THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Institute for Information Infrastructure Protection (I3P)
thei3p@gwu.edu
http://www.thei3p.org

2100 Pennsylvania Avenue NW
Suite 310
Washington, DC 20037
t 202-994-5829

44983 Knoll Square
Suite 147
Ashburn, VA 20147
t 571-553-3761

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 provide comments on education and training programs focused on strengthening the U.S. cybersecurity workforce – 82 Fed. Reg. 32172 (Jul. 12, 2017), Docket No. 170627596-7596-01. This document includes responses to specific questions outlined in the Notice.

The Institute for Information Infrastructure Protection (I3P)[1] is a national consortium of leading academic institutions, national laboratories and non-profit research organizations that identifies critical challenges in information infrastructure protection, sustains a collaborative community of multidisciplinary researchers to address them, serves as a trusted partner for industry and government, and provides an independent forum that facilitates the open exchange of ideas.
The I3P is hosted by The George Washington University and managed in collaboration with SRI International. 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 cyber security challenges. Member institutions are listed at the end of this response.

The I3P executive director prepared the comments provided in this document with input from a subset of I3P representatives. The views do not necessarily represent the views of the full membership or their institutions.

Comments on 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)?

Dr. Diana L. Burley, the I3P Executive Director, is a global leader in cybersecurity education and workforce development and each of the 26 member institutions are recognized leaders in cybersecurity workforce development. The I3P institutional representatives have broad experience developing and leading cybersecurity educational programs as university faculty members and administrators; and as government executives and leaders in non-profit research institutions responsible for addressing cybersecurity workforce needs. Dr. Burley's biography, along with the list of institutions and institutional representatives, is included at the end of this response.

[1] Institute for Information Infrastructure Protection, http://www.thei3p.org

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Institute for Information Infrastructure Protection (I3P)
thei3p@gwu.edu N
http://www.thei3p.orgN

2100 Pennsylvania Avenue NW N
Suite 310 N
Washington, DC 20037N
t N202-994-5829N

44983 Knoll Square N
Suite 147 N
Ashburn, VA 20147N
t N571-553-3761N

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); developed through the collective efforts of multiple federal agencies, industry working groups and academic participants; provides a comprehensive listing of workforce categories, specialty areas, work roles and their associated k n o w l e d g e /skills/abilities.

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 breadth of the cybersecurity workforce is highlighted by the 52 different work roles identified in the National Cybersecurity Workforce Framework. All members of the cybersecurity workforce should have a basic understanding of fundamental cybersecurity principles and concepts, however, specific knowledge and skill requirements will vary based on the work role and the context.

I3P members are particularly focused on preparing a cybersecurity workforce that is better able to protect critical industrial infrastructures from cyber attack. Three primary challenges underpin any discussion on how to better protect the nation's critical industrial infrastructures from cyber attack. First, the digital economy depends entirely on the availability of reliable, uninterrupted electricity. Second, there exists an extreme shortage of skilled operational technology (OT) cybersecurity practitioners necessary to secure the grid and its numerous generation, transmission, and distribution elements. Third, the nation's current capacity to develop substantial numbers of new OT cybersecurity practitioners is almost non-existent.

Institute for Information Infrastructure Protection (I3P)
thei3p@gwu.edu
http://www.thei3p.org
2100 Pennsylvania Avenue NW
Suite 310
Washington, DC 20037
t 202-994-5829
44983 Knoll Square
Suite 147
Ashburn, VA 20147
t 571-553-3761

Regarding 2nd challenge: After defining the minimum set of capabilities one must possess to be considered a skilled OT cybersecurity practitioner, establish a baseline by determining how many skilled OT cybersecurity practitioners we currently have in Fed Government (including DoD, DOE, DHS), industrial sector asset owner/operators, technology supplier and services companies.

Regarding the 3rd challenge: Working with the DOE, DHS, DoD, universities, cybersecurity training companies and industry stakeholders, develop a curriculum and pipeline to speed the development of an OT security workforce large enough to meet the challenges of the next decade. Supporting the expansion of current efforts like the ACM Joint Task Force on Cybersecurity Education can expedite these workforce development priorities.

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?

Several effective cybersecurity programs exist. In fact, many of these programs are offered at I3P member institutions. However, in order to scale cybersecurity workforce development activities, the U.S. needs model curricular guidance to support a range of cybersecurity programs. The Joint Task Force on Cybersecurity Education (JTF)[2] is developing the first set of global cybersecurity curricular guidelines to support these scalable solutions. As a collaboration between major computing societies: the Association for Computing Machinery (ACM), IEEE- Computer Society, the Association for Information Systems (AIS), and the International Federation of Information Processing (IFIP), the JTF is producing comprehensive cybersecurity guidance to support the development of a broad range of post-secondary cybersecurity program offerings. The I3P executive director, Dr. Burley, and executive committee member Dr. Matthew Bishop of the University of California at Davis, lead this development effort. The mission of the CSEC2017 curricular volume is to provide:

- Comprehensive and flexible curricular guidance in cybersecurity education that will support future program development and associated educational efforts at the post- secondary level; and
- 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.

[2] Joint Task Force on Cybersecurity Education website: http://www.csec2017.org

Institute for Information Infrastructure Protection (I3P)
thei3p@gwu.edu N
http://www.thei3p.orgN

2100 Pennsylvania Avenue NW N
Suite 310 N
Washington, DC 20037N
t N202-994-5829N

44983 Knoll Square N
Suite 147 N
Ashburn, VA 20147N
t N571-553-3761N

Combined response to questions 6 and 7. (6) What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development? (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 (CPS)?

Cybersecurity savvy workforces need to be developed, not just in computer science and engineering, but it all disciplines, from civil engineering to biology, and beyond. Adopting a broad definition of cybersecurity to provide a foundation for workforce development efforts will support the development of cybersecurity across the curriculum initiatives. As such, we support the following definition of cybersecurity developed by the ACM Joint Task Force on Cybersecurity Education:

"A computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries."

While government agencies and national programs can, and should, foster cybersecurity education and workforce development priorities, it is of critical importance that these entities support broad-based community initiatives led by collaborations between professional societies, academicians, and industry-based practitioners.

Role and Adversary-based Preparation

Persistent challenges in cybersecurity workforce development include:

- Disagreement about the exact nature of the need and workforce priorities;
- Uneven attention to parts of the workforce development ecosystem;
- Inconsistent academic programs; and
- Unclear linkages between academic program (content) and job readiness (competence).

Addressing these challenges requires that we move away from "general" discussions of cybersecurity education and toward specific (or role-based) preparation models that include a combination of knowledge and skill development tailored for the specific needs of the workplace context and job function. The ACM Joint Task Force is taking this approach. Consider, for instance, the specific needs of the OT workforce.

Workforce Demands in OT

Present estimates put the number of US and allied OT security practitioners in the hundreds, while demand signals and technical trends indicate we need at least several thousand in near- mid-term timeframe, and possibly many more than that in the long term. The challenge is ponderously large, yet the pressing need demands swift action. As a nation, we must grow a substantial workforce of highly trained and experienced OT security practitioners to better secure DoD and critical industrial infrastructure (CI) sectors.

What might not be initially obvious is the increasing presence of OT devices outside traditional industrial environments. OT is now finding its way into homes and the everyday lives of consumers

Institute for Information Infrastructure Protection (I3P)
thei3p@gwu.edu
http://www.thei3p.org
2100 Pennsylvania Avenue NW
Suite 310
Washington, DC 20037
t 202-994-5829
44983 Knoll Square
Suite 147
Ashburn, VA 20147
t 571-553-3761

and small businesses via so-called IoT systems. Not only is the availability and increasing ubiquity of these devices (and the Internet services that enable them) becoming more important in our society (e.g., home automation, smart roadways and vehicles, medical devices, etc.) but the implementation quality of privacy protecting elements of cyber security - integrity and confidentiality - will influence how rapidly the technologies are accepted as we seek to enjoy their full benefits.

One thing is certain: the rapid spread of IoT and Industrial IoT (IIoT) technologies will only serve to exacerbate the shortfall in OT security practitioners. It's a yawning national security gap we must begin to close.

We offer the following set of recommendations:
This will be the work of several years and possibly a decade. However, the initial tasks will likely include:

- Conduct a precise survey to capture a broad OT security practitioner headcount baseline / starting point;
- Identify all current OT security practitioner workforce development initiatives underway at DOE and DOE labs, DHS, DoD, as well as commercial orgs and academic institutions;
- Examine orthogonally related interest groups and clubs (e.g., STEM, robotics, makers, etc.);
- Examine current time and monetary commitments DoD and critical infrastructure sector organizations to educate / train their employees to become OT security practitioners;
- Per above, seek to uncover their tolerance for having employees do rotations / residencies … living and working in operational environments to improve their skills and increase their exposure to a broader variety of systems;
- Identify stakeholders and their primary interests and drivers in this domain; and
- We must simultaneously train selected mid-career workers for short and mid-term numerical gains and initiate a college curriculum pipeline that will greatly and sustainably expand the numbers in the longer-term.

    - Mid-career: IT cybersecurity professionals should be trained in OT principles; OT professionals (e.g. electric utility engineers and operators, naval propulsion engineers and operators, etc.) will be trained in OT-tuned cybersecurity principles. This training must include both classroom and on-line coupled with extensive hands-on experiences in the field.
    - College: By injecting OT material into existing cyber curricula and cyber concepts into mechanical and other related engineering curricula, we could produce, when supplemented with hands-on internship experiences, new graduates ready to be immediately productive contributors and primed to mature into a new breed of deep OT security practitioners. Also must remember to leverage community college system, where a large percentage

Institute for Information Infrastructure Protection (I3P)
thei3p@gwu.edu N
http://www.thei3p.orgN

2100 Pennsylvania Avenue NW N
Suite 310 N
Washington, DC 20037N
t N202-994-5829N

44983 Knoll Square N
Suite 147 N
Ashburn, VA 20147N
t N571-553-3761N

of distribution system engineers and operators begin their education.

Thank you again for the opportunity to provide comments on strengthening the U.S. cybersecurity workforce and to inform the assessment and report of the Secretaries of Commerce and Homeland Security to the President. We welcome the chance to provide additional information on any of the topics addressed in this document or under discussion.

Sincerely,

Diana L. Burley

Diana L. Burley, Ph.D. Executive Director
& Chair
Institute for Information Infrastructure Protection The George Washington University

Institute for Information Infrastructure Protection (I3P)
thei3p@gwu.edu
http://www.thei3p.org
2100 Pennsylvania Avenue NW
Suite 310
Washington, DC 20037
t 202-994-5829
44983 Knoll Square
Suite 147
Ashburn, VA 20147
t 571-553-3761

Diana L. Burley, Ph.D. Biography

Diana L. Burley, Ph.D. is executive director and chair of the Institute for Information Infrastructure Protection (I3P) and full professor of human & organizational learning at The George Washington University (GW). Prior to joining GW, she managed a multi-million dollar computer science education and research portfolio and led the Cyber Corps program for the US National Science Foundation. Dr. Burley is a globally recognized cybersecurity expert who currently co-chairs the ACM/IEEE-Computer Society Joint Task Force on Cybersecurity Education
to produce the 1st set of global cybersecurity curricular guidelines. In 2013, she served as co-Chair of the US National Research Council Committee on Professionalizing the Nation's Cybersecurity Workforce. Dr. Burley has written more than 75 publications on cybersecurity, information sharing, and IT-enabled change. She has testified before the US Congress, conducted international cybersecurity awareness training on behalf of the US State Department, and served two appointments on the Cyber Security Advisory Committee of the US Commonwealth of Virginia General Assembly Joint Commission on Technology & Science (2012, 2013).

Her honors include: one of SC Magazine's 2017 "Eight Women in IT Security to Watch;" 2016 Woman of Influence-Public Sector/Academia by the Executive Women's Forum in Information Security, Risk Management and Privacy; the 2014 Cybersecurity Educator of the Year; and a 2014 Top Ten Influencer in information security careers. She is the sole recipient of both educator of the year and government leader of the year awards from the Colloquium for Information Systems Security Education and has been honored by the US Federal CIO Council for her work on developing the federal cyber security workforce. Sponsors such as the US National Science Foundation, US National Security Agency, Intel, and IBM have supported Dr. Burley's research; and her board service includes Goodwill Industries International, the AlphaTech Group, and the UK National Cyber Security Centre Cybersecurity Body of Knowledge Project.

She holds a BA in Economics from the Catholic University of America; M.S. in Public Management and Policy, M.S. in Organization Science, and Ph.D. in Organization Science and Information Technology from Carnegie Mellon University where she studied as a Woodrow Wilson Foundation Fellow.

Institute for Information Infrastructure Protection (I3P)
thei3p@gwu.edu
http://www.thei3p.org
2100 Pennsylvania Avenue NW
Suite 310
Washington, DC 20037
t 202-994-5829
44983 Knoll Square
Suite 147
Ashburn, VA 20147
t 571-553-3761

Institute for Information Infrastructure Protection Member Institutions

Institutional Member	Primary Representative	Secondary Representative
Binghamton University	John Bay	Scott Craver
Carnegie Mellon University, H. John Heinz III College of Public Policy and Management	Rahul Telang	Alessandro Acquisti
Carnegie Mellon University, Software Engineering Institute	Greg Shannon	–
Dartmouth College	Denise Anthony	Sean Smith
George Mason University	Massimiliano Albanese	Sushil Jajodia
George Washington University	Diana Burley	Rhea Siers
Georgia Institute of Technology	Seymour Goodman	Mustaque Ahamad
Idaho National Laboratory	Andrew Bochman	Zachary Tudor
Indiana University	Apu Kapadia	Steve Myers
Johns Hopkins University	Richard "Dickie" George	Tony Dahbura
Lawrence Berkeley National Laboratory	Sean Peisert	Deborah Agarwal
MITRE Corporation	Bruce Bakis	Richard Pietravalle
New York University	Nasir Memon	Quanyan Zhu
Oak Ridge National Laboratory	Stacy Prowell	–
Pacific Northwest National Laboratory	Wayne Meitzler	David Manz
Purdue University	Melissa Dark	Mathias Payer
RAND Corporation	Daniel Gonzales	Henry Willis
Sandia National Laboratories	Heidi Ammerlahn	Robert Hutchinson
SRI International	David Balenson	Ulf Lindqvist
University of California, Berkeley	Anthony Joseph	–
University of California, Davis	Matt Bishop	Hao Chen
University of Idaho	James Alves-Foss	Gregory Donohoe
University of Illinois	David Nicol	Zbigniew Kalbarczyk
University of Massachusetts Amherst	Emery Berger	Amir Houmansadr
University of Tulsa	Sujeet Shenoi	Mauricio Papa
University of Virginia	Anh Nguyen	Jack Davidson