Written Testimony of
Steven Weber, Faculty Director, UC Berkeley Center for Long-Term Cybersecurity
Jesse Goldhammer, Associate Dean, UC Berkeley School of Information
and Betsy Cooper, Executive Director, UC Berkeley Center for Long-Term Cybersecurity

Before the
Subcommittee on Information Technology,
Committee on Oversight and Government Reform,
U.S. House of Representatives

April 4, 2017

We are pleased to contribute written testimony to the Committee regarding the cybersecurity workforce talent gap, particularly with regard to the committee's interest in public and private skills shortages, and the prospects for an industry-government rotational workforce. As representatives of one of three national cybersecurity centers founded through the Hewlett Foundation Cyber Initiative—and the only one at a Tier One public research university—we are deeply concerned about the shortage of cybersecurity professionals to fill available jobs. UC Berkeley will contribute to narrowing the human capital gap as we plan to launch in 2018 an online cybersecurity masters' degree program that will be available to students across the country.[1]

At the same time, we believe that the committee should focus its attention not just on the numbers that describe the cybersecurity labor market gap, but on the specific reasons why skills are lacking and jobs remain unfilled. We believe that one significant reason the federal government is struggling to fill its cybersecurity workforce is that there are few opportunities for private-sector technologists to work for the government without having to relocate to Washington, DC to take a permanent government job. Put simply, the dynamic flows of knowledge and talent that energize the Silicon Valley technology and human capital ecosystem are not mobilized to the benefit of government cybersecurity needs. In the below testimony, we outline the skills shortage issue and propose a solution —a Silicon-Valley based Cyber Workforce Incubator—that can address this urgent challenge.

Importantly, we do not believe that this organization should be based in a federal agency, nor should it be solely funded by federal dollars. An independent 501(c)(3) in the model of In-Q-Tel, and funded jointly by the government and private sector, will best reduce the friction that discourages private-sector technologists from working on government problems, and often prevents West Coast talent from working in East Coast government agencies.

The Nature of the Cybersecurity Skills Shortage Problem

Cybersecurity is arguably the fastest-growing and most important subfield of information technology. Yet the dramatic rise in the importance of cybersecurity has been accompanied by a severe shortage of trained professionals. In the private sector, "[t]he demand for the [cyber security] workforce

[1] For more information, see cybersecurity.berkeley.edu.

is expected to rise to 6 million (globally) by 2019, with projected shortfall of 1.5 million."[2] Already, more than 209,000 cybersecurity jobs in the United States are unfilled; demand is expected to grow by 53 percent through 2018."[3] Cisco estimates there are more than one million unfilled cybersecurity jobs worldwide,[4] while the UK House of Lords estimates two million.[5]

The United States cybersecurity infrastructure has also struggled to recruit private-sector talent into the federal government. The Department of Defense aimed to find 6,200 operators to fill CYBERCOM's 133 Cyber Mission Force teams by 2018, with an interim goal of reaching "initial operating capacity" by the end of 2016.[6] In 2015, Admiral Mike Rogers said that CYBERCOM was "already hard pressed" to find qualified candidates to fill its 133 Cyber Mission Force teams.[7] As of January 2017, there are reportedly 123 teams, with only 27 operating at full capacity.[8] These problems are not limited to the military; even prior to the recently implemented hiring freeze in the federal government, more than 1,000 federal cybersecurity jobs were unfilled.[9]

The prototypical way of explaining this cybersecurity labor market shortage is to describe it as a "market failure" into which the government should intervene. But we believe that treating the entire cybersecurity market as a unilateral entity that is "failing", or to assume that one policy solution could resolve this problem, would be a mistake. Instead, there are likely multiple markets for cybersecurity professionals, and/or multiple challenges or failures to be faced, requiring separate solutions.

We focus here on 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. 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, many structural, bureaucratic, and cultural factors have contributed to the acute government labor shortage, including:

---

[2] Steve Morgan, "One Million Cybersecurity Job Openings In 2016." *Forbes* (Jan. 2, 2016) (quoting Michael Brown, CEO of Symantec), https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#3bd0a4b827ea.

[3] Setalvad, Ariha. "Demand to Fill Cybersecurity Jobs Booming." Peninsula Press (March 31, 2015), http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/.

[4] Cisco. *Mitigating the Cybersecurity Skills Shortage* (2015), http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf.

[5] Morgan, Lewis, "Global shortage of two million cyber security professionals by 2017," IT Governance (Oct. 30, 2014), http://www.itgovernance.co.uk/blog/global-shortage-of-two-million-cyber-security-professionals-by-2017/.

[6] United States. Department of Defense. "The Department of Defense Cyber Strategy." April 2015. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[7] Rogers, Mike. "A Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities." March 4, 2015. http://docs.house.gov/meetings/AS/AS26/20150304/103093/HHRG-114-AS26-Wstate-RogersM-20150304.pdf

[8] Maucione, Scott. "CYBERCOM's New Buying Power Now Closer to Reality." *Federal News Radio,* January 2017. http://federalnewsradio.com/acquisition/2017/01/cybercoms-new-buying-power-now-closer-reality/

[9] 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.

- 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.

Moreover, even if the US Government *could* find ways to convince sufficient numbers of West Coast professionals to relocate to Washington, we do not believe this would be advisable because the quality of that talent depends precisely on its intimate, ongoing connection to the entrepreneurial ecosystem present in Silicon Valley. This ecosystem, which is most fertile in Silicon Valley but also present in other entrepreneurial hubs, 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.

Especially in the short to medium term, this system simply cannot be replicated inside government. As a result, it is important for the federal government to find a way to access cybersecurity talent within the Silicon Valley ecosystem, and not remove talent from it.

A New Model for an Industry-Government Rotational Workforce: The Cyber Workforce Incubator

We have so far argued that West Coast cybersecurity professionals do not want to work for the federal government under current conditions. But this is not the same as saying that West Coast cybersecurity professionals do not want 'government jobs' per se. We believe that, if such professionals were given the ability to work on national security challenges without degrading their cutting-edge technical skills or requiring them to give up their livelihoods, work cultures, and social networks—and to leverage that experience to advance their career—many would jump at the opportunity.

Other proposed industry-government rotational workforce solutions—such as a Cyber Reserve Force or temporary appointments within the US Digital Service—are not well equipped to provide this type of work experience. While a traditional rotational program would reduce one barrier to entry—enabling short-term private-sector engagement with interesting US Government problems—it would not attract those deterred by the cultural differences, geographic distance, or career rigidities within the federal government.

We have released a white paper, "Cyber Workforce Incubator," (available at https://cltc.berkeley.edu/, and attached as an appendix), 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. 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 donations, ensuring that private-sector organizations share some of the costs of training talent from which they will benefit

By giving technologists and government workers the opportunity to work side by side on unique government problems through short deployments, an incubator will fill a unique workforce niche that government agencies cannot solve themselves or through conventional contractor relationships with academics or private-sector companies. By overcoming a manageable number of geographic and bureaucratic hurdles, such an incubator can help the US government to solve some of its toughest technical innovation challenges, recruit top talent, build a strong reputation, and lay the groundwork for long-term, private-sector cyber technology innovation partnership that will benefit the nation for generations.

We do not believe such an organization should be housed in a federal agency. Instead, following the model of In-Q-Tel and its relationship to CIA, the CWI should be an independent 501(c)(3) nonprofit that is anchored to a particular agency—likely the Department of Defense, CYBERCOM, or NSA—but also serves the needs of other sister agencies. In-Q-Tel, which operates as a venture capital resource to promote technology development for the intelligence community, functions differently than a government agency because of its independent status. In-Q-Tel has successfully identified promising early-stage technologies for the intelligence community because it stands between the public and private

sectors, and so can understand the needs of the intelligence community and translate those needs to start-ups. A cybersecurity incubator could similarly identify promising solutions to difficult problems through its ability to liaise between the public and private sector. This structure would also make it possible for the incubator to work on problems that sit under different authorities (e.g., Title 10 and Title 50).

We believe that joint federal and private-sector funding is the best model for setting up a Cyber Workforce Incubator. Because the CWI experience will provide its participants with marketable skills, the private sector should share the burden in supporting participant stipends and direct operating costs. At the same time, federal investment is necessary to set up the organization, and to demonstrate ongoing US Government support for the initiative. Federal expenses will likely be more significant in the first few years of operation, and will decrease as CWI develops the expertise, relationships, and reputation required to consistently raise private funds.

Conclusion

Today, the nation's most talented cyber technologists face a stark choice between private- and public-sector employment. This choice does not serve the nation well, and the costs to national security are mounting as technology evolves and the gap between the private- and public-sector workplace experiences widens. CWI provides the US government with a low-risk, high-impact, and organizationally proven way to leverage top talent without also needing to massively restructure its own work environment, incentives, and systems. We urge the Committee to consider this model as a way to begin closing this particular aspect of the cybersecurity workforce talent gap.

About the Authors

Steve Weber is Faculty Director of the UC Berkeley Center for Long-Term Cybersecurity, as well as a Professor in the School of Information. Jesse Goldhammer is Senior Advisor to the Center, as well as Associate Dean for Business Development and Strategic Planning at the UC Berkeley School of Information. Betsy Cooper is the Executive Director of the Center.

The Center for Long-Term Cybersecurity is a research and collaboration hub housed within the University of California, Berkeley School of Information (I School). Funded through a generous seed grant from the William and Flora Hewlett Foundation, the CLTC has a mission to design solutions to cybersecurity issues that arise wherever humans and digital systems interact, based on a long-term vision of the internet and its future. Working with researchers from UC Berkeley and outside organizations, we are building a diverse community of partners to advance concepts, technologies, and recommendations that will help governments, corporations, and individuals better prepare for the challenges of cybersecurity throughout the 21st century. We focus our work on three streams of activity: Research, Education, and Engagement.