Cybersecurity Workforce RFI

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

From: Tenable

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.**

Tenable is a major corporate sponsor for The Cybersecurity Diversity Foundation (CDF). The CDF was established to support diversity and inclusion in the field of cybersecurity. Its vision includes a career field that welcomes, supports and provides opportunity and access to all from entry-level to executive and board positions. The foundation works to promote actions that will make a difference in the field of cybersecurity – from providing scholarship funds to championing corporate pledges to fostering workforce diversity programs.

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?**

When it comes to cybersecurity education, metrics can be measured based on the ability of cybersecurity professionals to execute knowledge learned from classes or certification. The ability to quickly identify risks, confirm or detect a threat can be measured based on agility of cybersecurity professionals who actively participate in ongoing training and threat simulations. Gathered metrics should be shared with leadership staff to identify areas of improvement.

In addition to generating qualitative metrics, quantitative metrics should be taken into account to measure the effectiveness of the program. For example, the return on investment of staff training can be measured against the costs associated with a potential breach caused by an email phishing attack.

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

Unlike professions in medicine or law, cybersecurity still lacks an established set of skills, degrees and qualifications that define what a career in the industry looks like. The result means that candidates and employers are unsure of the qualifications and skills needed in their workplaces.

However, programs such as the Cybersecurity Workforce Framework, created by The National Institute for Standards and Technology (NIST), a group under the U.S. Department of Commerce, are creating more awareness of workforce categories and needed skill-sets. The work being done at a Federal level is a step in the right direction, but more work needs to be done on the commercial and industry side of the equation to further create cohesiveness in understanding workforce categories and roles.

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

In order to tackle today's modern security challenges in a creative and effective way, it's clear that employers must rethink how they hire, attract and retain cyber talent. Though employers may appreciate the need to recruit new talent to address growing cyber threats, they're unable to identify the qualifications and skills required to address their workplace needs. This is because there are no established sets of skills, degrees and qualifications that define a successful cybersecurity career.

However, employees who are adaptable to the constant changes associated with latest cyber threats and have a good understanding of networking and systems tend to be valuable assets to cybersecurity programs. Employers first need to define their needs in order to determine the knowledge and skills they're looking for to fill roles in their organization. We believe NICE's Challenge Project will allow employers to evaluate prospective hires, which will ultimately assist with building their cybersecurity workforce.

Employers need to ensure that cybersecurity professionals are aware of the latest security domains associated with the Certified Information System Security Professional program, undergo continuous training to know how to protect against attack vectors and understand how cyber risks impact all business units.

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?**

There are currently a number of cybersecurity education, training and workforce development programs. For example, there are 217 universities accredited as NSA Centers of Academic Excellence in Cyber Defense and another 50 dedicated to Cyber Offense. There are also more than 85 cybersecurity-related certifications. In addition, the National Science Foundation (NSF)'s CyberCorps Scholarship for

Service program has been working to increase and strengthen the government's cybersecurity workforce by providing scholarships to students who work for the government.

A new model is emerging in the cybersecurity profession that emphasizes the diverse, multidisciplinary and fluid nature of the cybersecurity field. As we mentioned before, NIST has created a Cybersecurity Workforce Framework that provides an initial contextual understanding of the range of jobs and associated skills needed in key roles. This provides the field with its first data-driven snapshot of open cybersecurity job positions and allows us to reimagine cybersecurity as a profession with both lateral and vertical career paths, just like medicine or law.

NIST's National Cybersecurity Education Initiative (NICE) has developed a Challenge Project to develop virtual challenges and environments to test students and professionals to perform tasks associated with the Cybersecurity Workforce Framework. Not only can this be used as a platform for instruction, but it can also be used to evaluate those who wish to be part of the cybersecurity workforce. We agree that this will allow employers to have better performance data on prospective hires and will give future employees the right environments to evaluate their knowledge and skill-sets.

This framework is a start. The next step must come from employers that are uniquely situated to articulate the knowledge, skills and abilities most needed in their cybersecurity roles. Once they do that, they may even begin to start training existing employees, saving money on expensive recruiting efforts.

Non-profit industry organizations like the CDF are another pathway toward workforce development. The CDF has guidelines that help corporations create standards for hiring a diverse workforce. And while the CDF welcomes the support of corporate sponsors, it also asks them to go beyond a financial donation to embrace specific tenets in the pursuit of diversity, while also demonstrating their commitment through actions in their own businesses.

This can take the form of:

- Publication of diversity statements on public websites
- Profiles of those within their organization who represent diversity in leadership, including executive and board positions
- Enacting hiring policies that incorporate blind resume consideration, reviewing candidates on experience and merit, and not influenced by names, gender or race
- Financially supporting efforts in the industry to improve the diversity of the up-and-coming cybersecurity workforce

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

There is a well-documented cybersecurity skills shortage that will continue to grow if the industry as a whole fails to act. The Global Information Security Workforce Study (GISWS), released by the Center for Cyber Safety and Education and (ISC)^2 in February 2017, projected that the workforce shortage will reach 1.8 million people by 2022.

A major challenge is that there are no established sets of skills, degrees and qualifications that define what a career in cybersecurity looks like based on the type of business. The result leaves candidates and employers unsure of the qualifications and skills needed in their workplaces. Hiring managers often get over-certified and under-qualified candidates, relying on keywords from their recruiting teams rather than hiring for the skills their organization needs.

To solve the cybersecurity challenges we face today, we need to make sure we are recruiting, developing and maintaining top talent. This is only possible if we improve diversity at all levels of the organization. According to the 2017 Global Information Security Workforce Study: Women in Cybersecurity, women constitute only 14 percent of the cybersecurity workforce in North America and just 11 percent of the cyber workforce globally. Cybersecurity needs to draw in candidates with diversity of thought, experience and perspective.

We need a bold, new cyber workforce strategy that develops and advances the ranks of people from all walks of life, because a lack of diversity is a barrier to success. At Tenable, we have implemented the "Rooney Rule," a founding principle of the CDF, and are setting an example of greater diversity in our leadership ranks. And while the private sector can lead the way, we need buy-in and partnership from the government.

We must think innovatively and revisit our approach to attracting and retaining talent. By encouraging, engaging, actively recruiting and developing minority cybersecurity professionals, we make our industry stronger. This starts with an emphasis and encouragement of Science, Technology, Engineering and Math (STEM), through increased funding for grade school and middle school programs. We also must ensure management and leadership courses are more inclusive to diversity. Only through increased inclusion and diversity in perspective and thought, can our industry achieve greater creativity, innovation, and develop new solutions to our most vexing challenges.

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)?**

The old tools and approaches organizations are using to understand cyber risk have not served organizations well, even in the traditional world of client/server, on-premises data centers and a linear software development lifecycle, where there is less complexity and more control over security. Compare that to today's complex mix of compute platforms and environments, which vary by system longevity, location, manageability, importance and function. Assets and their associated vulnerabilities are constantly expanding, contracting and evolving like a living organism. This elastic attack surface has created massive blind spots, which result in a Cyber Exposure gap. This has impacted organizations' ability to manage, measure and reduce their cyber risk.

To tackle this Cyber Exposure gap, we must better leverage our current cyber talent pool. The need for continuous, updated education, training and development is crucial to ensure today's cyber professionals are prepared and equipped to secure the modern attack surface.

However, our efforts to expand the human workforce will inevitably fall short of the insatiable demand for cyber talent, and we have to prepare for that. We need to have a complementary focus on technology and automation, enabling us to make the most of the human experts we have. Asymmetrically leveraging our cyber talent through the use of technology is the only path to success.

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?

The Administration recently released the Cybersecurity Executive Order (EO), which specifically addresses the need for growth and sustainment in the cybersecurity workforce. The EO directs the Secretary of Commerce and Secretary of Homeland Security, in consultation with other agency heads to assess the efforts to educate and train the American cybersecurity workforce of the future. Also, the Director of National Intelligence, in consult with other agency heads, is ordered to review the workforce development efforts of potential foreign cyber peers to help identify foreign workforce development practices that will affect long-term U.S. cybersecurity competitiveness. We are supportive of this order to ensure that our country maintains a long-term cybersecurity advantage.

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?