RESPONSE to NIST Request for Information (RFI)
Federal Register Document 2017-14553
Regarding National Cybersecurity Workforce Education and Development

RFI Response By:
Alan B. Watkins
Owner/Consultant, ABW Consulting Services
Core Adjunct Professor, National University, School of Engineering & Computing

RFI Dates
Comments must be received by 5 p.m. Eastern time on August 2, 2017.

RFI Addresses
Online submissions in electronic form may be sent to cybersecurityworkforce@nist.gov. Please include the subject heading of ''Cybersecurity Workforce RFI''. Attachments to electronic comments will be accepted in Microsoft Word or Excel, or Adobe PDF formats only. Written comments may be submitted by mail to Cybersecurity Workforce RFI, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899. Comments containing references, studies, research, and other empirical data that are not widely published should include copies or electronic links of the referenced materials. All submissions, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. Sensitive personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Submissions will not be edited to remove any identifying or contact information. Do not submit confidential business information, or otherwise sensitive or protected information. Please do not submit additional materials. All comments received in response to this RFI will be made available at https://nist.gov/nice/cybersecurityworkforce without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information). Comments that contain profanity, vulgarity, threats, or other inappropriate language will not be posted or considered.

RFI Supplementary Information
The Commerce Department's National Institute of Standards and Technology is soliciting comments from the public that will aid the Department of Commerce (DOC) and the Department of Homeland Security (DHS) in preparing the assessment and report to the President. For the purposes of this RFI, ''education and training'' of the American cybersecurity workforce does not include general workforce cybersecurity awareness efforts. Rather, ''education and training'' refers to curriculum- or practicum-based programs to increase the effectiveness of the workforce addressing cybersecurity challenges.

RFI Background Information
Given the nature and importance of the Executive Order, NIST requests information from the public about current, planned, or recommended education and training programs aimed at strengthening the U.S. cybersecurity workforce.

Respondents are encouraged – but are not required – to respond to each question and to present their answers after each question. The following questions cover the major areas about which NIST seeks comment. They are not intended to limit the topics that may be addressed. Respondents may address related topics and may organize their submissions in response to this RFI in any manner. Responses may include estimates; please indicate where the response is an estimate.

All responses that comply with the requirements listed in the DATES and ADDRESSES sections of this RFI will be considered.

Comments containing references, studies, research, and other empirical data that are not widely published should include copies or electronic links of the referenced materials. Do not include in comments or

otherwise submit proprietary or confidential information, as all comments received in response to this RFI will be made available publicly at https://nist.gov/nice/cybersecurityworkforce. Comments that contain profanity, vulgarity, threats, or other inappropriate language will not be posted or considered.

General Information

Question A. 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.

Response (A):

Yes, I have been involved with cybersecurity since 1998, and specifically with education and training since 2010. There are four primary areas of my experience related to the subject of this RFI.

[1] I am a Core Adjunct Professor in the Master's Degree in Cyber Security and Information Assurance (MS-CSIA) program at National University, teaching courses for 5 years and have rewritten updated curricula for two of the courses in the last 18 months. In addition, I am now also teaching in the new Bachelor's Degree CSIA program, which started in Spring 2017, and over the last 12 months, I wrote the original curricula for two of the new BS-CSIA courses.

[2] I am an active member and former IT Sector co-Chief with the InfraGard San Diego Members Alliance. I am participating with the InfraGard Houston Members Alliance on their Cybersecurity Workforce Enhancement Task Force (CWETF). The CWETF goal is creating community-based, regional partnerships between academia, business, workforce development agencies, and economic development agencies to facilitate entry-level training and education of new cybersecurity workers and providing avenues into the workforce pipeline, as well as ongoing training and education for current cybersecurity workers. One of my contributions to this effort, will be a Basic Information Security Training course, consisting of 42 modules in 10 lessons.

[3] In support of a non-profit organization in San Diego, California, I created a training course for them to train veterans in cybersecurity basics to help them transition into a civilian career. The training course, "Implementing Cyber Hygiene for SMBs," provides instruction on how to implement the first five CIS Critical Security Controls tailored for small-medium businesses (SMBs) and small office/home office (SOHO) organizations. I have coordinated this training course with the Center for Internet Security (CIS) and it will be made available for free. I will also be part of the team providing input for version 7 of the Critical Security Controls.

[4] In Fall 2016, I was on a national panel of cybersecurity experts from academia and industry, administered by the National CyberWatch Center (NCC), to map the course content, learning objectives, and practical lab outcomes from five fundamental courses to the NSA Centers of Academic Excellence in Cyber Defense (CAE-CD) Knowledge Units (KUs), the NICE Cybersecurity Workforce Framework (NCWF) Knowledge, Skills, and Abilities (KSAs), and industry job functions. From June 2017 to April 2018, I am the designated Managing Editor for a follow-on, NSA grant-funded project under NCC, to develop competency-based and performance-based curriculum for a foundational cybersecurity course, as well as a model process for rapid course development.

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?

Response (1):

I have not been involved in data collection or metrics to measure the effectiveness of education and training efforts. As far as organizing and sharing information, I am a member of the San Diego InfraGard chapter and I am participating in the Houston InfraGard's Cybersecurity Workforce Enhancement Task Force (CWETF), to help coordinate efforts between the two regions. The CWETF's mission is "to provide a forum for a collaborative effort amongst all cyber-related community entities, security professionals, vendors, businesses, academia and government to discuss best practices, innovative solutions, and practical approaches to communicate and provide venues to improve cyber workforce development, worker skills, job placement, and retention." As its stated purpose, the CWETF "is committed to identifying and sharing best practices, resources, networks, and security education techniques to improve the supply of qualified, skilled cyber workers and minimize risks to organizations and the community, which is fundamental to InfraGard's mission." The goal is to develop the partnerships and processes in Houston, then migrate the program to San Diego, which already has a well-developed cybersecurity community.

The San Diego Cyber Center of Excellence (https://sdccoe.org/) conducted an extensive cyber education and workforce survey and study, providing numerous statistic and measures on the supply and demand for cyber workers. In June 2016, they issued "An Economic Impact Analysis and Workforce Study" on the cybersecurity industry in the San Diego region (link to report: https://sdccoe.org/wp-content/uploads/2015/01/CCOE-EIS-2016-.pdf).

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

Response (2):

I do not believe there is sufficient understanding or agreement – businesses, as well as academic institutions, are confused by the proliferation of cybersecurity job titles and roles with their corresponding KSAs. The 50+ work roles defined in the current version of the NCWF are fairly recent, compared with roles which were previously defined by industry or professional organizations (which are generally not aligned with the NCWF); for example, ISACA (Information Systems Audit and Control Association). However, **if** the NCWF roles and job

functions can be aligned with industry skills requirements (common standards for both public and private sectors) at different proficiency levels (e.g., entry or novice/apprentice level, intermediate or journey level, and advanced or expert level), then those job role definitions could form a basis for national standards, as long as they are also consistent with requirements from the U.S. Office of Equal Employment Opportunity Commission (EEOC) and the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization (ISO) related to guidelines for recruitment and selection processes for cybersecurity professionals.

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?

Response (3):

I am a sole proprietor consultant, so I keep myself educated; however, part of my business is providing clients with information security policies and procedures, including employee education and training. The policy template I created includes requirements for an ongoing training program for three different audiences – (a) IT and Information Security staff, (b) employees (from the CEO down), and (c) non-employees, meaning 3rd party partners, suppliers, and others who might have access into a company's IT systems. To my knowledge, two local government organizations, where I provided the education and training policy, have both successfully implemented their policies. I also share my templates by posting them online for other cybersecurity professionals to use.

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)?

Response (4):

First, and separate from the technical security skills, employers across several industry sectors have expressed the need for their technology staff, including security analysts, to have a solid understanding of business risk management principles. The want to have technology and security issues and solutions expressed in terms of the risks to business operations – either increasing or decreasing those risks. Small business owners have tended not to know what specific technical skills are needed and, therefore, count heavily of standard certifications, such as CISSP, CISM, CISA, SSCP, GSEC, etc. More knowledgeable business owners seek workers who have several years of hands-on security experience, plus one or more certifications, and often combined with an undergraduate degree. The positions being filled by this level of worker appear to be more mid-level and senior-level information security jobs, rather than entry-level positions. There is a fluctuating trend between giving more weight to candidates with certifications or candidates with degrees, which seems to be leaning toward the certifications. Larger organizations that have had active information security operations for many years, probably have realistic requirements and expectations for their own needs, because they have the background experience in managing those operations. Smaller organizations may be confused by the proliferation of job titles and definitions, as well as varying certifications, and likely do not know what requirements are needed to create and fill positions in their company. I do not have enough exposure across multiple industry sectors to be able to comment on differences or similarities between them.

From a workforce/student pipeline point of view, my experience with teaching at National University has resulted in several students who graduated from the Master of Science degree program in Cyber Security & Information Assurance (MS-CSIA), getting promotions, transfers or new jobs in the cybersecurity field as a result of their education. National University has combined lecture with hands-on lab work for almost all of the MS-CSIA courses, so that students leave with actual, usable skills. The MS-CSIA program receives regular input from local and regional businesses on the job skill requirements they are needing, so that course content and labs can be geared toward preparing the students for the local job market.

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?

Response (5):

I am involved with an information sharing effort to coordinate regional cybersecurity education, training, internships, and apprenticeships, as part of the Houston InfraGard Members Alliance, through participation in its Cybersecurity Workforce Enhancement Task Force (CWETF). By taking advantage of the multi-sector InfraGard membership and making contact with local schools (a high school and community college, to start), local or regional businesses, regional workforce development agencies, and the U.S. Small Business Administration (SBA), the CWETF is gathering information on education and training resources, both currently available and some in development, to be a source of information for anyone wanting to get into the cybersecurity field. That is, provide entry level cyber knowledge and skills training to seed the apprenticeship-level workforce, thus helping to seed those 1-2 million cyber workers needed in the next five years. Since this effort is still in its start-up phase, its effectiveness won't be known for another year.

Existing programs of which I am aware, which I believe are effective, include the following:

(a) NICE Challenge Project, managed and hosted by CyberWatch Center West at the University of California in San Bernardino (UCSB); where they provide online cybersecurity "challenges" based on the Knowledge, Skills, and Abilities (KSAs) from the NIST/NICE Cybersecurity Workforce Framework (NCWF). This is an online lab environment for use by colleges or universities, free of charge for students, and it offers detailed instructions for each challenge. Although, this is not a typical set of lab tasks where students are learning step-by-step procedures, these challenges present a goal and several hurdles for students to overcome to solve the challenge by having to decide what steps are necessary and taking proper corrective actions. In addition to using the NCWF as one basis for the challenges, they are also aligned with the NSA's Centers for Academic Exellence (CAE) Knowledge Units.

(b) InfoSec Learning, LLC provides an online lab environment to host a series of learning labs based on the National CyberWatch Center's education and training curricula (five core courses). There is a wide array of beginning-level and intermediate-level labs where students learn the step-by-step procedures to accomplish defined tasks. The labs and the related learning materials are also mapped to the National Cybersecurity Framework functions and categories. While there is a fee for these labs, InfoSec Learning will work with schools to

customize a set of labs to match the course materials being taught. Students can repeat labs as many times as they want, within the course time period, to improve their skills and achieve the highest level of successful completion.

(c) National University, School of Engineering and Computing, has had a Master of Science in Cyber Security and Information Assurance (MS-CSIA) program for about 8 years, and in March 2017, started a new Bachelor of Science program (BS-CSIA). Both programs combine textbook and lectures with hands-on lab assignments to both learn skills being taught in the lectures and to learn how to select the proper security tools to perform assigned tasks, such as vulnerability assessments, network and system discovery scans, configuring firewalls and routers using ACLs, analyzing network traffic (i.e., TCP streams), and performing progressive penetration testing. For the capstone project needed for graduation, teams of students contact and work with local companies to perform security assessments, including vulnerability scans, and make recommendations to the company for security policies and procedures, as well as specific remediation and mitigation steps to resolve found vulnerabilities and other security gaps.

(d) The Joint Task Force on Cybersecurity Education (https://www.csec2017.org/) has been working toward common standards for post-secondary cybersecurity curricula. I contributed comments on the last two draft versions (ver. 0.5 and ver. 0.75). The breadth of participation among the supporting organizations should provide well-rounded guidelines that are focused on workforce requirements. Once they finish the upcoming work to map curricular content to the NCWF roles and KSAs, these standards and guidelines should prove to be a valuable tool for academic institutions wanting to develop new cybersecurity courses. It may prove to be a little more difficult for academic institutions with established cybersecurity programs to make modifications to their courses so they align with these standards and guidelines. One key success factor will be ensuring that courses are designed to be competency-based and directly related to the job functions required in the workforce, so that graduates from post-secondary schools using the standardized curricula, are assured of not simply learning and knowing textbook information, but having usable skills to meet workforce demands.

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

Response (6):

I believe one of the greatest challenges for cybersecurity education in our nation, is getting the appropriate cyber learning materials integrated into K-12 STEM programs – creating a STEM-C initiative. Concurrent with that, another challenge is providing incentives for training entry-level cybersecurity workers who can fill positions and provide necessary security services for small businesses, at a minimal cost, where more skilled and higher-level positions are not always needed, nor will they be affordable. Since SMBs comprise over 90% of all businesses in the U.S. and create half the new jobs annually, the Nation must focus on a win-win-win proposition of helping entry-level cyber worker candidates, SMBs, and the Nation's cybersecurity posture overall.

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)?

Response (7):

To answer the last part of the question first – it will be very important, even critical, for cybersecurity education, training, and workforce development programs to stay ahead of, or at least in line with, new advances in technology. There will be a need for cybersecurity workers to have knowledge of current and developing technologies, to be able to take advantage of their benefits and also to be able to implement security measures. The general principle and goal of protecting the data, no matter where it is located, and IoT manufacturers (in particular) should build-in and activate security measures prior to sale and installation or use of their devices.

New technologies will both help cybersecurity workers and present new challenges and threats for existing technology environments. They will provide benefits through automation and the ability to analyze and correlate millions of pieces of information (such as Indicators of Compromise) to help detect and protect against cyber attacks, as well as self-healing technologies to speed the response and recovery processes. The proliferation of unmanaged IoT devices opened dozens of new threat vectors, in places where traditional security controls are not in place nor intended to be (i.e., smart appliances, wearable medical devices, etc.). To take advantage of the benefits and to combat the new threats, cybersecurity education and training programs need to keep pace with new technologies or even second-guess what will be coming with each "next generation" device or software. Those education and training programs need to incorporate critical thinking and analysis skills and the ability to perform detailed and accurate research on a topic.

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:

At the Federal level?
At the state or local level, including school systems?
By the private sector, including employers?
By education and training providers?
By technology providers?

Response (8):

(a) First, as a Nation, we need to establish a common core of basic cybersecurity job roles with requisite knowledge and skills that are common across public sector and private sector, for any industry. The Joint Task Force on Cybersecurity Education is a step in the right direction. Those standard role definitions and functional requirements must be easily and readily available to anyone – both job seekers and employers. Second, as a Nation, we should have standardized, basic cybersecurity curriculum focused on providing entry-level skills; with a goal of lowering barriers of entry into a cybersecurity career and providing low cost candidates for small businesses.

(b) At the federal level, the FedVTE system/platform should continue to provide, and increase the number of cybersecurity training courses for government employees, and especially for military personnel who are about to transition into a civilian career. There should be a variety of courses available – in breadth to cover several cybersecurity topic areas, and in depth to cover beginning, intermediate, and advanced levels of competency.

All of the courses should be aligned with and mapped to the appropriate functional job requirements and KSAs in the NCWF and other relevant workforce competency and capability models. For those who are trying to get into the field of cybersecurity, there needs to be several foundational (or fundamental) courses including, but not limited to, the following topics: basic computer systems and operating systems, basic networking, network security, concepts of security controls (e.g., CIS 20 Critical Security Controls), overview of cryptography, identity and access management, and risk management.

(c) At the state or local levels, including school systems, there should be acceptance, support, and integration of the national core cybersecurity roles and standardized curricula into government staffing plans and statewide, approved curriculum requirements for secondary and post-secondary institutions. Similarly to the CWETF in Houston, which will be replicated in San Diego, there should be regional partnerships or consortiums of academic, government, industry, workforce development, and economic development organizations, coordinating and collaborating to meet the local needs for educating new cyber workers and training existing workers for advancement and to retain them.

(d) In the private sector (for employers), larger organizations should support regional workforce development efforts through training programs, internships, apprenticeships, and participation in workforce partnerships or consortiums which provide assistance to small businesses for entry-level cyber workers. The practice of "seeding" the cyber workforce pipeline, starting with the entry-level workers to support small/medium businesses (SMBs), should benefit larger organizations by having those workers gain experience, knowledge, and skills at SMBs, which large organizations are seeking in their cyber workers. This benefits the cyber workers in looking at a potential career path, which starts by gaining experience with SMBs and finding mid-level and advanced positions with larger companies.

(e) Education and training providers should provide low cost or subsidized cybersecurity training in support of federal efforts to train military personnel who are transitioning into civilian jobs and veterans who are interested in getting into the cybersecurity field. In addition, they should participate collaboratively in community, regional, and state efforts to provide multiple workforce education and development resources for potential cyber workers, including adoption of a standardized core set of materials for at least entry level skills.

(f) Technology providers should, most importantly, "build-in" security into their products, so that they are primarily secure when delivered to customers and only require some custom configuration for the specific customer environment. Technology providers should provide non-proprietary training materials related to securely configuring their products, to be used in generalized training courses for cybersecurity workers (i.e., "how to secure hardware product X" or "how to secure software product Y"). They should also provide more specific (proprietary) training materials for cybersecurity workers who are installing their products or implementing their technologies. If the technology provider doesn't offer training itself, then they should partner with a separate training provider.