PennState
Applied Research Laboratory

P.O. Box 30
State College, PA 16804-0030
(814) 865-6531

From: Pennsylvania State University, Applied Research Laboratory

To: National Institute of Standards and Technology (NIST), Department of Commerce

SUBJECT: Growing and Sustaining the Nation's Cybersecurity Workforce
(Docket Number 170627596-7596-01)

General Information:

The Pennsylvania State University (PSU), to include the PSU Applied Research Lab (PSU/ARL), understands the critical nature of information sharing and cybersecurity, the way we buy and sell goods and the sheer amount of data shared and exchanged via technology, pointing to an increased need for a skilled workforce. This requires individuals who can recognize and anticipate failures and intrusions and those who can ensure network and system security.

PSU has created a Master of Professional Studies in Information Sciences (MPS in IS) that combines a highly relevant course curriculum real-world business issues and simulations. The program takes a multidimensional perspective on cyber-domains that is defined by using a socio-technical approach to generate solutions to complex problems. The goal is to help our students prepare for confines outside of PSU. Our College of Information Sciences and Technology (IST) is a leader among information schools, and the faculty are a diverse group of thought leaders from numerous fields, including computer science, engineering, psychology, chemistry, artificial intelligence, and more. Additionally, PSU, through the School of Electrical Engineering and Computer Science (EECS), offers Bachelor of Science (B.S.) degrees in Computer Science, Computer Engineering, and Electrical Engineering, and graduate degrees (M.S., M.Eng., and Ph.D.) in Computer Science and Engineering, and Electrical Engineering, respectively. EECS focuses on the convergence of technologies and disciplines to meet today's industrial demands.

PSU also offers a major in Security Risk Analysis (SRA). This major helps students protect organizational information, people, and other assets by applying principles of risk management. This includes skill sets in risk analysis, threat identification, risk control strategies, decision making, emergency response, and intelligence analysis. The SRA major looks at how to design systems that are secure, how to measure risk, and how ensure that proper levels of privacy are maintained for individual technology users, businesses, government, and other organizations. Within the SRA major, there are three options. At the time when a student requests entrance to the SRA major, an option must be chosen. The SRA major is based on an interdisciplinary curriculum that integrates areas of study in information assurance (both digital and physical security), intelligence analysis, and cyber forensics. It also would provide leadership and venue-specific skills needed in this area.

Finally, PSU will offer a new B.S. degree in Cybersecurity Analytics and Operations offered by Penn State's College of Information Sciences and Technology (IST) to help meet the growing demand for cybersecurity

P.O. Box 30
State College, PA 16804-0030
(814) 865-6531

professionals. The degree will be available to students at the University Park campus beginning in the fall 2017 semester. The program is one of the first of its kind in the nation, and will equip students with the knowledge and skills needed to critically assess and respond to modern information security threats. IST designed the new degree in response to a critical gap in cybersecurity education that had direct ramifications on students entering the workforce. The PSU curriculum will build on a foundation of mathematics and computer programming while addressing three key areas of expertise: technical cyber defense strategies, risk management, and data-driven cybersecurity analytics. Similar to other IST programs, the cybersecurity degree also emphasizes real-world applications across a variety of fields.

Q 2: Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

From an academic standpoint, this is a critical area that must be highlighted in order to address efforts to evolve curricula which meet the requisite knowledge/skills/abilities (KSAs) that support current and future workforce categories, specialty areas and roles. Sufficient understanding does not fully exist such that academic institutions may not adequately equip students to effectively enter a technical workforce, especially in areas such as science and engineering, which fall prey to exponentially advancing rates of technology. A growing concern from an academic perspective is how best to prepare students to enter the workforce and fill the necessary work roles, become adept in specialty areas and bolster technical workforce categories. Academic curricula should not exist in a vacuum compared to the needs of the workforce but should function as an initial training ground to foster a student's understanding of fundamental KSAs which therefore support workforce requirements. However, this must be reflected in more flexible curricula and a continually learning faculty where technical workforce KSAs become academic end states.

Q 6: What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

In higher education considerable research and debate focus on *how* to teach and the personal skills students should lean, but *what* to teach is seldom discussed. This disregard of academic curriculum leads to a substantial problem, students are not graduating with the knowledge they need to succeed in the long run (Long, 2016), http://er.educause.edu/articles/2016/4/evolving-curricula-for-an-exponential-world. The disparity between human learning rates and the rates at which technology changes can become very problematic, particularly in higher education and the associated student curricula pipelines. Additionally, the speed of curriculum change also becomes a limiting factor with regards to student knowledge of advancing technologies. Academics once received their PhD in a particular field and then proceeded to research and teach within that field for the duration of their careers. However, the rate of technology change can render their research focus irrelevant, particularly in science and engineering. Lifelong learning is essential for everyone, including faculty, but many find changes in research and teaching directions difficult to navigate. In order to keep pace with technology advances, it is imperative that higher education implement changes in two critical areas, curriculum and faculty.

PennState
Applied Research Laboratory

P.O. Box 30
State College, PA 16804-0030
(814) 865-6531

Changing curriculum entails many challenges. Adding material to the curriculum requires removing other material in order to fit within the standard four-year program. At universities, removing content is also a challenge, as there is rarely consensus as to what must be eliminated. Also, changes to curriculum must endure an elaborate and slow bureaucratic approval process, which may typically take years to complete. Faculty present an additional challenge in that many current academics were trained before the PC, Internet or cell phones were commonplace in society. As a result, today's students often spend time learning very difficult material that they don't need or has been rendered obsolete by current technologies. Therefore, these students are generally not exposed to critical information that is important to achieving success in the new Information Age.

Q 7: How will advances in technology (e.g., artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems?

Advances in technology (Artificial Intelligence, Internet of Things, etc.) pose significant risks for the cybersecurity workforce needed in the future due to the fact that the rate which technology advances and is incorporated exceeds the rate at which those advances can be incorporated into traditional academic constructs. To address such advances, PSU has begun offering minor degrees and certificates for both undergraduate and graduate students. We have also created a graduate minor program in computational science and several different undergraduate minors in information, science and technology. Students in every major can benefit from a minor, augment their foundational knowledge and still graduate in four years. And although there may be some material that should be removed from curriculum, with this particular approach, focused on a minor and/or certificate, it is not necessary and easier for faculty to embrace and implement. Therefore, the curricula can be augmented much more rapidly and keep at a closer pace to advancing technology more effectively while allowing faculty to become more flexible to shifts in technology. Our aforementioned programs at PSU seek to address these advances by providing a unique and open-ended approach to these currently undefined problem sets and position our students to become leaders in the cybersecurity field by building on the interdisciplinary foundation already in place within the college.