GEORGETOWN UNIVERSITY
School of Continuing Studies

MEMORANDUM

August 2, 2017

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

FR: Georgetown University
School of Continuing Studies

Otter, Kelly
Dean, School of Continuing Studies

CC: Smith, Jason
Executive Director, Enrollment Management

RE: Request for Information (RFI)
Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development
Document Citation: 82 FR 32172
Agency/Docket Number: Docket Number 170627596-7596-01
Document Number: 2017-14553

General Information

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)? Note: Providing detailed information, including your specific affiliation is optional and will be made publicly available. Commenters should not include information they do not wish to be posted (e.g., personal or confidential business information) and are strongly encouraged not to include Personally Identifiable Information in their submissions.

Faculty from Georgetown University's School of Continuing Studies, who work in the fields of Cybersecurity, Intelligence, Technology Management and Systems Engineering, and Staff, responsible for data stewardship, responded to this RFI.

- *Frederic Lemieux, Ph.D. – Faculty Director and Professor of the Practice for the Applied Intelligence Program*
- *Maria Trujillo, Ph.D. – Associate Professor of the Practice and Faculty Director of the Technology Management and Systems Engineering Programs*
- *Adam Firestone, Lecturer, School of Continuing Studies, Master of Professional Studies in Systems Engineering Management, Editor In Chief at United States Cybersecurity Magazine*
- *Jean Stanford – Lecturer, School of Continuing Studies, Master of Professional Studies in Technology Management and Certificate in Cybersecurity Strategy*
- *Jeremy Stanton – Chief Digital Officer and Data Steward, School of Continuing Studies*

Growing and Sustaining the Nation's Cybersecurity Workforce

1. What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

There is not very useful data for summarizing available cybersecurity education, training, or workforce developments, as information about programs is scattered, and terms are used broadly, making it difficult to discern the knowledge, skills and abilities that are conveyed in a given program.

However, there are varieties of certifications and credentials that individuals can seek to validate their knowledge and skill-set in a specific area, especially relating to technical skills and competencies. This is a useful mechanism for employers to evaluate individual's skill-sets. Examples include the Certified Information Systems Security Professional (CISSP) and the Certified Information Security Management (CISM) certifications.

Furthermore, the NSA and DHS have collaborated to create Centers of Academic Excellence in Cybersecurity. Accredited institutions may apply to have their program(s) certified if the program's curriculum aligns with the specific cybersecurity-related knowledge units (KUs) that NSA and DHS have developed to guide the development of cybersecurity education. There are two separate programs under the umbrella of the Centers of Academic Excellence in Cybersecurity:

- *National Centers of Academic Excellence in Cyber Defense (CAE-CD) program: The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise for the Nation.*

- *National Centers of Academic Excellence (CAE) in Cyber Operations program: This program supports the President's "National Initiative for Cybersecurity Education (NICE): Building a Digital Nation" and furthers the goal to broaden the pool of skilled workers capable of supporting a cyber-secure nation.*

By maintaining a current list of certified programs, the Centers of Academic Excellence in Cybersecurity should provide a repository of appropriately vetted programs.

One significant challenge related to sharing information about cybersecurity education is the outdated Classification of Instructional Programs (CIP) codes that exist in the cybersecurity space. These codes are developed by the National Center for Education Statistics (NCES) and are used for a variety of reporting and classification purposes, including being able to track degree conferrals. Currently, cybersecurity programs are clustered into a couple of ill-fitting categories because nuanced CIP codes do not exist within this discipline. This means that it is impossible to accurately report the number of degrees that are being conferred in cybersecurity operations versus cybersecurity governance/policy, etc.

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

No. The faculty of the School of Continuing Studies (SCS) believes that a fundamental misunderstanding of the nature of the cybersecurity workforce challenge has led to a proliferation of educational programs focusing on traditional information assurance (IA) skills. Additionally, empirical data suggests that the return on investment (with respect to actual risk mitigation and security improvements) associated with these programs is significantly lower than desired.

At the School of Continuing Studies, we believe that many of the cybersecurity educational programs offered by institutions of higher education focus solely on technical skills and knowledge. The need for such experience is real but often overshadow non-technical skills required by employers. We believe that cybersecurity is a field characterized by multilayered

challenges requiring cross-disciplinary formation instead of a discipline-centric approach. This misunderstanding and oversimplification of cybersecurity issues through technology solutions created a substantial gap in workforce skills such as analytical and strategic thinking, communication, risk management, leadership and ethics, etc.

The misunderstanding stems from a definition of the cybersecurity workforce that is so egregiously limited in scope as to mischaracterize the nature of the workforce to traditional information security roles. These roles comprise only a small portion of the overall cybersecurity workforce, which as a whole, includes roles that require the use of information technology in a variety of ways. Data breach research indicates that most successful cyber-attacks exploit a lack of knowledge or skills on the part of the general workforce, and not the specialized security workers.

As a result, SCS believes that there are four discrete workforce categories when it comes to cybersecurity:

- *Security workers: Information security, information assurance, security engineers, etc.;*
- *Enterprise leadership: Those responsible for managing enterprise risk policies, programs, and ensuring organizational compliance;*
- *Enterprise human resources: Those responsible for employee standards and training; and,*
- *Employees: The rest of the enterprise workforce.*

It is SCS's contention that while security workers are both adequately trained and not generally the targets of malicious internet activity; they are the focus of almost all "cybersecurity workforce" efforts. Leadership, human resources and general employees, who are most often the target, are not well supported by education and training options. In sum, it is our recommendation that education and training should target the non-technical workforce and provide employees with the training options they are lacking.

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

Yes. Georgetown University maintains an Information Security Policy that defines and describes the responsibilities and required practices for all members of the University community with respect to information security and the protection of University information (more information on the policy is available at this link: https://security.georgetown.edu/technology-policies/executive-summary). The University has a Chief Information Security Officer (CISO), an Information Security Office (UISO), and maintains compliance with FERPA, HIPAA, PCI, and numerous other information security and handling standards. The University has defined a Data Classification structure and Data Stewardship architecture, which establishes a community of Data Stewards that have stewardship over particular types of data within their respective management units. The Data Steward for the School of Continuing Studies has implemented a data-security training program, which, in conjunction with training provided by UISO, is mandatory for all staff to complete as part of their on boarding into the organization.

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 and financial sectors)?

It is important to distinguish between what employers need and what they value. Many enterprises have invested in extensive cybersecurity operations, including threat intelligence analysis, information assurance and security operations centers to achieve only marginal improvements in information security. Consequently, employers' expectations, realistic or not, are not being met. These expectations result from a perceived correlation between investment in security tooling, personnel, and reduced levels of risk.

Unfortunately, this correlation is a chimera, and the areas that will result in a security return on investment (ROI) remain underfunded and misaligned with the knowledge and skills of the general workforce and student pipelines. As noted above, it is not the security workers who require significant improvement in their cybersecurity skills and training, it is enterprise business leadership, human resources and the general employee pool. The general cybersecurity ignorance of these groups is what attackers exploit. If the malicious activity value chain is disrupted, the root cause, the likelihood of return on investment in malicious activity must be minimized. This requires a combination of technical capabilities and workforce education solutions that, when applied to the workforce as a whole reduce or eliminate workforce cybersecurity ignorance.

In a recent focus group of cybersecurity subject matter experts held at the School of Continuing Studies, participants agreed that education and training should focus on policy, strategy, and design and not on operational and technical cybersecurity skills. Some of the knowledge, skills and abilities that surfaced during this focus group included:

1. *Data translation, analysis, and correlating patterns*
2. *Designing resilient, security-based systems*
3. *Strategic thinking and the ability to "bring it all together"*
4. *Business acumen and supporting core operations*
5. *Adaptive learning and critical thinking abilities*
6. *Data science in a cyber-context*
7. *Global awareness of privacy laws*
8. *Eagerness to solve different problems*
9. *Creative thought processes*
10. *Cased-based skills and experience*

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?

Most American cybersecurity workforce education programs focus exclusively on security workers. While there is no doubt that the country could use more trained security workers, as noted earlier, security workers are neither the cause of nor a routinely targeted demographic in the cybersecurity challenges facing the United States.

Consequently, most cybersecurity education, training, and workforce development programs conducted in the United States today are ineffective with respect to addressing macro-information security issues.

The SCS vision for effective cybersecurity education, training and workforce development centers on the three workforce groups that can have meaningful impact on cybersecurity. These are:

- *Enterprise leadership, who must be trained in organizational risk assessment, establishing security accountability policies and the root causes of enterprise vulnerability;*
- *Enterprise human resources, who must be trained in the implementation of security policies and training as well as how to train the non-security worker components of the enterprise in cybersecurity essentials; and*
- *Employees, who must be trained in cybersecurity essentials.*

The non-credit Cybersecurity Strategy Certificate Program offered by SCS is one of the most effective cybersecurity education programs in the U.S. because of its rigorous curriculum and faculty of academics and industry experts. The Program approaches the practice of cybersecurity through a managerial lens and uses applied learning experiences to place students in the role of the Chief Information Security Officer (CISO) throughout the program.

The goal of the program is to cultivate the skills needed to design and implement a comprehensive information security strategy, from prevention to crisis management. The program is successful in reaching this goal because it requires the successful completion of six courses, for a total of 10.8 Continuing Education Units (CEUs) or 108 contact hours. The courses in the certificate include:

- *Making the Business Case for Cybersecurity*
- *Threats, Vulnerabilities and Social Engineering in Cybersecurity*
- *Leadership and Strategy in Cybersecurity*
- *Technical Countermeasures and Risk Assessment*
- *Managing Security*
- *Applied Cybersecurity and Crisis Management*

Upon successful completion of the six required courses, students are able to:

- *Support the business case for a cybersecurity strategy*
- *Summarize national and global cybersecurity issues*
- *Compose a comprehensive cybersecurity strategy*
- *Calculate information security risks*
- *Express related legal, regulatory, and compliance frameworks*
- *Develop a crisis management plan*

The Certificate is currently offered on campus at the School of Continuing Studies in Washington, DC. However, to meet growing global demand for these skills, the Certificate will also be offered online beginning in fall 2017. This Certificate Program can also be delivered as a custom education program and tailored to the specific training and educational needs of a government agency or any industry organization.
Furthermore, SCS is building upon its successful and evolving professional graduate programs in Technology Management and Applied Intelligence, and is actively engaging in discussions on

how to better train and educate our students through master's degree programs in the field of Cybersecurity.

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

Through extensive market research, professional experience, and their own research and engagement in the discipline, SCS faculty consider the following items to be the nation's greatest challenges for cybersecurity education, training and workforce development:

- *Lack of awareness around cybersecurity considerations and issues outside of information security functions or roles; need to build awareness of cybersecurity considerations so that organizations can make informed decisions at all levels of employment: C-Suite, Human Resources, technical team and non-technical employees;*
- *Lack of training for end-users on social engineering avoidance, etc. Need to develop simple messages that are repeated often in order to increase cybersecurity awareness across the workforce;*
- *Current failure to train business analysts who can analyze the enterprise architecture and communicate with the entire enterprise (including the CISO team and the technologists) about the types of risks it is facing and how they can be managed within the budget;*
- *Lack of education and training programs that are competency-based and aligned with cybersecurity frameworks (identify, protect, protect, respond, and recover). There are currently too many education and training programs that are not preparing students with competencies that are needed by employees and in demand in cybersecurity (problem-solving, strategic thinking, communication, leadership, etc.) Many of the current education and training programs focus solely on technical skills or theoretical knowledge;*
- *Lack of faculty in cybersecurity education programs who have real-world experience and can transfer applied knowledge to cybersecurity students;*

- *Lack of cross-disciplinary formation in cybersecurity field and lack of coordination among university departments, such as, Law, Computer Science, Organizational Science, Criminology and Management;*
- *Lack of responsiveness from traditional academia to develop educational programs that respond to the emerging needs of the workforce;*
- *Lack of stable partnerships between employers and institutions of higher education (practicum, internships, applied research, etc.);*
- *Lack of problem-solving and analytical thinking skills integrated into currently-available specialized training courses, certifications, and degree programs;*
- *Failure of current education programs to teach skills and knowledge that are current and future-facing (many existing programs teach content that is obsolete by the time students receive their degree);*
- *Lack of scholarship programs or other funding mechanisms to support training and formation of the cybersecurity workforce;*
- *Lack of race and gender diversity in the cybersecurity workforce;*
- *Failure to recognize that enterprise cybersecurity challenges exist largely outside of the traditional security workforce, and the resulting misallocation of resources;*
- *Failure to provide degree- and certificate-producing educational frameworks geared towards the cybersecurity requirements of the non-security workforce;*
- *Failure to establish meaningful standards and accountability for cybersecurity-related actions and activities.*

Any of these challenges can transition into opportunities given the right education and training that focuses on competency-based education that align with cybersecurity frameworks and an organization's cyber priorities.

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)?

There is a general trend that shows a convergence between technological innovations and security considerations. This trend is expected to increase in scale and velocity at an exponential rate. The eventual outcome will be the elimination of "security" as a separate discipline and/or technology stream - not because security is not important, but because it is so important that it will become integral to everything. The Internet of Things (IoT) is an example of this trend.

The result will be the obsolescence of current educational and training paradigms (and technologies) that emphasize security as a distinct silo. Security technology will become transparent to users. The nature of threats and the targeted demographics will remain the same.

Protection of emergent CPS, as noted above, will require training that prepares key-targeted demographics (enterprise leadership, human resources and the general workforce) to successfully navigate a hostile cyberspace.

8. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:

i. At the Federal level?

ii. At the state or local level, including school systems?

iii. By the private sector, including employers?

iv. By education and training providers?

v. By technology providers?

In order to achieve effective cybersecurity, the nature of the cybersecurity workforce must be understood holistically. Until and unless it is realized at all levels that the cybersecurity workforce

is the ENTIRE workforce, breaches and malicious activity will remain commonplace, and technical advances will yield only marginal returns.

At the Federal level, educational standards for cybersecurity and computer science, beginning at the elementary level and progressing through the postsecondary level, must be developed, promulgated and funded. Continuing research on cyber teaching effectiveness is critical. The federal authorities should be working with all stakeholders to improve cyber resilience.

States and local authorities must implement security and computer science education at all levels, but in a meaningful way. For example, while the Virginia Standards of Learning now require that computer science be taught and tested at the third grade level or earlier, there is no state funding or requirements definition for the curriculum at this time.

The private sector, including employers, must demand security and computer literacy (and enforce standards for these) from all employees. It is assumed that workers will come to a position with an inherent knowledge of productivity applications such as Microsoft Word. It should also be assumed that the employee would come to a position knowing what a phishing attack looks like.

Education and training providers must develop an understanding of the broad applicability of cybersecurity to the general workforce and develop programs that apply generally.

Technology providers must continue the technical and procedural de-siloization of cybersecurity and its incorporation into the general technology stream.