TESTIMONY OF

Dr. Diana L. Burley

Professor, Human and Organizational Learning
Executive Director, Institute for Information Infrastructure Protection
The George Washington University
Washington, DC

BEFORE THE

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

HEARING ON

Strengthening U.S. Cybersecurity Capabilities

February 14, 2017

Rayburn House Office Building
Washington, DC

Chairwoman Comstock, Vice Chairman Abraham, Ranking Member Johnson, members of the Committee, I am honored to appear before you today to discuss strategies for strengthening U.S. cybersecurity capabilities as our nation faces the a global threat environment where cybercrime damage is projected to exceed $2 trillion by 2019.[1]

My name is Diana Burley. I am professor of human & organizational learning and the executive director and chair of the Institute for Information Infrastructure Protection[2] (I3P) at The George Washington University (GW).

For more than 15 years, I have worked to build the nation's cybersecurity workforce by leading workforce development initiatives, defining best practices in cybersecurity education, and informing policy and practice through rigorous research and analysis. I have authored nearly 75 publications on the subject and have been honored as both the cybersecurity educator of the year and the government leader of the year; as well as a top influencer in information security careers. In short, my experiences across government, academia and industry provide me with a unique vantage point from which to offer the committee insight and recommendations on building the nation's cybersecurity workforce.

In my remarks today I will:

- Provide background and describe the current cybersecurity workforce context;
- Discuss workforce development recommendations offered in the January 2017 CSIS Cyber Policy Task Force report and the December 2016 report of the Commission on Enhancing National Cybersecurity; and
- Suggest actionable steps toward meeting the national need for a cybersecurity workforce capable of meeting the evolving threat.

Taken together, my recommendations support a holistic approach to building the nation's cybersecurity workforce – one that includes both evidence-based short-term interventions that address immediate needs, and strategic long-term initiatives that address the entire ecosystem of educational, professional and environmental challenges.

Institute for Information Infrastructure Protection

The I3P is a national consortium of leading academic institutions, national laboratories, and non-profit research organizations. The I3P is housed at The George Washington University where I manage the consortium in collaboration with SRI International and an executive committee currently comprised of representatives from Johns Hopkins University Applied Physics Laboratory, Dartmouth College, the MITRE Corporation, and the University of California, Davis. In my role as executive director and chair I work with

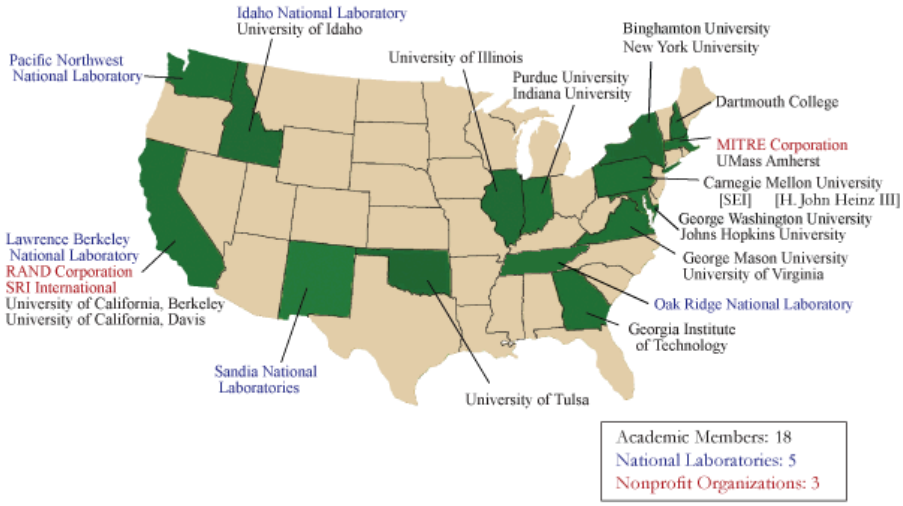
[1] https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
[2] I3P website: http://www.thei3p.org
[2] I3P website: http://www.thei3p.org

our executive committee to establish strategic priorities, engage with project sponsors, launch and manage research projects, and advise stakeholders on research results.

Since its' founding in 2002 at Dartmouth College, the I3P has been a cornerstone in cybersecurity research and development. The I3P brings together researchers, government officials, and industry representatives to address cybersecurity challenges affecting the nation's critical infrastructure. Drawing from its member institutions, the I3P assembles multi-disciplinary and multi-institutional research teams that bring in-depth analysis to complex cybersecurity challenges. The I3P's impact on cybersecurity research, policy, and practice has taken many forms, including:

- **49 national workshops** that convened cybersecurity subject matter experts across academia, government and industry to address challenges related to security the nation's critical information infrastructure.
- **65+ journal papers** resulting from I3P driven research projects (many of these projects were sponsored by the Department of Homeland Security, the National Institute of Standards and Technology, and the National Science Foundation).
- **366+ technical reports, workshop and conference proceedings, and Congressional testimonies** produced by I3P researchers and disseminated to national (and in many instances, global) stakeholders.
- **12 tools/technology transfers** between academic institutions, national laboratories, non-profit research institutions, and government agencies.
- **19 postdoctoral research fellowships** that advanced scientific discovery and dissemination by linking researchers across academia, government and industry.

The 26-member I3P consortium includes 18 academic research institutions, 5 national laboratories, and 3 nonprofit research organizations – a roster that brings intellectual breadth and depth to the analysis of cybersecurity challenges.



The Cybersecurity Workforce Context

As evidenced by this hearing today, building a highly capable cybersecurity workforce remains a top national priority. To meet this critical workforce need, the U.S. federal government sponsors several major initiatives.

The U.S. National Science Foundation Scholarship for Service: Cyber Corps program provides scholarships to students who will join the federal cybersecurity workforce and capacity building funds to academic institutions developing cybersecurity programs. I led this program from 2004-2007. During that period, the federal government was challenged with building a cybersecurity workforce that had little structure, uncertain priorities, and limited awareness of the nature of the threat or specific workforce needs. The federal government also faced significant challenges in attracting young professionals to public service. In addition to these demand-side challenges, academic institutions tasked with providing a supply of new professionals, were largely developing programs alone. With the exception of the National Security Agency (NSA) Centers of Academic Excellence (CAE) [3] program, which provides curricular content for programs in information assurance, academic institutions had little guidance on how to develop cybersecurity programs. Since that time, federal efforts led by the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE)[4] have established a workforce framework with work roles and career pathways, assisted in the development of workforce priorities, raised awareness of workforce and educational needs, and contributed to the generation of curricular resources to aid in program development.

These initiatives are, in large part, responsible for the steady increase the number of cybersecurity professionals entering the national workforce. Yet, while these federal programs serve as a major driver of the cybersecurity workforce, they have not been sufficient to address the growing demand. In fact, despite significant efforts to increase the size and quality of the workforce, the U.S. still faces a projected shortfall of nearly 1.5 million cybersecurity-related professionals by 2020[5]. The workforce need is acute, immediate, and the gap between supply and demand is growing.

Recent Recommendations to Build the Cybersecurity Workforce

Recent reports by the CSIS Cyber Policy Task Force and the Commission on Enhancing National Cybersecurity recognize this critical need and identify cybersecurity workforce development as a critical success factor for strengthening U.S. cybersecurity capabilities.

[3] NSA Centers of Academic Excellence Program: https://www.nsa.gov/ia/academic_outreach/nat_cae/
[4] National Initiative for Cybersecurity Education: http://csrc.nist.gov/nice/about.html
[5] See, for example, CSO Online: http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

Specifically, the January 2017 CSIS report, "From Awareness to Action: A Cybersecurity Agenda for the 45th President[6]," recommends:

> "The next administration should develop and implement an ambitious education and workforce model for cybersecurity, with a system for accrediting training and educational institutions; a taxonomy of cybersecurity roles and the skills that practitioners must demonstrate to claim competence in each specialty; and a robust network of professional credentialing entities."

A Comprehensive Model

The call for a comprehensive cybersecurity education and workforce development model that standardizes interdisciplinary curricula, serves as a foundation for accreditation efforts, integrates with existing programs, and provides the taxonomy of work roles, is echoed in recommendation 4.1 of the Commission on Enhancing National Cybersecurity report[7].

In fact, academic institutions are also calling for a comprehensive curricular model. Institutions across the spectrum of computing disciplines are launching initiatives to establish cybersecurity programs and need curricular guidance based on a holistic view of the cybersecurity field, the specific demands of the base computing discipline, and the relationship between the curriculum and cybersecurity workforce frameworks.

The Association for Computing Machinery (ACM) Joint Task Force on Cybersecurity Education (JTF)[8] is developing the curricular model called for by these groups. As the first set of global curricular guidelines in cybersecurity education, Cybersecurity 2017 (CSEC2017) will provide:

- Comprehensive and flexible curricular guidance in cybersecurity education that will support future program development and associated educational efforts at the post-secondary level.
- A curricular volume that structures the cybersecurity discipline and provides guidance to institutions seeking to develop or modify a broad range of programs rather than a prescriptive document to support a single program type.

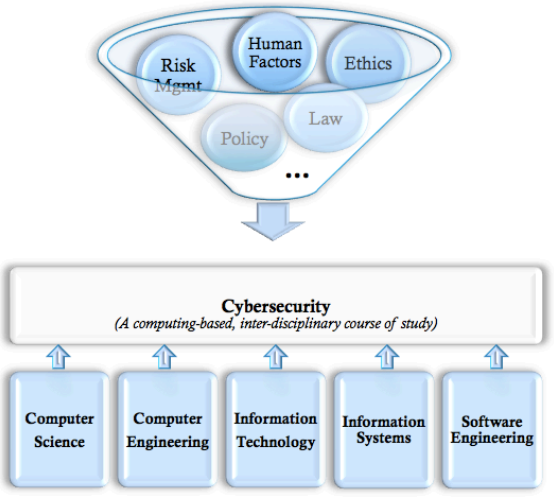
I serve as the CSEC2017 task force co-chair. The development process is well underway and the curricular volume will be published in late 2017. **I strongly urge the federal government to leverage this effort in the implementation of the recent recommendations for several key reasons.**

---

[6] CSIS report: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf
[7] Commission on Enhancing National Cybersecurity: https://www.nist.gov/cybercommission
[8] ACM Joint Task Force: http://CSEC2017.org

First, the CSEC2017 is being developed by global subject matter experts across academia, government and industry; and the professional societies leading this effort have nearly 50 years of experience developing curricular guidance. With over 100,000 members, the ACM is the largest global computing society. For nearly five decades, starting with Computer Science 1968[9], the ACM has collaborated with other professional and scientific societies to establish curricular guidelines for academic program development in the computing disciplines[10]. Currently, ACM curricular volumes provide guidance in computer science, computer engineering, information systems, information technology, and software engineering. The curricular recommendations produced by this task force will be endorsed by major international computing societies: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS)[11], Association for Information Systems Special Interest Group on Security (AIS SIGSEC)[12], the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)[13], and the Cyber Education Project (CEP)[14].

Second, the model is grounded in both the interdisciplinary nature of cybersecurity and the inherently technical foundation of the field. Cybersecurity is emerging as an identifiable discipline. While cybersecurity is an interdisciplinary course of study; including aspects of law, policy, human factors, ethics, and risk management; it is fundamentally a computing-based discipline. As such, and as depicted below, academic programs in cybersecurity are both informed by the inter-disciplinary content, and driven by the needs and perspectives of the computing discipline that forms the programmatic foundation.



[9] ACM Curriculum Committee on Computer Science. 1968. Curriculum 68: Recommendations for Academic Programs in Computer Science. *Comm. ACM* 11, 3 (Mar. 1968), 151-197.
[10] ACM Computing Disciplines Overview: http://acm.org/education/curricula-recommendations
[11] IEEE CS website: https://www.computer.org/
[12] AIS SIGSEC website: http://aisnet.org/group/SIGSEC
[13] IFIP WG 11.8 website: https://www.ifiptc11.org/wg118
[14] Cyber Education Project website: http://cybereducationproject.org/about/

Cybersecurity programs require curricular content that includes: (1) the theoretical and conceptual knowledge essential to understanding the discipline and; (2) opportunities to develop the practical skills that will support the application of that knowledge. The content included in any cybersecurity program is requires a delicate balance of breadth, depth, along with an alignment to workforce needs. It also demands a structure that simultaneously provides for consistency across programs of similar types while allowing for flexibility necessitated by both local needs and advancements in the body of knowledge.

Third, the CSEC2017 model organizes curricular content, facilitates the alignment between curricular content and workforce frameworks, and forms the foundation of emerging accreditation standards. The CSEC2017 joint task force is actively coordinating with workforce framework developers within the federal government in order to provide a bridge between the curricular content and specific work roles. In addition, members of the task force also serve as leaders in the Accreditation Board for Engineering and Technology (ABET) process to develop accreditation criteria for both computer science-based and engineering-based cybersecurity degree programs.

Credentialing

The CSIS and Commission reports also assert the need for additional professionalization requirements; advanced training, skill-based demonstrations, and a network of credentialing associations all have been advanced as important components of a comprehensive workforce development strategy.

The call for additional credentialing requirements is not new. Although I strongly support the need to ensure cybersecurity professionals have and maintain the highest level of competency, I also caution against blanket professionalization requirements that do not consider differences in occupational needs. In 2013, I co-chaired the U.S. National Research Council Committee on Professionalizing the Nation's Cybersecurity Workforce[15]. Our report, sponsored by the Department of Homeland Security, highlighted the breadth of the field and provided criteria for decision-makers on whether, when, and how to assess the need for additional professional requirements. We argue that before professionalization activities such as licensure, certifications, or skill-based exams are undertaken, an occupation must have well-defined characteristics: stable knowledge and skill requirements, stable job roles, occupational boundaries, and career ladders. Further, the specific workforce deficiencies to be remedied by the professionalization mechanism must be identified and aligned with the intervention.

As a final step to determining if additional credentialing requirements are appropriate, the tradeoffs associated with additional requirements must be considered:

- *Do the benefits of a given professionalization measure outweigh the potential supply restrictions resulting from the additional barriers to entry?*

[15] Professionalizing the Nation's Cybersecurity Workforce: https://www.nap.edu/read/18446/chapter/1

- *Does the potential to provide additional information about a candidate outweigh the risks of false certainty about who is actually best suited for a job?*

- *Do the benefits of establishing the standards needed for professionalization outweigh the risks of:*

    - *Obsolescence (when the knowledge or skills associated with the standard are out-of-date by the time a standard is agreed on) and*

    - *Ossification (when the establishment of a standard inhibits further development by workers of their skills and knowledge)?*

It is important to note that professionalization can serve as a magnet that attracts people to the occupation, as a funnel that restricts the supply of people entering the occupation, or as a sieve that filters people out of the occupation based on increased requirements.[16]

Given the significant workforce shortages, a thoughtful approach to additional credentialing requirements must be taken. The danger of increased requirements leading to people exiting the field is particularly important given the increasingly integrated nature of cybersecurity work roles. The Commission on Enhancing National Cybersecurity report highlights this point, asserting that "cybersecurity work roles and responsibilities are increasingly being integrated into a growing array of jobs at all levels with nearly all organizations.[17]" Individuals performing these hybrid roles will likely be subject to an abundance of requirements. While additional requirements associated with additional responsibilities will most certainly be expected, workforce development framers should be careful not to unnecessarily overload professionals.

I urge the federal government to consider the recommendations put forth in the National Research Council Professionalizing the Nation's Cybersecurity Workforce: Criteria for Decision-Making report before implementing additional professionalization and credentialing requirements.

Building the Workforce Pipeline

Developing the K-12 pipeline is a key strategy for building a cybersecurity workforce of sufficient capacity and capability to address current and emerging threats. K-12 educators (teachers, counselors, and administrators) are a critical factor in supporting student participation in cybersecurity career development activities (e.g. high school computer science curricula, cybersecurity competitions and clubs). As such, cybersecurity educators provide an increasing number of professional development opportunities for K-12 educators. These opportunities typically take the form of summer boot camps, workshops and access to resources.

[16] Diana L. Burley, Jon Eisenberg, and Seymour E. Goodman. 2014. Would cybersecurity professionalization help address the cybersecurity crisis?. *Commun. ACM* 57, 2 (February 2014), 24-27. DOI: https://doi.org/10.1145/2556936

[17] cite quote

While helpful, these professional development efforts leave major gaps. First, they primarily target computer science or technically oriented teachers; leaving out the vast majority of K-12 teachers and administrators. Second, they rely on the participation of self-selected teachers who have the time, interest and pre-requisite knowledge to take advantage of the opportunities. Third, teachers have limited support for integrating the cybersecurity content into their courses. Fourth, the current approach is primarily focused on 'raising awareness' of cybersecurity topics for the vast majority of K-12 teachers, counselors, and administrators. While awareness is important, as the primary interface with the students we want enter the cybersecurity career pipeline, K-12 educators need more than post-degree professional development. They need cybersecurity educational opportunities that are integrated into their formal educational degree programs.

I recommend that the federal government collaborate with post-secondary colleges of education to develop and disseminate curricular guidance and resources for teachers, administrators, and other school staff members to provide a continuum of learning experiences which result in the development of actual cybersecurity skills and a portfolio of teacher-developed resources to support the integration of cybersecurity and cybersecurity career awareness into broad teaching practice.

Raising Awareness

Both reports call on the new administration to implement programs that will raise awareness and engagement among the general citizenry. In this context, the term "engagement" is key.

I recommend that cybersecurity awareness programs be reconstituted to emphasize the behavioral changes that depend on participant engagement. Raising awareness of cybersecurity threats is necessary but behavioral change relies on participant understanding of the impact of their actions.

Broadening Participation

Efforts to attract women, members of underrepresented minority groups, and veterans to the cybersecurity field are growing. These types of programs should be expanded to consider other special populations. For instance, several programs that focus on individuals with desired cognitive traits for specific work roles are being piloted to target potentially well-qualified entrants who think critically, rapidly recognize patterns, efficiently analyze quantitative data, and focus precisely: the exact profile of many cognitively able individuals with autism. At GW, we are launching the CyberBlue™ initiative – a collaboration between the I3P and the Autism and Neurodevelopmental Disorders Institute (AND), as a bold, scalable solution that uses one social challenge to solve another.[18] I recommend that the federal government encourage the development and implementation of creative solutions such as CyberBlue™ that expand the cybersecurity workforce pipeline beyond traditional populations.

[18] CyberBlue™ video introduction: https://youtu.be/oJhzM4ttW-E

The field also suffers from a lack of leaders. Strategies to increase the supply of mid-level and senior-level employees with the cybersecurity experience and capabilities are critical.

I support the recommendations offered to build an executive cyber corps equipped with knowledge of technical cybersecurity concepts, the organizational and behavioral phenomena that will impact the successful implementation of cybersecurity initiatives, and advanced research and analytical skills that will allow them to adapt strategies in the face of evolving and increasingly complex threats.

Summary

Despite significant efforts to increase the size and quality of the workforce, a persistent and growing gap between supply and demand for skilled cybersecurity professionals exists. Strengthening U.S. cybersecurity capabilities requires a comprehensive and coordinated effort to build the cybersecurity workforce.

While workforce development experts assert the need to quickly surge the cybersecurity workforce, the recommendations implemented by the federal government must address both short- and long-term needs. A holistic approach to building the nation's cybersecurity workforce must include both evidence-based short-term interventions that address immediate needs, and strategic long-term initiatives that address the entire ecosystem of educational, professional and environmental challenges.

Actions implemented as a result of these recommendations should be empirically based, sustainable and scalable. Current initiatives are constrained by limited resources and a lack of models. These limitations prohibit the type of scaling which will be necessary if these programs are to meet an ever-growing societal need for a cadre of cybersecurity professionals.

The needs are immediate and the challenges are broad. So broad, in fact, that, as then NSA Director Admiral Michael Rogers said to the House (Select) Intelligence Committee in 2014, "It is going to take a true partnership between the private sector, the government, and academia to address [them]."[19]

I urge the federal government to leverage existing multi-sector stakeholder groups – consortia like the I3P, to integrate, accelerate, and guide existing cybersecurity workforce development activities that address both short- and long-term needs.

[19] https://www.nsa.gov/news-features/speeches-testimonies/testimonies/adm-rogers-testimony-20nov2014.shtml

Strengthening U.S. Cybersecurity Capabilities
Summary Testimony of Dr. Diana L. Burley

Strengthening U.S. cybersecurity capabilities requires a comprehensive and coordinated effort to build the cybersecurity workforce. Despite significant efforts to build the workforce, the gap between supply and demand persists. The workforce need is acute and immediate with a projected shortfall of nearly 1.5 million by 2020.

Of the recommendations offered in the recent reports by the Commission to Enhance National Cybersecurity and the CSIS Cyber Policy Task Force, I will address two:

Summary Recommendation 1: Develop a comprehensive cybersecurity education and workforce development model that standardizes interdisciplinary curricula, serves as a foundation for accreditation, and integrates with existing programs and taxonomies.

Comment: The Association for Computing Machinery (ACM) Joint Task Force on Cybersecurity Education is developing this type of model. As the first set of global curricular guidelines in cybersecurity education, CSEC2017 will structure the cybersecurity discipline, and provide comprehensive and flexible curricular guidance. I co-chair the CSEC2017 task force and the volume will be published in late 2017.

- The ACM has nearly 50 years of experience developing curricular guidance.
- The CSEC2017 is being developed by global subject matter experts across academia, government and industry; and will be endorsed by major computing societies: ACM, IEEE Computer Society, Association for Information Systems, and the International Federation for Information Processing.
- The model is grounded in both the interdisciplinary nature of cybersecurity and the inherently technical foundation of the field. It facilitates the alignment between curricular content and workforce frameworks, and forms the foundation of emerging accreditation standards.

Summary Recommendation 2: Add new credentialing requirements such as advanced training, skill-based demonstrations; and develop a network of credentialing associations.

Comment: The call for additional credentialing requirements is not new. I support the need to ensure cybersecurity professionals maintain the highest level of competency, but caution against blanket professionalization requirements that do not consider differences in occupational needs. Cybersecurity is a broad field with many occupations and the needs of each occupation must be considered separately. I co-chaired the 2013 National Research Council Committee on Professionalizing the Nation's Cybersecurity Workforce that addressed this issue. Before professionalization activities such as certifications or skill-based exams are undertaken, consider the occupational characteristics, specific workforce deficiencies, and the trade-offs associated with additional requirements.

To meet the growing societal need for a cadre of cybersecurity professionals, initiatives should address both short- and long-term needs; be empirically based and scalable; engage a broad cross-section of society; and target entry-, mid- and senior-level professionals. I urge the federal government to leverage existing multi-sector stakeholder groups – consortia like the I3P, to integrate, accelerate, and guide existing cybersecurity workforce development activities.