CSIA RFI Responses, January 15, 2019

Update to the 2016 Federal Cybersecurity Research and Development Strategic Plan RFI Responses

DISCLAIMER: The RFI public responses received and posted do not represent the views and/or opinions of the U.S. Government, NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD), NITRD National Coordination Office, and/or any other Federal agencies and/or government entities. We bear no responsibility for the accuracy, legality or content of all external links included in this document.

NEW AMERICA

January 15, 2018

NCO/NITRD,
Tomas Vagoun,
2415 Eisenhower Avenue,
Alexandria, VA 22314,

Submitted to cybersecurity@nitrd.gov

Response to the Request for Information on the Federal Cybersecurity R&D Strategic Plan

New America is pioneering a new kind of think and action tank: a civic platform that connects a research institute, technology lab, solutions network, media hub, and public forum. We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

One of the areas of focus for our Cybersecurity Initiative is workforce development. We believe that a well-taught and appropriately prepared cybersecurity workforce is a central component in securing America against cybersecurity threats. Accordingly, we seek to identify best practices and develop policy tools to align educational pathways with employer needs. Therefore, understanding the data and trends that characterize the workforce is essential to our work, and so we have a significant interest in the development of the Federal Cybersecurity R&D Strategic Plan.

We offer the following comments on research and development in cybersecurity. We appreciate the opportunity to provide our feedback in the RFI.

Federal support has been a critical driver in the development of new programs in cybersecurity workforce development targeted at many different ages and groups. We hope this support continues. However, we also see an opportunity to invest in research that allows the community to better understand trends in the workforce. While some data around the cybersecurity workforce does exist, there are major gaps in the cybersecurity community's understanding of our workforce. In fact, in New America's recent paper on cybersecurity workforce development, we dedicated an appendix to laying out these questions. That work is available here:

https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-workforce-development/appendix-unanswered-questions-in-cybersecurity-workforce-empirics.

However, on a more general level, there are three particular trends in research on cybersecurity workforce development that we feel merit particular attention: (1) very little longitudinal data is available to evaluate the effectiveness of different educational pathways and programs; (2) data from job postings likely distorts perceptions of industry needs and expectations; (3) data lacks consistency between studies.

Longitudinal Data is Critical to Measuring Effectiveness

A number of different sources have taken the first steps into better understanding the empirics of the cybersecurity workforce. Notably, CyberSeek, the joint project between the National Initiative for Cybersecurity Education (NICE), Burning Glass, and CompTIA catalogues job openings in the United States and categorizes it by a range of different criteria. $(ISC)^2$'s Cybersecurity Workforce Study (formerly the biannual Global Information Security Workforce Study) gives insights into the existing workforce via survey data. Several other polls and studies fill in various pieces of the puzzle around demographics, retention, and other topics. The value of this research cannot be undersold. It provides a vital first step in understanding the trends and patterns of hiring in the industry, and it also shines a light on the scale of the problem, thus adding weight and urgency to calls for additional efforts.

Now that we, as a community, begin to understand the scale and scope of the unfilled jobs in cybersecurity, we must turn our attention to evaluating solutions as well. The next step in this body of research should provide a basis for determining which educational pathways are most effective and under what circumstances. To do that, we need longitudinal data that connects degree programs, apprenticeships, bootcamps, informal learning, employee training programs and other learning systems to long-term learner outcomes. For example, how quickly do learners find jobs? What types of jobs are they? Were the learners able to advance in those jobs over the span of years? Were they equipped for managerial positions, or did they need to pursue further study? Did employers find their education effective, or did they conduct additional training?

Cybersecurity workforce development is an issue area with increasing profile. As educators, policymakers, employers, and researchers turn their attention to the subject, a growing range of potential pathways into the workforce has emerged. Many of these pathways--apprenticeships, boot camps, online education, upskilling for existing workers and others--are relatively nascent in cybersecurity and quite small in scale. It will take a great deal of investment to develop these pathways into systems that are effective at scale. Without data that ties educational pathways to long-term outcomes, both for employees and employers, the community of stakeholders involved has little more than anecdotes and extrapolations from other industries to inform their decisions as to the pathways in which they invest. Longitudinal data that connects long term

outcomes with education and training systems would be invaluable for informing public and private sector decisions on cybersecurity workforce development.

Hiring Data Differs from Job Posting Data

Much of the existing data on the cybersecurity workforce comes from job postings. This data can tell us what certifications are in demand, how common degree requirements appear to be, and many other useful pieces of information that speak to how employers are thinking about their workforce and needs. However, this information does not tell us much about the workforce itself, or even about the new hires that fill the jobs that are posted.

For example, according to CyberSeek.org, 77,492 job postings currently request a CISSP certification. However, since fewer than 76,000 CISSP certifications have been awarded (and those awardees are very likely to be already employed), many of those 77,492 jobs are likely to be filled by new hires who do not hold a CISSP. The same holds for many other requests and requirements in job postings, thus it is almost certain that the requirements reflected by job posting data inflate the qualifications of those actually hired. Gaining an understanding of the "successful" candidate, rather than the "ideal" candidate is likely to present a much more accurate and informative picture as educators and job seekers continue to try understand what employers are seeking.

Data Consistency

Existing data on the cybersecurity workforce varies considerably by source. For example, the $(ISC)^2$ 2018 Cybersecurity Workforce Study estimates nearly half a million unfilled cybersecurity jobs in North America; whereas, CyberSeek.org estimates just over 300,000 in the United States. Even recognizing the difference in geographical scope, that is a remarkable variance, and it creates challenges in identifying trends in the workforce from study to study or year to year.

It appears that much of this variance is a result of differing criteria for what qualifies as cybersecurity jobs. Increased adoption of the NICE Cybersecurity Workforce Framework is likely to mitigate much of this variation and increase data consistency because it offers a standard taxonomy for these jobs. While some--ourselves included--have made the case that the Framework cannot capture absolutely all jobs that make up the immensely diverse and cross-cutting cybersecurity industry, it does provide a very effective means for establishing a standard. As such, research into cybersecurity workforce development should be encouraged to use the Framework as a guide for criteria for inclusion in developing empirical data around cybersecurity jobs and workers.

By addressing these three trends in research on the cybersecurity workforce, the forthcoming Federal Cybersecurity R&D Strategic Plan can make significant steps in improving the

cybersecurity community's understanding of the workforce and thus its ability to fill open jobs. I appreciate your willingness to consider these comments.

Sincerely,

Laura K. Bate
Policy Analyst
Cybersecurity Initiative
New America