CYBER WORLD INSTITUTE

Response to Public Comments on NIST 800-181 RFI

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.

   RESPONSE: CWI has provided IT and Cybersecurity Training and Certification for 32 years. CWI is an authorized partner of four of the five global credentialing bodies, CompTIA, ISC2, EC-Council, and ISACA.

   Cyber World Institute was created two years ago to leverage the partnerships, experience and credentials of The Learning Center, Inc. (TLC) in a rapidly evolving and expanding cybersecurity certification training market. TLC has a 32+ year history of delivering IT certification training. Throughout its history, it has morphed and evolved to the ever-changing demands for skilled and certified IT professionals. While TLC has been doing cybersecurity certification training for twenty years, the volume and nuances of the training required are growing exponentially. To meet both the competency and shortage of cybersecurity professionals, we created the Cyber World Institute (CWI) a Nevada corporation. The name Cyber World Institute better describes the focus and reach the enterprise.

   While certifications remain important, employers demand competency (an observable and measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that individual needs to successfully perform a job). CWI has partnered with an innovative performance-based cyber skills developer who has created over 300 labs that, thru the application of knowledge, produce skills and abilities that achieves on-the-ground competency. That competency is holistically and quantifiably measured

against a defined set of tasks with results mapped to the NIST/NICE Framework. CWI is shifting the training paradigm from just knowledge based (certifications) to knowledge + skills + abilities = competency.

CWI offers a cybersecurity skills performance-based scoring assessment. Employers can't afford to hire or employ marginally competent staff. They need to know the cyber competency of current staff and/or new hires. This assessment tool uniquely and adaptively measures an individual's skills across a range of credible responses to a defined set of tasks. Using the same engine as the labs, it also maps key knowledge, skills, and abilities into a set of gradable tasks based on scenarios also keyed to the NIST/NICE Framework.

To shift our education/training programs to "experiential learning" CWI established a partnership with the Merit Network Inc., a 50-year mature organization governed by Michigan's public universities, CWI has access to a cyber range. This virtual environment provides a secure sandbox for individuals/students to develop and hone their skills in a safe and secure environment. Our authorized content is enhanced by the integration of hands-on labs designed to certify competency.

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?

RESPONSE: The existing model of IT and Cybersecurity education and training are knowledge-based. This knowledge-based certification/education model provides only for the measurement of individuals knowledge and does not provide a true measure of their skills and abilities to perform a work role.

This is identified by a lack of metrics and data collection resulting in identifiable skills gaps across the workforce. Many organizations conduct surveys of their membership asking questions about staffing shortfall or training gaps; however, many these surveys are not independent and the result vary greatly. No accurate metrics exist on measure workforce competency, due in large part to the fact the nearly all workforce education, training, and certification effort measure only individual knowledge and NOT skills and abilities.

To reach a point of accuracy regarding the nation's cyber workforce, trainers, educators and certifiers must develop an assessment model to ensure individuals have the requisite skills needed to perform the tasks related to their job roles. In the span of 5-10 years it is conceivable that our nation shifts to a licensure model similar to the UK (IT driver's license), Healthcare and Aviation.

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

RESPONSE: YES, the evolution of the NCWF 3.0 provides a high-level view as well as a granular breakdown of tasks and abilities. This has resulted from 7+ years of gathering information, conducting workshops, expert input, and socialization, the NCWF has created a sufficient understanding and agreement regarding the scope, areas, roles, and KSAs to meet the specific job tasks demanded by organizations who require cybersecurity to facilitate business functions.

The NICE Working Groups which bring all stakeholders to consensus and continue to define and refine our nation's workforce development strategy.

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: Yes, our institution ensures our staff is current and updated to the latest policies, regulatory guidance, threats, and updates to industry recognized certifications.

Most private sector organizations are driven to implement a cybersecurity awareness training programs for their employees due to requirements within particular sector. However, most are inconsistent in enforcing their policy as evidenced by 80% of all breaches are caused are by the end user. One significant driving force in this area is Cyber Insurance requirements.

4. a) What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? b) Are employer expectations realistic? Why or why not? c) Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? d) How do these types of knowledge and skills vary by role, industry, and sector, (e.g., energy vs financial sectors)?

RESPONSE: a) The NICE Framework identifies quite succinctly the knowledge and skills needed in an IT ecosystem and workforce. The 2017 ISACA State of Cybersecurity Workforce Survey further supports employer demand and identifies technical skills, communication (soft skills) and knowledge of business as the most desired skills sets. Additional studies completed by (ISC)2, Microsoft, and Intel Security support the same common thread. The theme is employers are requiring competencies at a practitioner level.
b) Yes, employer's expectations are directly correlated to the cyber threat landscape. Employers are using the NCWF to define expectations within their workforce.
c) The conundrum is the pool employers have to = draw from does not have the requisite skill or ability they require. Employers find talent with knowledge, but very little skill and ability related to job role tasks. 62% of open positions take up to six months or more to be fill or never can get fill at all. This statistic supports the existence of this skills chasm. Also evident is the fact that only 30% of organizations value formal education as most important in this profession, while 70% value practical verification (hands-on skills), specific training, and certification as more important.

d) While there are some minor nuances between the required knowledge and skills among sectors, it is more important right now to address the fundamental skills shortages common across all sectors

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?

CWI Response: The most effective education, training and workforce programs ensure students acquire the requisite knowledge, skill, and ability to perform a NCWF work role. Currently in the United States there is NOT such an overarching program that provide all three components of role performance. However, there are examples of such programs beginning to appear. The goals of these programs are to certify competency. By combining academic or certification program coursework/lecture with hands-on labs in a range environment via an instructor live instructional delivery modality; the US has a scalable education/training and workforce development program. Currently Cyberworld Institute has such a program.

Our vision for our nation is to steer the development of "a vibrant, innovative and sustainable economy while protecting our critical data and infrastructure"; with the solution being an agile competent cybersecurity workforce. To achieve our objectives, our organization is committed to developing competencies linked to employer demand in existing and emerging industries. Our nation's capacity to provide a highly-skilled workforce that meets the needs of the IT employer community will be depend on its ability to leverage existing programs, innovative initiatives to improve the quality of our workforce. Strategies should include:

- Non-college bound youth 17-24
- Veterans with transferable sills into IT/Cyber careers
- Women in Cybersecurity
- Augmenting existing academic and training programs in a competency based model

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

Response: Nationally we face a systemic fundamental divide in our IT and Cybersecurity Workforce Development. A paradigm shift is the genesis and highest priority in the education, training, and workforce development arena in developing individuals with IT and cybersecurity capabilities. Development of individuals with transferable skills-sets and non-traditional backgrounds should be identified as capable of entering the IT and cyber workforce. Like other professions (medicine & aviation); professional development must evolve to an experiential learning model that not only includes knowledge, but skills and abilities development from day one at a practitioner level.

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: Any technology advances will have a domino-effect on the nation's cybersecurity workforce. The talent pool deficit will be further exacerbated by innovations in AI, IoT, etc. Education is particularly constrained due to lack of funding, lack of certified instructors, and a prolonged process to create/update curricula. What is critical, is a more flexible fast-track process be implemented to evolve curricula. As the landscape of the internet continues to expand; the technology (both hardware & software) will continue to evolve at the pace of consumer demand. It is likely that security will remain an after-market product. Education, training, and workforce development program will only be able to adapt if they are flexible. Flexibility is possible through augmentation of existing academic and certification programs with current hands-on labs that contain latest tools and threat data. Labs develop and hone skills to certify individual competencies.

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:

a. At the Federal level?

i. ***SFS program*** is critical and should be continued and expanded to encouraged students to enter government service at federal, state, and local levels.

ii. **CAE program** must be continued and expanded, there are over 4700 colleges and universities in the United States according to the National Center of Education Statistics. Currently the CAE program boosts 226 colleges and universities that is only 4.7% of degree granting institutions in the U.S. The new 2017 requirements for designation or re-designation are critical to the growth and sustainment of the nation cyber workforce because they are requiring members to develop requisite skills and abilities along with the knowledge development that has been the centerpiece for years. Designated key partners for institutions to work with institutions to meet new requirements.

iii. **Introduction of a student loan forgiveness program**. The federal government must work with the private sector to offer loan forgiveness for students with degrees and certification to enter the cybersecurity profession for a minimum of 5-6 years.

iv. **National licensure program.** In the coming years, a competency assessment and certification tri-annual hands-on evaluation is required to license an individual to defend networks is necessary, similar to that in healthcare and the aviation.

v. **Further expand workforce development tool kit:** Further specialize the push-button PD to be critical infrastructure sector specific. DHS & NSA need to develop a guide for academia and training providers that moves them to a skill-based education and training model. NICE should work closely with SHRM to develop a focus area within their certification model for HR professionals that support the cybersecurity workforce.

vi. **VA programs** should highlight IT and Cybersecurity careers as "the most in-demand occupation in our nation. It is highly recommended that the Findings from the NICE Veterans Workshop be reviewed and implemented by the VA. Identifying and funding veterans initiatives should be focused to leverage our "tech-savvy" veterans that are mission focused, strategic thinkers as a means of staffing up our cybersecurity workforce. Investing in programs that upskill non-traditional workers should be implemented and funded. Our veteran community is a talent rich pool that should be tapped "before" they out-process. The current transition program doesn't always open up all career perspectives to veterans and therefore is an area of immense opportunity.

b. At the State or Local level, including school systems?

i. **Cybersecurity Awareness Training**: Mandatory annual training for all school age children to teach cyber security awareness to children as young as kindergarten. Relate Internet usage to stranger danger on the computer; discuss what information a child should never reveal on the Internet. Additionally, ALL programs in colleges and universities should include a cybersecurity component across all programs and studies.

ii. **Cybersecurity Fundamentals**: Should be a mandatory requirement in high schools. Internationally most schools do not offer coding until high school. We need to bring this down to a middle school level. We need to have our children primed in the middle school years to meet the challenges that lay ahead.

iii. **Pathways to Novice Level Certifications**: In high schools, students should be afforded the opportunity to graduate with basic level IT/Cybersecurity certification to enabling to enter the profession right after high school. Due to the lack of qualified teachers, students should be afforded a voucher to attend a local or distance in to training centers to receive certification prep training. Elite school districts should be incented to

engage in technology programs focused on certifications with matriculation of credit to college.

iv. **Continue and expand funding for the Cyber Teacher Program**: Expand significantly the funding and promotion of the DHS Cyber Teacher & Student Development that training teachers on how to integrate cybersecurity into existing courses/classes and provides content for plug-n-play curricula. The constraints on our talent pool is particularly evident in the teaching of IT and cybersecurity. Programs to incent both employers and seasoned practitioners to teach and educate should be developed and implemented.

c. By private sector, including employers?

i. **Promote:** Incent the private sector to integrate cybersecurity professionals into broader employee workforce planning efforts. Employers must become engaged in the process of education and workforce development and not be sidelined observers to the process.

ii. **Adoption of the NCWF**: Adoption is now critical. It creates and establishes standardization across the workforce, and provides a professional development pathway for both employers and employees.

iii. **Workforce development planning**: It simply needs to be part of the human capital plan. Introduction of individual development plans should be used to the development and retention of cybersecurity workforce.

iv. **Introduction of Education and Training Employer/Employee Contracts**: Employers engagement should include career development tied to service commitments so employers receive an ROI on education and training programs for their employees.

d. By education & training providers?

i. **Modify the current education/training paradigm**: Expand workforce development efforts beyond knowledge transfer. Credentialing bodies should add an experiential component to existing courses. Additionally, education and trainers need to modify existing assessments from knowledge only to skills-based.

ii. **Grow and sustain Cyber Ranges**: The continued development and expansion of safe & secure sandboxes is critical to the future development of the workforce. However, care must be give cyber ranges are popping up everywhere.

e. By technology providers?

i. Simply build-in security from the start: Ensure secure software and hardware development starts at the inception of a product.