NIST

Response to NIST RFI pertaining to "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development".

Version 1.0

August 1, 2017

Submitted to:

NIST

Submitted by:

CYBATI

August 1, 2017

CYBATI is responding to the NIST RFI pertaining to "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development". CYBATI is strategically positioned to partner with industry, academia and the government to develop, deliver and facilitate cybersecurity workforce development for Federal Networks and Critical Infrastructure. We greatly appreciate the open call for information and look forward to helping. We are intentionally providing succinct responses as we feel this is part of the challenge.

Sincerely,

CYBATI

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 Start funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)?
    a. **We provide cybersecurity education and research for critical infrastructure and control systems. Our participants vary from high school students, university degree seeking students and active professionals. We are expanding our program using the philosophy of build, break, secure and make.**

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?
    a. **We are not aware of any good metrics that truly represent the state of cybersecurity. The reality is our Nation accepted the model to not require an electronic capability similar to passports for people. Data can move freely around the globe. More effort is needed regulating and segmenting critical infrastructure, requiring cyber building codes, and developing skills-based certifications across all job classifications versus written tests**.

2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?
    a. **Almost 100 years ago our great Nation shifted to promote a service economy. The leaders at the time recognized our energy delivery system would change the landscape of the jobs necessary. We have a great separation of service industry jobs; however, we do not have a requirement for these job categories to include specific cyber and cybersecurity education matching with the responsibilities. As examples, what cyber and cybersecurity education should the Lawyer, Doctor, Accountant, Engineer, IT/ICS Administrator and Business Administrator be required to learn.**

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?
    a. **We are a growing organization providing cybersecurity education. We have requirements for all personnel to regularly be involved in red / blue cybersecurity exercises. These exercises are both tabletop and live scenario driven. All members and critical partners of the company are required to be involved. This is not an easy task even in our small company. It is very important to have an effective learning management system based upon job responsibilities and associated threats and defenses.**

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)?
    a. **This is a major challenge. We currently have a gigantic gap between the skills being taught by our school system and the skills needed by the workforce. The challenge is to build a model that inspires entrepreneurship, teaches each student how to multiply their efforts using our energy infrastructure and integrates cyber and security risks. These skills are not for everyone to continue following, but are necessary for them to learn.**

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?
    a. **Great programs are growing through community BSIDES, Maker and local cyber ranges. These programs leverage decentralized supporting personnel. Their challenge is to ensure continued dedication within each community. We believe it will be necessary to provide a centralized support mechanism for these decentralized grass roots efforts.**

    b. **We also feel that our educational platform serves as a tremendous model for cybersecurity workforce development. The platform is designed using a build, break, secure and make**

philosophy, allows a community to build upon it and is designed for both individual and team-based learning. Many cybersecurity professors, instructors and organizations rely upon self-built and/or unrelated resources leaving the participants to learn both the cybersecurity concepts and the educational delivery platform. We are trying to bridge this gap and provide an easy mechanism to educate both the active professional and new high school student.

c. **We are certain there are other great program and we look forward to reading additional submissions.**

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?
   a. **The Nation and corporations may need to be willing to accept lower workforce productivity numbers and seek goals beyond quarter-to-quarter capitalism. Essential functions of modern life should be de-centralized throughout the country increasing the costs of the attacker through diversity. Deep cybersecurity education needs to be integrated early in the teenage years and across all job classifications. Tools should be provided for students to learn the physical, financial and emotional benefits gained of cyber and cyber-physical systems. It will be paramount to balance the education between security and inventing.**

   b. **It may prove beneficial for everyone to be required to spend some time without the benefits of modern society to value what it offers. The challenge is to help convey the value of cybersecurity.**

   c. **It may also prove beneficial if each technology researched also required the researcher to develop a cybersecurity training module for the technology. This will help carry forward the concepts researched to the next generation.**

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)?
   a. **The current AI / IoT landscape is dire considering the exact same mistakes are being made as in ICS. We are attempting to secure large industrial control systems while AI and IoT systems are**

being adopted and insecurely deployed in mass without regulation. AI and IoT systems include crock pots, refrigerators, pressure cookers, vehicles, planes, energy and medical devices. The government has historically needed to step-in to provide seat belts to safeguard human lives, the time is now for cyber seat belts.

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. **Guidance with optional funding for each state to institute specific cyber building codes and education for all citizens.**
    b. At the state or local level, including school systems?
        i. **Specific requirements for tiers of required-to-be-segmented systems: Military, Critical Infrastructure, and Non-Critical**
    c. By the private sector, including employers?
        i. **Sponsorship of curricula, educational kits and citizens**
    d. By education and training providers?
        i. **Adoption of a standardized educational platform and support for the local government requirements**
    e. By technology providers?
        i. **Acceptance of some risk based upon insurance models**