August 2, 2016

Danielle Santos
National Institute for Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Submitted to cybersecurityworkforce@nist.gov

Request for Information on
Strengthening the Cybersecurity of Federal Networks and
Critical Infrastructure: Workforce Development

New America is a think tank and civic enterprise committed to renewing American politics, prosperity, and purpose in the Digital Age. We generate big ideas, bridge the gap between technology and policy, and curate broad public conversation. Structurally, we combine the best of a policy research institute, technology laboratory, public forum, media platform, and a venture capital fund for ideas. We are a distinctive community of thinkers, writers, researchers, technologists, and community activists who believe deeply in the possibility of American renewal.

We offer the following comments on workforce development in cybersecurity. We appreciate the opportunity to provide our feedback in the form of responses to questions in the RFI.

———

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?

As researchers and policy analysts, New America places a great deal of value on quantitative data to evaluate the state of the community and the impact of policy decisions. Tools like CyberSeek and reports from industry associations and other stakeholders are useful for understanding the magnitude and distribution of open jobs and workforce shortages in cybersecurity. Relatedly, industry certifications have some utility in certifying an individual's exposure to certain concepts. However, very few tools exist to quantitatively assess the effectiveness of particular education and training efforts from the perspective of the student.

This problem is not specific to cybersecurity, particularly at the postsecondary level. Program data exists from education providers, but rarely does that represent self-reported student outcomes like employment and earning potential. The lack of such data impedes proactive quality management in growing fields such as cybersecurity and creates difficulties in assessing the applicability of skills taught to available work. That is to say, if recent graduates are not readily employable, larger questions emerge as to the nature of the mismatch between education and job requirements, but the problem is hard to articulate without data to correlate geographic and economic mobility – and, ideally, industry feedback – with different academic programs.

At the secondary level, where state-level data is more abundant, variances in metrics between states present challenges in developing a wider understanding of the effectiveness of education programs. Pre-apprenticeships, internships, and other types of work-based learning especially, should be the target of more innovation for "counting" student skills (for example through portfolios or extended transcripts) in order to leverage them in the labor market.

———

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

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) provides a valuable taxonomy of occupations and specialties in the cybersecurity field. However, our understanding is that its utility and implementation across the cybersecurity community varies significantly by actor based on (1) maturity of understanding on cybersecurity human resources issues, (2) bureaucratic flexibility, and (3) sector.

We find that companies with a high degree of maturity in their understanding of the cybersecurity workforce—for example, established cybersecurity firms—are likely to rely on their own knowledge of the work they do, and typically have a preferred internal taxonomy. In these cases, such firms generally have the contextual knowledge to relate this to the NCWF, even if there is not direct concordance. By contrast, organizations with less experience in the industry—for example a company transitioning from a managed service provider for cybersecurity to an in-house team—may lack the understanding needed to navigate the variance in job titles, descriptions, and requirements. In this case, these hiring personnel might benefit greatly from a more streamlined and user-friendly adaptation of the NICE Cybersecurity Workforce Framework (NCWF), which we expect would be gratefully received in the human resources community.

Organizations with limited bureaucratic flexibility—for example, government organizations with an existing structure for information technology roles—may have limited ability to adapt to outside input on workforce taxonomies. Such organizations may understand (and prefer) their existing structure internally and be comfortable with its parallels to the NCWF's taxonomy, but

this variance is likely to remain confusing to job seekers and is difficult to capture in sector-wide workforce data and assessments.

The NCWF acknowledges that it cannot provide a comprehensive cyber personnel taxonomy for every organization or sector, which must necessarily consider their own imperatives in hiring cybersecurity staff. As priorities within industries such as healthcare, hospitality, finance, and education evolve, NICE should look to industry organizations to develop simple, sector-specific, and consensus-based workforce frameworks to share experiences and facilitate the training and hiring of candidates suited to each field's needs.

———

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

Beyond basic awareness and hygiene education, Question Three is not generally applicable to New America's workforce.

———

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)?

The filtering criteria that we have most often heard cited is a combination of formal education (i.e. academic degree), work experience, industry certifications, and ability to utilize particular tools and systems. However, these criteria used to initially filter applications are not necessarily the skills most valued by employers. More likely to be valued are "soft skills" like analytical ability, personal responsibility, or communication capacity; knowledge specific to the industry or position (e.g. industry regulatory requirements); or specific technical skills. Employers often report that potential employees lack one, two, or all three of these skills sets.

While it is difficult to generalize about the proportionality or realism of employer expectations, as many appear acutely aware of the challenges involved in hiring for cybersecurity roles, American employers across industries expect a lot from their candidate pool, but are rather unwilling to pay to develop it. So long as the preference to hire fully-trained candidates dominates hiring practices, our cyber workforce will remain insufficient. The development of community-wide collaborative efforts, perhaps established along the model of—or even in coordination with—existing information sharing and analysis organizations (i.e. ISACs and ISAOs), could lower the financial and time cost to developing educational tools like curricula and

skills metrics. This would encourage employers from all sectors to recognize that a robust cybersecurity workforce is fundamentally beneficial to all.

The mismatch between the student pipeline/current workforce and available jobs is particularly pronounced in positions that rely heavily on sector-specific knowledge. University programs are very rarely designed to produce graduates with a background in both cybersecurity and the needs of a particular sector. In these cases, employers can expect to hire for one skill set and provide training for the other. For example, A hotel chain looking to hire an executive-level cybersecurity director might do well to hire a veteran cyber professional whose experience lies entirely in another sector; in that case, the employer must be willing to spend weeks or months orienting that individual towards their particular risk profile and business needs. On the other hand, a marketing startup transitioning from managed cyber services towards a dedicated internal team might be best served by upskilling incumbent information technology employees with intuitive knowledge of the company's back end systems and client dynamics. This requires additional training expenses and time spent selecting appropriate training providers, but could be expected to pay off in security results.

———

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?

No single method stands out as a panacea for all stakeholders; however, certain training options show particular promise for scalability and utility across sectors.

At New America, we are exploring work-based learning, and particularly apprenticeships, as a viable method to address both the misalignment between jobseeker skills and employer requirements and the shortage of potential employees overall. These programs offer an opportunity for employers to ensure a pipeline of employees knowledgeable about their specific tools, methods, and business needs by way of a tailored training program and experience within the organization. When coupled with existing higher education institutions, these programs take advantage of such institutions' best practices and credit-bearing coursework while drastically improving learners' likelihood of a job upon program completion relative to other training options. While larger employers may have the workforce need and capacity to develop and operate such programs in-house, smaller employers may utilize regional/sectoral collaborations or intermediaries to lower the individual cost of development and implementation.

Other promising training opportunities exist. Dedicated cybersecurity undergraduate and graduate degree programs and specializations have emerged in recent years, having previously fallen under the larger umbrella of computer science and engineering. At least a dozen

dedicated, high-quality cybersecurity programs at 2-year and 4-year institutions now exist; the best among these involve an interdisciplinary approach that does not confine students to one sectoral silo, and work-based components (internship, apprenticeship, or a co-op structure) that deliver crucial hands-on experience prior to graduation. In order to ensure the continued success of such programs, educators would be well-served to consider the balance of near-term relevance and long-term durability of coursework, ensuring that curricula serve students well as they transition into mid-career and management positions. Above all, cybersecurity degree programs should be non-terminal, providing a basis for future study and upskilling.

Intensive training intended to help fill specific cyber positions can also play an invaluable part in an effective cybersecurity ecosystem. While there are some quality risks associated with bootcamps when they are primarily paid for by the trainee (as has been the model for most web and software development programs), these are less severe when employers select incumbent workers for training and shop around for quality providers. Analogously, programs designed around industry partnership and robust career placement services can diminish concerns of exploitation by bad actors. It should be mentioned that many of the most promising such options are currently still in development.

———

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

Despite the profound expertise, skill, and commitment of the cybersecurity workforce, the proliferation of unfilled cybersecurity positions hampers the community's ability to counter cybersecurity threats. The effects of this are not distributed evenly across stakeholders. State, local, territorial, and tribal governments face a particularly daunting recruiting environment due to budget constraints and a perception of a more mundane mission than other more glamorous federal agencies can offer. Meanwhile, the average age of the existing workforce at these levels of government is increasing steadily, foreshadowing greater need for new workers as experienced professionals retire.

Filling open positions requires tapping into a more diverse—and consequently larger—talent pool. More than simply demographic diversity, a more robust cybersecurity workforce also requires a diversity of background, educational history, and work experience. It is incumbent on the whole of the cybersecurity community to think critically about recruitment and retention efforts, and how a strategic, inclusive, and flexible approach to human resources policy can increase the talent pool and significantly improve overall output.

An additional challenge derives from the expansion of computer technology into practically every aspect of American communication, governance, and business. Accordingly, components of cybersecurity training beyond standard awareness and hygiene education will need to be wrapped into a greater number of other disciplines through training courses and modules

adapted to different professional specialties entirely (e.g. human resources, legal, etc). Furthermore, employers—and, just as importantly, the cyber advocacy, research, and education communities—should continue to break down the esotericism of cybersecurity, both to encourage new entrants to the cyber workforce and to address human cyber vulnerabilities.

———

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)?

Overall, the advance of information technology into new spheres of American life will continuously expose new vulnerabilities, both human and physical, making cybersecurity increasingly critical. In particular, the rising prevalence of internet-enabled devices demands a new focus on training cyber professionals to clearly communicate cyber risks and best practices to the general public, much in the same way that a more comprehensive healthcare ecosystem has created the demand for "care navigators".

More specifically, the inclusion of artificial intelligence systems in new industries (such as advanced robotics in manufacturing and predictive analytics in education) will result in mission-critical cyber competencies for previously purely mechanical or "human" occupations. The cybersecurity education market should respond by providing agile, modular training options for professionals who are not dedicated to the field of cybersecurity, but whose work will increasingly demand cyber skills.

———

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?

Many beneficial federal workforce training programs exist and should be continued, among them the Department of Homeland Security/National Security Agency’s Centers of Academic Excellence. Similarly, the Scholarship for Service CyberCorps should be preserved and prioritized in order to encourage promising students of diverse socioeconomic backgrounds to pursue careers as cyber professionals. Additionally, as a very significant component of the cybersecurity workforce pipeline, the military has a critical role to play in workforce training. It is difficult to overstate the role veterans play in the cybersecurity workforce, and as such, military training in cybersecurity should be allowed to articulate into other industries wherever reasonably practicable.

Community colleges can have a powerful role in responding to the proliferation of cyber vulnerabilities, especially into physical systems. As many of the professionals whose skills support physical infrastructure, capital, and utilities receive at least their initial training at community colleges, these provide an ideal opportunity to deploy and evaluate modular and sector-oriented cybersecurity training to protect cyber physical systems. Furthermore, no cybersecurity education program is complete without an applied, practical, or work-based component. Academic institutions deploying new programs should be wary of restricting their curriculum to classroom-based learning.

———

We appreciate your willingness to consider our comments. Please contact us at bate@newamerica.org and prebil@newamerica.org with any questions or concerns.

Sincerely,

Laura K. Bate
Program Associate
Cybersecurity Initiative

Michael Prebil
Program Associate
Center on Education & Skills at New America