CLTC
Center for Long-Term Cybersecurity

102 South Hall
Berkeley, CA 94720
510-664-7506
cltc@berkeley.edu

Subject: Cybersecurity Workforce RFI

To Whom It May Concern:

We thank NIST for the opportunity to submit information about current, planned, or recommended education and training programs aimed at strengthening the U.S. cybersecurity workforce. As representatives of the Center for Long-Term Cybersecurity (CLTC), a university-based research and collaboration hub focused on the future of cybersecurity, we are extremely pleased that the federal government is prioritizing investments in the cybersecurity talent pipeline.

Research, Metrics, and Data

We appreciate the concern of the RFI with various empirical questions relating to the cybersecurity labor market: what knowledge is necessary for the workforce; what training programs are most effective; and so forth. These are important questions, and deserve adequate attention. At the same time, we wish to highlight that underpinning these questions is a commonly held perspective: that cybersecurity, broadly defined, is being impacted negatively and significantly by a lack of human capital and talent, and that this is the result of a labor market failure into which the government should intervene.

It is indeed clear that the cybersecurity talent pipeline suffers from some kind of market failure, in the sense that demand and supply are visibly and significantly mismatched. But, before we can analyze important questions about what policy shifts are required in this space, we believe NIST should first *break down and analyze the precise causes and sources of market failure*. Research questions that we believe would contribute in that direction include:

- What are measures of a healthy labor economy for cybersecurity?
- What metrics can empirically tie an organizations' security to the expertise and maturity of its cybersecurity workforce?
- What are the most pressing threats the cybersecurity workforce is likely to address in the next 5 years, and how do the skills currently present in the labor market compare to those that will be needed?
- NIST has published marketplace data (like those on cyberseek.org) on the cybersecurity workforce, but it primarily focuses on technical positions. What peripheral positions are needed to support a healthy cybersecurity workforce (legal, HR/hiring specialists, policy), and what impact does cybersecurity literacy have on building effective teams?

We believe that understanding this market is an essential precursor to investigating important follow-on questions about the status of this market, including 1) challenges, both in terms of supply and demand, in getting sufficient and sufficiently trained persons working in cybersecurity; 2) challenges with regards to diversifying the cybersecurity workforce along a number of dimensions (and the possible benefits of doing so more boldly); and 3) opportunities, in terms of policy, incentives, and other solutions, to improve these outcomes.

At CLTC, we are beginning to explore a research agenda on the cybersecurity labor market. In addition to the above, example problems that might fit into this research agenda include but aren't limited to:

1) How can we grow a robust and adaptive cybersecurity workforce in part using persons without technical university degrees, for instance by training such persons efficiently at scale and/or using their non-technical skill sets to supplement technical knowledge?
2) What are the structural factors that are keeping diverse applicants from pursuing cybersecurity jobs, and what outcomes result from this lack of diversity?
3) How will automation change the cybersecurity workforce, and what risks and opportunities present themselves out of this change?
4) What role could and should government play in modifying supply and demand trends in cybersecurity? Are there additional actions that the private and/or philanthropic sectors could take in this regard?

We welcome partners -- including NIST -- interested in these questions, and in the cybersecurity labor market more broadly.

Education

We share NIST's concern with the lack of quality education programs in cybersecurity; particularly at top universities, there are very few opportunities for professional development in cybersecurity. For this reason, in collaboration with the College of Engineering and CLTC, UC Berkeley's School of Information (I School) is developing a new online degree program: the Master of Information and Cybersecurity.[1] The program, which is currently pending university approval, aims to address the technical aspects of cybersecurity while preparing students to consider policy making on the national, international and organizational levels. While we cannot currently report on results given that the program is yet to launch, we would be very happy to share results after classes begin, tentatively scheduled for May 2018.

Policy Solutions

Finally, we urge NIST, as it considers policy solutions to resolve any market failures identified in the cybersecurity space, to take into account innovative solutions outside the box of those normally approached by government. For instance, here is one particular market problem: today, when the US Government wishes to solve digital national security problems, it almost exclusively draws upon East Coast-based government employees or contractors. As a result, the federal government has struggled to fill cybersecurity jobs, especially in a classified setting.[2] In part, this is because, with rare exception, the West Coast's private-sector cybersecurity technologists, who often have precisely the skills most needed in the federal government, have displayed little interest in working for the national security community. While senior cybersecurity leaders recognize the need for this talent,

[1] For more information, see https://datascience.berkeley.edu/cybersecurity/.

[2] Even prior to the recently implemented hiring freeze in the federal government, more than 1,000 federal cybersecurity jobs were unfilled. Sternstein, Aliya. "Trump's hiring freeze blunts rush to recruit cybersecurity talent." *Christian Science Monitor Passcode*, January 25, 2017, http://www.csmonitor.com/World/Passcode/2017/0125/Trump-s-hiring-freeze-blunts-rush-to-recruit-cybersecurity-talent.

many structural, bureaucratic, and cultural factors have contributed to the acute government labor shortage, including:

- Demand for cybersecurity professionals that is expanding rapidly across sectors, leaving the federal government in competition with the private sector for top talent;
- A cultural disconnect between 'West Coast' and 'East Coast' work styles, which is partially the result of lengthy, bureaucratic decisionmaking that can delay testing and implementation of new technology solutions, as well as poor work environments in aging government buildings;
- Organizational tensions between government and private sector work structures, including lengthy, cumbersome security clearance processes that often cause applicants to lose interest in government jobs before their application process is completed, and security policies that can unnecessarily isolate employees from their social and professional networks;
- Geographic and career rigidities within the federal government, including risk averse government managers, and relocation requirements from preferred technology hubs like Boston, Austin, and, most importantly, Silicon Valley to the greater Washington, DC area; and
- The inability to easily transition between government and private-sector roles, particularly since it may be difficult to stay current on the latest private-sector technological developments while working in government.

While the US Government is already seeking to remedy these organizational challenges on a piecemeal basis, it takes significant time and effort to change large organizations. To make cybersecurity agencies hospitable to highly innovative, private-sector technologists would require senior US Government leaders to make significant and simultaneous structural changes to HR and security policies, professional incentives, work environments, and management techniques. Such changes would almost certainly be disruptive to the existing workforce and would likely be met with resistance from current government employees, rendering the changes ineffective.

With our colleague Jesse Goldhammer, we have released a white paper, "Cyber Workforce Incubator," (available at https://cltc.berkeley.edu/, and attached as an appendix),[3] describing an institution that we think could better attract the West Coast's best technologists to work for the US Government. Through a careful application and vetting process, the CWI would choose promising private-sector candidates for a one- or two-year workforce development program in a classified setting. Participants would undergo a rapid security clearance process before joining specialized teams that have needed technology skills; collaborate with defense, intelligence, and homeland security partners; and work on discrete projects that achieve defined mission objectives. CWI would replicate the environment, culture, and pace of West Coast startups, dramatically increasing the benefits and reducing the costs for private-sector technology talent to engage in national service. CWI would also provide state-of-the-art training and mentorship to participants, who will complete the program with new and more refined skills that will ultimately benefit federal, non-profit, or corporate employers. Incubator participant stipends would combine federal dollars and corporate

[3] The White Paper, as well as Congressional testimony submitted on the subject, is available at https://cltc.berkeley.edu/2017/04/06/cyber-workforce-incubator/.

donations, ensuring that private-sector organizations share some of the costs of training talent from which they will benefit.

The cybersecurity workforce incubator is not a traditional government solution – and that is precisely the point. Such ideas draw from the entrepreneurial ecosystem, which is most fertile in Silicon Valley but also present in other entrepreneurial hubs, that develops talent through:

- A culture of relentless experimentation and the nimbleness to shift resources away from "dead ends" with relatively little friction;
- A relatively open labor market where people circulate and re-mix expertise by moving around through different companies;
- A large and dynamic professional community that shares common values, and that is continuously re-infused with research and thought leadership by two of the world's top universities; and
- Powerful economic incentives that encourage the rapid commercialization of emerging technologies.

As NIST considers policy recommendations, we urge it to think outside the box, in the way that Silicon Valley entrepreneurs often do, in thinking of policy solutions that may not reflect the traditional way that things are done within the Beltway. We would be more than happy to provide support as NIST considers these options.

Offer of Support

Finally, we note NIST's desire to host workshops on these important issues. As previous hosts of the White House Commission on Enhancing National Cybersecurity's West Coast forum, we would be honored to host such a session at UC Berkeley.

Sincerely,

Professor Steve Weber, Faculty Director
Betsy Cooper, Executive Director
Sean Brooks, Research Fellow

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@cltcberkeley