Association for Computing Machinery (ACM)

acm.org
facebook.com/associationforcomputingmachinery
twitter.com/theofficialacm

August 2, 2017

Cybersecurity Workforce RFI
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development – Docket No. 170627596-7596-01

Dear NIST:

Thank you for the opportunity to comment on current, planned, or recommended education and training programs aimed at strengthening the U.S. cybersecurity workforce., 82 Fed. Reg. 32172 (Jul. 12, 2017), Docket No. 170627596-7596-01. We provide responses to specific questions given in the Notice.

With more than 100,000 members, ACM (Association for Computing Machinery) is the world's largest educational and scientific computing society, uniting computing educators, researchers, and professionals to inspire dialogue, share resources, and address the field's challenges. These comments were developed by the ACM Joint Task Force on Cybersecurity Education. ACM Joint Task Force statements represent the views of the Task Force and do not necessarily represent the views of the Association.

Responses to Specific Questions

General Information

Question 1: Are you involved in cybersecurity workforce education or training (e.g., curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)?

The response is offered from the Joint Task Force on Cybersecurity Education[1]. In August 2015, the ACM Education Board initiated a Joint Task Force on Cybersecurity Education in collaboration with other professional and scientific computing societies to develop comprehensive curricular guidance in cybersecurity education.

[1] ACM Joint Task Force: http://CSEC2017.org

For nearly five decades, starting with Computer Science 1968[2], the ACM education initiative has collaborated with other professional and scientific societies to establish curricular guidelines for academic program development in the computing disciplines. Currently, ACM curricular volumes provide recommendations in computer science, computer engineering, information systems, information technology, and software engineering[3].

The Joint Task Force on Cybersecurity Education (JTF), launched in September 2015, is a collaboration between major international computing societies: the Association for Computing Machinery (ACM), the IEEE Computer Society (IEEE CS)[4], the Association for Information Systems Special Interest Group on Security (AIS SIGSEC)[5], the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)[6]; and the Cyber Education Project (CEP). The curricular guidance is expected to be released in late 2017 as a volume entitled, "CSEC2017."

JTF members each have deep expertise and broad experience in cybersecurity education and curriculum development. These nine leading cybersecurity professionals were selected by the participating professional societies to provide a diverse set of perspectives in the development process. The JTF members, along with their affiliations, are listed below:

Diana L. Burley, Ph.D. (JTF Co-Chair, ACM/CEP)
Professor, Human & Organizational Learning
Executive Director, Institute for Information Infrastructure Protection
The George Washington University, USA

Matt Bishop, Ph.D. (JTF Co-Chair, ACM/IFIP)
Professor, Computer Science
Co-Director, Computer Security Laboratory
University of California, Davis, USA

Scott Buck (ACM/CEP)
University Program Director
Intel Corporation, USA

Joseph J. Ekstrom, Ph.D. (IEEE CS)
Associate Professor, Information Technology
Brigham Young University, USA

[2] ACM Curriculum Committee on Computer Science. 1968. Curriculum 68: Recommendations for Academic Programs in Computer Science. *Comm. ACM* 11, 3 (Mar. 1968), 151-197.
[3] ACM Computing Disciplines Overview: http://acm.org/education/curricula-recommendations
[4] IEEE CS website: https://www.computer.org/
[5] AIS SIGSEC website: http://aisnet.org/group/SIGSEC
[6] IFIP WG 11.8 website: https://www.ifiptc11.org/wg118

Lynn Futcher, Ph.D. (ACM/IFIP)
Associate Professor
Nelson Mandela Metropolitan University, South Africa

BGen (ret) David S. "Hoot" Gibson, Ph.D. (ACM/CEP)
Professor Emeritus
Department of Computer Science
United States Air Force Academy, USA

Elizabeth Hawthorne, Ph.D. (ACM/CEP)
Senior Professor, Computer Science
Union County College, USA

Siddharth Kaza, Ph.D. (ACM)
Associate Professor, Computer & Information Science
Chair, Department of Computer & Information Science
Towson University, USA

Yair Levy, Ph.D. (AIS SIGSEC)
Professor, Information Systems and Cybersecurity
Director, Information Assurance and Cybersecurity Programs
Director, Center for e-Learning Security Research (CeLSR)
Nova Southeastern University, USA

Herbert Mattord, Ph.D. (AIS SIGSEC)
Associate Professor, Information Systems
Associate Director, Center for Information Security Education
Kennesaw State University, USA

Allen Parrish, Ph.D. (IEEE CS/CEP)
Professor, Cyber Science
Chair, Department of Cyber Science
United States Naval Academy, USA

Growing and Sustaining the Nation's Cybersecurity Workforce

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

The National Cybersecurity Workforce Framework (NCWF) provides a comprehensive listing of workforce categories, specialty areas, work roles and their associated knowledge/skills/abilities. The JTF references the current version of this framework in the curricular guidance.

Question 4: What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (e.g., energy vs financial sectors)?

The cybersecurity workforce is broad and complex. Using the National Cybersecurity Workforce Framework as a frame of reference, the workforce contains no fewer than 52 different work roles. While all members of the cybersecurity workforce should have a basic understanding of foundational concepts, specific knowledge and skill requirements will vary based on the work role. Given this variability, it is important to provide guidance on how to link work role requirements to the cybersecurity curricular guidelines. Moreover, these skill requirements can vary by industry sector; and over time.

In addition to specific content such as knowledge areas, knowledge units, and topics; the curricular guidance being developed by the JTF provides a framework for linking academic curriculum to professional practice through the use of curricular roadmaps to assist stakeholders (students, faculty, and practitioners) visualize the pathway between academic programs and workforce requirements. Each roadmap provides a rationale for knowledge and its importance for the specific work role; outlines a mechanism for identifying relevant courses and course modules within an academic institution; outlines strategies for obtaining the knowledge when specific courses are not available or accessible within the institution; and highlights challenges (and associated strategies to overcome them) to following the suggested course of study.

Question 5: Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

While several effective cybersecurity programs exist, the country is in need of a broad, flexible curricular guidance that will support the development of cybersecurity programs at a range of academic institutions. This type of guidance will support the development of scalable solutions that will narrow the gap between the supply and demand of qualified cybersecurity professionals across a range of work roles. The JTF is developing this curricular framework. As the first set of global curricular guidelines in cybersecurity education, we anticipate that the Cybersecurity 2017 (CSEC2017) curricular volume will be the leading resource of comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity offerings at the post-secondary level including associate- and baccalaureate programs. The CSEC2017 curricular volume 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.

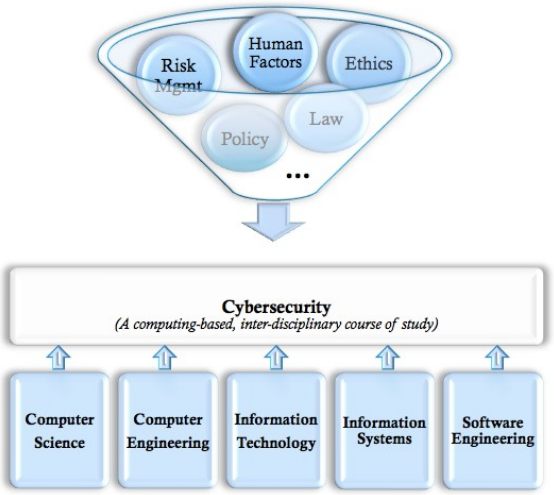
- A curricular volume that structures the cybersecurity discipline and provides guidance to institutions seeking to develop or modify a broad range of programs, concentrations and/or courses rather than a prescriptive document to support a single program type.

We urge the federal government to leverage this effort in the implementation of future cybersecurity education and workforce development strategies for several reasons.

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 in the computing fields. With over 100,000 members, the ACM is the largest global computing society. For nearly five decades, starting with Computer Science 1968[7], the ACM has collaborated with other professional and scientific societies to establish curricular guidelines for academic program development in the computing disciplines[8]. 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: the Association for Computing Machinery (ACM), the IEEE Computer Society (IEEE CS)[9], the Association for Information Systems Special Interest Group on Security (AIS SIGSEC)[10], the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)[11], and the Cyber Education Project (CEP)[12].

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 that includes 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.

[7] ACM Curriculum Committee on Computer Science. 1968. Curriculum 68: Recommendations for Academic Programs in Computer Science. *Comm. ACM* 11, 3 (Mar. 1968), 151-197.
[8] ACM Computing Disciplines Overview: http://acm.org/education/curricula-recommendations
[9] IEEE CS website: https://www.computer.org/
[10] AIS SIGSEC website: http://aisnet.org/group/SIGSEC
[11] IFIP WG 11.8 website: https://www.ifiptc11.org/wg118
[12] 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 for cybersecurity competency. The content included in any cybersecurity program is requires a delicate balance of breadth and 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.

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

Through the JTF CSEC2017 curricular guidance, the nation has a significant opportunity to leverage the collective expertise and efforts of leading professional computing associations; representing the broad spectrum of community stakeholders (academic leaders, training providers, and practitioners) that will support scalable program development. By accomplishing the following goals, the curricular volume will enable efficient program development and growth:

- To describe a vision of proficiency in cybersecurity;

- To define a structure for the cybersecurity discipline by developing a thought model that defines the boundaries of the discipline and outlines key dimensions of the curricular structure;
- To support the alignment of academic programs and industry needs in cybersecurity;
- To involve broad global audience of stakeholders through continuous community engagement during the development process;
- To develop curricular guidance that is comprehensive enough to support a wide range of program types; and
- To develop curricular guidance that is grounded in fundamental principles that provide stability, yet is structured to provide flexibility to support evolving program needs.

Thank you again for the opportunity to comment on education and training programs aimed at strengthening the U.S. cybersecurity workforce. The members of the ACM Joint Task Force on Cybersecurity Education are available if you have questions or would like additional information about the issues raised in this public comment.

Sincerely,

The Joint Task Force on Cybersecurity Education