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

September 9, 2016

Thomas E. Donilon, Chair
Sam Palmisano, Vice Chair
Commission on Enhancing National Cybersecurity
c/o National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: NIST Docket 160725650-6650-01: Information on Current and Future States of Cybersecurity in the Digital Economy

Chair Donilon, Vice Chair Palmisano, and Commissioners:

Thank you for the opportunity to support the work of the Commission on Enhancing National Cybersecurity as established through EO 13718, by providing comments about the current and future states of cybersecurity in the digital economy. This document includes comments on the topics of: the science of cybersecurity; protecting critical industrial infrastructures from cyber attack; and cybersecurity education and workforce development.

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 I3P representatives from The George Washington University, Johns Hopkins University Applied Physics Laboratory, Idaho National Laboratory, Pacific Northwest National Laboratory, and the University of California, Davis. The views do not necessarily represent the views of the full membership or their institutions.

---

[1] Institute for Information Infrastructure Protection, http://www.thei3p.org
[2] Science of Security, http://cps-vo.org/group/SoS

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

Comments on Specific Topics

Topic: The Science of Cyber Security

Despite general agreement that cybersecurity is more than "just" an engineering problem, the dominant paradigm in cybersecurity research and practice still treats the security of cyber space as an engineering discipline – with few principles, laws or well-defined dynamics that a scientific discipline would more readily provide. Rather than continuing with the current trial and error approach in which defenders deploy technologies with limited assurance of performance outcomes, greater attention to the development of the science of cyber security would provide a more systematic approach. The science of cybersecurity includes provable theories, objective measures, mechanics, axioms and laws related to cyber-social phenomenon, and predictive algorithms.

In the next 1-2 years, we recommend that researchers and research funders focus on expanding the development of the science of cybersecurity. While some portions of the national conversation do address the science of cybersecurity (see, for example, the Science of Security[2] virtual community organized by the National Security Agency), critical research funding needed to advance the scientific discipline is not increasing rapidly enough. If we consider the assertion that all of research and development relies on the integrity of computing and networked resources, it is reasonable to argue that national investments in supporting the computing infrastructure should resemble National Institutes of Health-style large-scale data collections, spanning many different populations. Large-scale scientific test beds on the order of Department of Energy (DOE) national accelerator laboratories would significantly advance our ability to study the complex, emergent and ever-changing nature of critical cyber-physical systems. Two examples of such DOE facilities, which perform pioneering research exploring questions of major scientific and technological interest to society, include SLAC National Accelerator Laboratory[3] and Fermilab[4].

Topic: Better Protecting 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

[2] Science of Security, http://cps-vo.org/group/SoS
[3] SLAC National Accelerator Laboratory, https://www6.slac.stanford.edu/
[4] Fermilab, http://www.fnal.gov/

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

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.

To address these challenges, we recommend the following:

Regarding the 1st challenge: Rather than continuing with a broad perspective, we suggest that NIST narrow its focus, at least partly, to allow greater emphasis on improving security in the most critical sectors, and especially energy.

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 Gov (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 (see below in this document) can expedite these workforce development priorities.

In addition, we offer the following comments on the "Supplemental Information" within this topic.

"The Internet is used every day … to make purchases, store sensitive data, and provide critical information services. These services and infrastructure have come under attack in recent years in the form of identity and intellectual property theft, deliberate and unintentional service disruption, and stolen data."

Comment 1: While the harms described merit attention, perhaps more significant and certainly with potential to cause much greater damages and economic disruptions, are cyber attacks targeting critical industrial infrastructures and in particular, the electric sector.

"Steps must be taken to enhance existing efforts to increase the protection and resilience of the digital ecosystem…."

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

Comment 2: "Enhancing existing efforts", or in other words, doing more of what we are currently doing, is clearly not going to produce the desired results. The attackers are and will remain much more nimble in their adaptations to defenders' slowly evolving "best practices." This is an unsustainable situation and only significantly divergent approaches stand a chance at turning the tables in our favor. See our discussion regarding the development of the science of cybersecurity and the reference to DOE accelerator laboratories as a possible path forward.

Topic: Education and Workforce Development

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 offer 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 often in the context of adversaries.[5]"

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. One such initiative is the ACM Joint Task Force of Cybersecurity Education[6]. This task force was launched in September 2015 to develop comprehensive curricular guidance in cybersecurity education that will support future program development and associated educational efforts. The JTF is a collaboration between major international computing societies: Association for Computing Machinery, IEEE Computer Society, Association for Information Systems Special Interest Group on Security, and International Federation for Information Processing Technical Committee on Information Security Education. The task force grew from the foundational efforts of the Cyber Education Project (CEP)[7]. The

[5] ACM Joint Task Force on Cybersecurity Education, http://www.csec2017.org/
[6] Ibid
[7] Cyber Education Project, http://www.cybereducationproject.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

curricular volume is scheduled for publication in December 2017. Updates on the work of the task force are available through the website.

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 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.

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

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
- 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 of distribution system engineers and operators begin their education

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

Finally, we suggest that the national conversation move away from "awareness" to "engagement" where engagement is a cyber-aware citizenry who understand the implications of what they know, appreciate the impact of their behavior, and accept the relationship between the two.

Thank you again for the opportunity to provide comments on the current and future states of cybersecurity in the digital economy. We look forward to the final report of this Commission and 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

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

Institute for Information Infrastructure Protection Member Institutions

- Binghamton University
- Carnegie Mellon University, H. John Heinz III College of Public Policy and Management
- Carnegie Mellon University, Software Engineering Institute
- Dartmouth College
- George Mason University
- George Washington University
- Georgia Institute of Technology
- Idaho National Laboratory
- Indiana University
- Johns Hopkins University
- Lawrence Berkeley National Laboratory
- MITRE Corporation
- New York University
- Oak Ridge National Laboratory
- Pacific Northwest National Laboratory
- Purdue University
- RAND Corporation
- Sandia National Laboratories
- SRI International
- University of California, Berkeley
- University of California, Davis
- University of Idaho
- University of Illinois
- University of Massachusetts, Amherst
- University of Tulsa
- University of Virginia