in which ***public*** and ***private*** sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development. The working group is further divided into six sub-working groups focused on:

- K12 Education
- Collegiate Education
- Training and Certifications
- Competitions
- Apprenticeships
- Workforce Management

NICE Strategic Plan

The Cybersecurity Enhancement Act of 2014 authorized NICE and requires a strategic plan to be updated and submitted to Congress every five years. During 2020, NICE is embarking upon a consultative process that will result in a new 5-year strategic plan that is informed by the community that we serve.

The 2016 NICE Strategic Plan includes the following goals:

- 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*
- Nurture a Diverse Learning Community - *Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce*
- Guide Career Development and Workforce Planning - *Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent*

Each of these goals are supported by objectives, tactics, and measures of success.

As an example, one of the objectives in the NICE Strategic Plan is to "facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs" which is why NIST issued a Federal Funding Opportunity to pilot six Regional Alliance and Multi-stakeholder Processes Stimulating (RAMPS) Cybersecurity Education and Workforce Development. NIST received over 60 applications from almost 40 different states. The selected RAMPS communities were employer-led, learner-centered, community-oriented, standards-based, and outcomes-driven. The pilots were held in local economic communities in five different states. A *Roadmap for Successful RAMPS Regional Alliances and Multi-stakeholder Partnerships to Build the Cybersecurity Workforce* has been published as a NIST Informational Resource that identifies the challenges and successes of the RAMPS pilot.

As another example of an objective in the strategic plan, NICE sought to "identify and analyze data sources that support projecting present and future demand and supply of qualified cybersecurity workers." The "forecasting of future cybersecurity workforce needs" was specifically directed in the Cybersecurity Enhancement Act which is why NICE awarded a grant to CompTIA and Burning Glass to develop the website known as CyberSeek - www.CyberSeek.org - that includes both an interactive heat map as well as a cybersecurity career pathway portal. The jobs heat map is updated periodically and currently reflects that as of November 2019 there are 504,316 open jobs in cybersecurity across the United States. It further indicates that there are 997,058 individuals employed in cybersecurity. The map can be searched for cybersecurity workforce demand by state. For example, there are 8,760 open cybersecurity jobs in Michigan, 5,603 in Tennessee, and 4,533 in Indiana. One can also determine the workforce demand by major metropolitan area within a state or across state boundaries. For example, the DC Metropolitan area includes 64,089 open jobs.

NICE Cybersecurity Workforce Framework

One of the challenges in cybersecurity education, training, and workforce development is the need to be speaking the same language and having the same reference point for cybersecurity. That is why NIST as a standards organization was well positioned to publish the NICE Cybersecurity Workforce Framework -- NIST Special Publication 800-181. The NICE Framework provides a common taxonomy or lexicon for describing cybersecurity work. It is a reference resource that can be used by employers in both the public and private sectors to structure their workforce, including the development of positions descriptions, identification of training and development needs of employees as part of performance management plans, and the description of career pathways for both the incoming and current workforce. The NICE Framework also contains detailed task descriptions and knowledge, skills, and abilities statements that education and training providers can use to ensure that they are developing the workforce that employers need. For students or job seekers, it begins to demystify a career in cybersecurity by showing the variety of types of work roles that exist and the multiple career pathways for entering into and advancing in a cybersecurity career.

The program is currently embarking upon a review and update of the NICE Framework during 2020 to ensure that it remains relevant for all of the stakeholders – from employers to learners to educators and training providers – and to capture the different applications and uses of the NICE Framework. NIST announced a Request for Comments in November of 2019 and is currently reviewing the input received. NIST will engage in a consultative process to further engage stakeholders in an effort to improve the next draft of the NICE Framework. In addition to our interests to continuously improve the NICE Framework, the Executive Order on America's Cybersecurity Workforce requires the Secretary of Commerce to provide annual updates to the President regarding effective uses of the NICE Framework by non-Federal entities and make recommendations for improving the application of the NICE Framework in cybersecurity education, training, and workforce development.

The Federal Cybersecurity Workforce Assessment Act of 2015 requires the Federal Government to use the NICE Framework to assess its cybersecurity workforce and identify gaps in areas of critical need. The Executive Order on America's Cybersecurity Workforce will also extend use of the NICE Framework to federal contractors. Additionally, the executive order directs the

Secretaries of Commerce, Labor, Education, and Homeland Security, as well as the heads of other appropriate agencies, to "encourage the voluntary integration of the NICE Framework into existing education, training, and workforce development efforts undertaken by State, territorial, local, tribal, academic, non-profit, and private-sector entities, consistent with applicable law." The implementation of the Executive Order is in progress.

Growing and Sustaining the Nation's Cybersecurity Workforce

In 2017, the Department of Commerce and Department of Homeland Security delivered a report to the president entitled, "Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future".[1] The report was developed in response to Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructures that directed the Secretary of Commerce and 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."

The report sets forth a vision to "prepare, grow, and sustain a national cybersecurity workforce that safeguards and promotes America's national security and economic prosperity" and identifies four imperatives along with a corresponding set of 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.
- Imperative 2: Transform, elevate, and sustain the learning environment to grow a dynamic and diverse cybersecurity workforce.
- Imperative 3: Align education and training with the cybersecurity workforce needs of employers and prepare individuals for lifelong careers.
- Imperative 4: Establish and leverage measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

In May of 2019, the America's Cybersecurity Workforce Executive Order directed the Secretary of Commerce and the Secretary of Homeland Security, in coordination with the Secretary of Education and the heads of other agencies, to "execute, consistent with applicable law and to the greatest extent practicable, the recommendations from the report[.]"

Looking Ahead

As NICE develops its strategic plan for the next five years, a few trends continue to emerge: the need to enhance cybersecurity career discovery for learners of all ages, transform the learning process to emphasize the multidisciplinary nature of cybersecurity and the multiple career

[1] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/executive-order-13800/report

pathways, and modernize the talent acquisition process to facilitate skills-based hiring and career mobility. All of these trends and the current activities of NICE directly support the goals of the National Council for the American Worker, which Secretary Ross co-leads with Advisor Ivanka Trump. Established under Executive Order, the National Council is creating the first ever national workforce strategy. This strategy is promoting the importance of multiple pathways to careers (not just a 4-year university education), the essential role of employers as part of our national education and workforce system, the need for companies to employ skill-based hiring and the need for greater transparency in the skills that companies need and the return on investment of different educational pathways.

Conclusion

NIST is excited about the accomplishments of the National Initiative for Cybersecurity Education program in addressing the future of cybersecurity education in the U.S. in order to increase the number of skilled cybersecurity professionals helping to keep our Nation secure. NIST looks forward to continuing to support the country's ability to address current and future cybersecurity challenges through standards and best practices.

Thank you for the opportunity to testify today. I would be happy to answer any questions that you may have.

Rodney Petersen
Director of the National Initiative for Cybersecurity Education (NICE)

Rodney Petersen is the Director of the National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce. He previously served as the Managing Director of the EDUCAUSE Washington Office and a Senior Government Relations Officer. He founded and directed the EDUCAUSE Cybersecurity Initiative and was the lead staff liaison for the Higher Education Information Security Council. Prior to joining EDUCAUSE, he worked at two different times for the University of Maryland - first as Campus Compliance Officer in the Office of the President and later as the Director of IT Policy and Planning in the Office of the Vice President and Chief Information Officer. He also completed one year of federal service as an Instructor in the Academy for Community Service for AmeriCorps' National Civilian Community Corps. He is the co-editor of a book entitled "Computer and Network Security in Higher Education". He received his law degree from Wake Forest University and bachelor’s degrees in political science and business administration from Alma College. He was awarded a certificate as an Advanced Graduate Specialist in Education Policy, Planning, and Administration from the University of Maryland.