DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
[Docket Number 170627596-7596-01]

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development

With this submission, University of Maryland University College (UMUC) responds to the National Institute of Standards and Technology Request for Information (RFI) on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development [Docket Number 170627596-7596-01]. Our observations and recommendations are informed by 1) our academic alliance with the Office of Personnel Management (OPM)[1] through which we serve Federal Government agencies, 2) our academic alliances with Federal contractors, and 3) as an engaged participant and leader in cybersecurity workforce development initiatives.

Founded in 1947, University of Maryland University College (UMUC) is one of 12 accredited, degree-granting institutions in the University System of Maryland (USM). It currently has over 89,000 students worldwide. The university offers cybersecurity courses through classroom-based and online programs using a variety of scheduling options and delivery formats Since 2010, UMUC has produced more than 8,000 cybersecurity graduates, and 10,000 undergraduate and graduate students are currently enrolled. It has been a major part of the DoD VOLED program since its inception, and a large number of its cybersecurity graduates are either active-duty military or veterans.

UMUC is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools and holds several honors for online education. UMUC's mission is to educate adult, part-time students. UMUC has been designated as a National Center of Academic Excellence in Information Assurance and Cyber Defense Education by the National Security Agency and the Department of Homeland Security and as a National Center of Digital Forensics Academic Excellence by the Defense Cyber Crime Center Academic Cyber Curriculum Alliance.

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 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)?

UMUC has developed and maintains a suite of cybersecurity degree and certificate programs addressing public and private sector cyber workforce development needs that align to industry standards and Federal education frameworks.[2] UMUC's cybersecurity curriculum is designed to produce high-caliber cybersecurity professionals with an applied, multi-disciplinary, and integrative approach to securing the cyberspace, using current tools and learning techniques.

[1] https://www.opm.gov/WIKI/training/Federal-Governmentwide-Academic-Alliances.ashx
[2] http://www.umuc.edu/cyber

Bachelor Degrees
Computer Networks and Cybersecurity
Cybersecurity Management and Policy
Software Development and Security

Master's Degrees
Cloud Computing Architecture
Cybersecurity Management and Policy
Cybersecurity Technology
Digital Forensics and Cyber Investigation
Information Technology: Information Assurance

Undergraduate Certificate
Computer Networking

Graduate Certificates
Cybersecurity Management and Policy
Cybersecurity Technology
Information Assurance

Credential Stacking

In addition to offering degrees and certificates, it is important to note that UMUC has designed a number of its courses so that they not only contribute to degree progress but also prepare students to sit for industry certification exams. This encourages credential stacking to enhance employment outcomes. These courses are identified below.

	Certification	UMUC Course (credits)
CompTIA	A+	Fundamentals of Computer Troubleshooting (3)
	Network+	Fundamentals of Networking (3)
	Security+	Network Security (3)
	LPIC1 and CompTIA Linux+	Linux System Administration (3)
Microsoft	Exam Number 70-410	Installing and Configuring Windows Server (3)
	Exam Number 70-411	Administering Windows Server ((3)
	Exam Number 70-412	Configuring Advanced Windows Server Services (3)
	Exam Number 70-413	Designing and Implementing a Server Infrastructure (3)
	Exam Number 70-414	Implementing an Advanced Server Infrastructure (3)
	Exam Number 70-417	Installing and Configuring Windows Service (3) Administering Windows Server (3) Configuring Advanced Windows Server Services (3)
International Information Systems Security Certification Consortium	Certified Information Systems Security Professional (CISSP)	Advanced Information Systems Security (3)
EC-Council Certification	Certified Ethical Hacker (CEH)	Ethical Hacking (3)

International Society of Forensic Computer Examiners (ISFCE) Certification	Certified Computer Examiner	Digital Forensics Analysis and Application (3)
CERT Certification	Computer Security Incident Handler (CSIH)	Network Forensics (3)
Global Information Assurance Certification (GIAC)	GIAC Certified Incident Handler (GCIH)	Network Forensics (3)
	GIAC Reverse Engineering Malware (GREM)	Malware Analysis (3)
Mobile Forensics Certification	AccessData Mobile Examiner (AME)	Mobile Forensics (3)

Partnerships and Alliances

As part of its workforce development activity, UMUC partners with over 60 organizations to provide their employees with quality education that enhances development, closes skills gaps, and drives employee engagement and retention. Because of the strength, breadth, and accessibility of our programs, public and private sector employers look to UMUC to provide courses, certificates, and degrees that will enhance the cyber skills of their workforce.

Specifically, one of UMUC's Federal contractor alliances in cybersecurity education has graduated almost 300 individuals in a cybersecurity certificate program over the last six years. The National Security Agency is enrolling employees in UMUC online courses focused on Certified Ethical Hacker, Security+, and Network+ certifications content, and using the certification exam, or an exam closely modeled on it, as the final assessment. This solution addressed their challenge of increasing certifications among their workforce, which is distributed across the country, by resolving logistical issues such as scheduling face-to-face classes in different locations with a variety of vendors, getting enough students to register in a particular location to justify holding the face-to-face class, and improving outcomes on certification exams. UMUC also provides credit toward a degree for those individuals interested in completing a bachelor's degree.

Growing and Sustaining the Nation's Cybersecurity Workforce

Question 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 a lack of national data about the progress the nation's postsecondary level is making in closing the skills gap. This could be an opportunity for NICE to work with the US Department of Education and the NSA/DHS CAE program. NCES' data do capture graduates by school, major, and academic year, but NCES data aggregate fields in a way that precludes accurate measurement. For example, UMUC's cyber graduates are reported under "cyber/forensics/counterterrorism". A clear identification of programs as "cyber" under the NCMF and aggregating their graduates on a given frequency is a tall order. But perhaps it could start with reporting of graduates of CAE-certified programs as part of the NCES dataset.

As a measure of workforce developments, *Cyberseek* is an excellent tool for all the reasons we know. It offers fairly current market data aligned to the NCMF and provides these data on a granular basis both as to the location of positions and their requirements. We do not think this tool is well known among computer science and cybersecurity faculty and career counselors or workforce development specialists at regional economic development entities or state departments of commerce.

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

Within academia, there is a developing consensus or convergence of understanding and agreement in these areas that has certainly been facilitated by the NCMF but also by efforts like the Joint Task Force on cybersecurity education. (see *Cybersecurity Curriculum 2017* [Version .75 Report 12 June 2017] at https://docs.wixstatic.com/ugd/895bd2_e3443415db4c432da8a66b59d076e151.pdf).

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

UMUC views its institutional cybersecurity as a ‘whole of organization’ responsibility. The university’s IT Risk and Compliance team conducts regular training towards this end through its security awareness training program, a compliance program, and other IT policies governing faculty, staff, and students.

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)?

According to our Office of Career Services, employers value a wide variety of technical expertise and look to industry certifications as evidence of that expertise. The most sought after certifications by employers of UMUC students are Security+ and Network+ for aspiring network engineers, Licensed Penetration Testers for aspiring pen testers, Certified Ethical Hacker for general cyber professionals, and CISSP for aspiring IT and cyber managers. These employers also value oral and written communication skills and experience, depending on the position. Government contractors value security clearances and degrees because of requirements associated with government contracts.

Employers are aware of the challenges they face in recruiting. In UMUC’s interactions with contractors, they have indicated that they would like the leeway to recruit from a broader pool with fewer years of experience and without security clearances. Many would be willing to sponsor clearances, but because of the lengthy process, most want to only hire those with existing clearances, and this can be extremely challenging. A college degree prepares one to communicate effectively and to be technically proficient. Requiring industry certifications is not necessarily always realistic because it is a great financial burden on those who have yet to become employed in their new field. The number of years of experience required can also be unrealistic and may not consider transferable experience from another field. The industry itself is young and many technologies have not existed for as many years as the number of years’ experience sometimes requires. Last year at CyberMaryland, during one of the panel discussions, panelists spoke of “purple unicorns” and how employers, particularly HR folks, build job requirements that are unrealistic and impossible to fill. (One example was asking for 10 years' experience in a particular tool or technology that has not existed that long.)

The hardest-to-fill cybersecurity jobs call for financial skills, such as Accounting or knowledge of regulations associated with the Sarbanes-Oxley Act, alongside traditional networking and IT security skills. Because finance and IT skills are rarely trained for together, there is a skills gap for workers who try to meet the requirements of the "hybrid jobs." Expectations that the cyber workforce will be prepared from a technical and soft-skill standpoint is in line with the workforce and student pipeline, but the requirements for certifications on top of college degrees, and years of experience are not in alignment. There seems to be a disproportionate number of mid-level and senior positions and too few entry-level positions and internships.

Other industries are not as stringent in requiring industry certifications and security clearances as government contractors are. These other industries, such as healthcare, sometimes struggle with competing for talent because their pay ranges are lower than contractors' pay ranges.

UMUC provides the technical skills, soft skills, and preparation for many certification exams through our courses, certificates, and degree programs. Our pipeline of students is prepared to enter the workforce and eager to contribute but applicants are finding a dearth of entry level and on-the-job internship or apprenticeship development opportunities.

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?

UMUC would classify itself as an effective/scalable cybersecurity education program. It is both a CAE school, and its cyber forensics program is certified through DC3. The school offers degree options that prepare students to sit for industry certification exams. Its faculty are largely practitioners close to the day-to-day challenges in cybersecurity, and its programs have a practical or on-the-job orientation. One outcome measure is the success of the UMUC student cyber team, which each year wins top placement in major cyber competitions. The university's programs are offered online as well as face-to-face. The online modality and use of adjunct faculty permits the university to scale its cyber programs. As mentioned, UMUC currently has 10,000 students enrolled in such programs.

Looking outward, there have been a number of studies that have asked the question about "best schools" in cyber. While there are methodological criticisms that can be made of them, their findings tend to converge. For example. a 2014 Ponemon report was based on interviews with about 2,000 practicing IT professionals in industry and government representing only 4% of the original sample set. (http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf). That study identified the following factors that correlated with the highest quartile These resonate with the larger literature and certainly our own sense of what constitutes an effective cyber program:

- Interdisciplinary program that cuts across different, but related fields – especially computer science, engineering and management.
- Designated by the NSA and DHS as a center of academic excellence in information assurance education.

- Curriculum addresses both technical and theoretical issues in cybersecurity.
- Both undergraduate and graduate degree programs are offered.
- A diverse student body, offering educational opportunities to women and members of the military. Faculty composed of leading practitioners and researchers in the field of cybersecurity and information assurance.
- Hands-on learning environment where students and faculty work together on projects that address real life cybersecurity threats.
- Emphasis on career and professional advancement.
- Courses on management, information security policy and other related topics essential to the effective governance of secure information systems.
- Graduates of programs are placed in private and public sector positions.

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

There are no surprises here.

- Without question, building the pipeline in computer science and cybersecurity in K-12 is a major challenge. The recent publication of the curricular guidelines by the CSTA is a large step forward as have been the efforts to stimulate interest by organizations such as by LifeJourney and code.org. But schools face the very difficult problems of qualified teachers and the budget support for the infrastructure to enable such programs. This is true even in top tier public school systems, such as those in Maryland.

- Anticipating what the jobs will be in a rapidly changing environment and therefore what curricula should be preparing students for represents another challenge. AI is the most often mentioned wildcard that will certainly transform cybersecurity, the jobs that require people and how people will work in tandem with AI.

Question 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)?

As noted above, AI, the deployment of sensors everywhere, and big data are likely to eliminate many lower level and even mid-level jobs in cyber and other industries like finance. But these developments will also change the character of jobs that remain. Increasingly, technology observers are talking about the human/AI interface as the new workforce model in cyber and many industries. This will change how we educate and prepare workers. In cyber, AI will require an understanding of AI itself and its limitations (the risks it brings with it), the human/AI interplay, and how to incorporate AI into cyber operations and to manage it. The cyber operators of the future will still be required to understand networks, threats, and best security practices, but their involvement with systems will likely become less direct and operate more through AI itself. The cyber workforce of the future—that would make a substantial NICE webinar series and even a great topic for a one-day NICE convening.

Question 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?

Here are four recommendations:

1) Provide Federal funding for middle and high schools to support participation in cyber camps and cyber competitions.
2) Expand the scope of the Scholarship for Service program to include part-time students.
3) Provide Federal funding for apprenticeship programs to bring down the cost of these to industry, realizing that apprenticeship programs are a pathway for underrepresented populations into cybersecurity fields and can serve as a vehicle for starting security clearances for promising talent.
4) Create a "national university cyber range" that, like an FFRDC, would be funded in part by the Federal Government and operated by a firm or consortium of firms with the capacity to offer current real world red team/blue team operator scenarios at various skill levels for schools around the nation. This range could be offered on a subscription basis to high schools, colleges, and universities and could serve as a driver for the adoption of good curricular models.