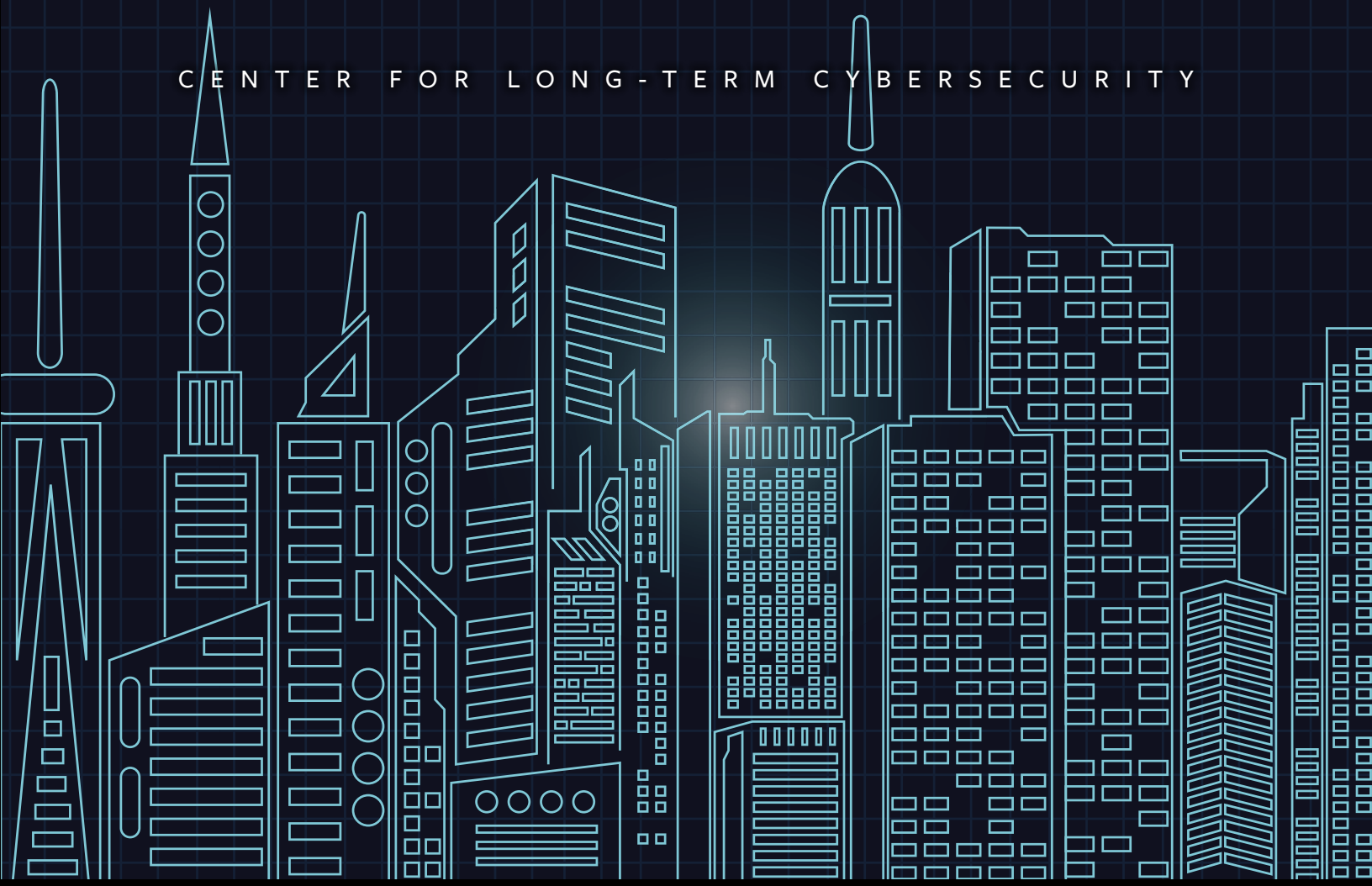
CENTER FOR LONG-TERM CYBERSECURITY



CLTC OCCASIONAL WHITE PAPER SERIES

# Cyber Workforce Incubator

JESSE GOLDHAMMER, STEVEN WEBER, AND BETSY COOPER

# Summary

The United States urgently needs highly innovative, technically trained personnel for cyber defense and security to protect critical infrastructure and assure vital military and civilian missions. The Defense, Intelligence, and Homeland Security communities struggle to acquire, train, and retain sufficient numbers of cutting-edge technologists who can help the government innovate faster and more effectively than our adversaries, specifically in the domain of cybersecurity.

Cyber defense and security require a highly skilled, deeply technical workforce that has experience with the latest hardware and software as well as the know-how and mindset to solve a wide range of complex, ambiguous problems. Women and men across the West Coast have these capabilities because they live and work in a regionally distinctive innovation ecosystem that enables them to constantly upgrade their knowledge and experience. Today, however, they have no viable, short-term professional opportunities to place their talents in the service of US national security. Moreover, even when the government can attract these workers, those who choose to stay often struggle to keep abreast of fast-moving technology developments in the private sector, which is the center of cyber innovation. This places our government in a position of structural disadvantage. We propose here an approach to overcome and reverse that.

A new, nimble, and innovative not-for-profit Cyber Workforce Incubator would allow the West Coast's best technologists to work on national security challenges without degrading their cutting-edge technical skills or requiring them to give up their livelihoods, work cultures, or social networks. 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.

# Introduction

Today, the private sector dominates technology innovation in cybersecurity and data science. Thanks to the rapid growth of private-sector technology companies, large segments of the nation's best technology talent are building commercial products and services in established companies and startups, especially on the West Coast. As primary drivers of global technology innovation, these companies are combining speed, agility, ingenuity, creativity, and the profit motive to fundamentally change how humans and machines interact everywhere on the planet. The men and women who work in these companies are driving the future of technology and in the process profoundly shaping how and where the work of cyber innovation takes place.

The United States does not currently have an agile way to leverage the talent of these cybersecurity operators to solve tough, often classified, government cybersecurity problems. As a result, the government is also falling behind in its efforts to create a more resilient federal cybersecurity infrastructure. A not-for-profit Cybersecurity Workforce Incubator (CWI) will help address this problem by providing a low-risk, high-impact, and organizationally proven way to get top West Coast technologists focused on critical mission work. Such an organization would also serve as a unique example of government workforce innovation, as it will draw features from private-sector startups — such as team-building, a risk mindset, and innovation culture — and put them in the service of the government.[1]

# The Cybersecurity Workforce Gap

The United States cybersecurity infrastructure — particularly US Cyber Command (CYBERCOM), the Military cybersecurity components, and the Department of Homeland Security (DHS) — struggle to recruit private-sector talent into the federal government. The Department of Defense (DOD) has 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.[2] In 2015, Admiral Mike Rogers said that CYBERCOM was "already hard pressed" to find qualified candidates to fill its 133 Cyber Mission Force teams.[3] As of January 2017, CYBERCOM is reported to have 123 teams, with only 27 operating at full capacity.[4] These capacity problems are not limited to the military; before the Trump Administration implemented a hiring freeze on the federal government, more than 1,000 federal cybersecurity jobs remained unfilled.[5]

In 2013, the DOD released its Cyberspace Workforce Strategy, which recognized that the Department faces "fierce competition" in the labor market and must position itself as an "employer of choice" using a variety of tactics. One strategy the report recommended is to create more transition opportunities "between and within military and civilian service."[6] However, this strategy focused on retaining existing service members, rather than engaging the private-sector talent pool.

One reason that the federal government has struggled to recruit top cybersecurity talent is the East Coast-West Coast divide. Today, when the US Government wishes to solve classified national security problems, it almost exclusively draws upon East Coast-based government employees or contractors. With rare exceptions, the West Coast's private-sector cybersecurity technologists have displayed little interest in working for the national security community. While senior cybersecurity leaders recognize the need for this talent, many bureaucratic and cultural factors mute and dull the call to service, including:

- Lengthy, cumbersome clearance processes that often cause applicants to lose interest;
- Risk-averse government managers who sacrifice innovation to professional advancement;
- The cost and burden of relocating from preferred geographic technology hubs like Boston, Austin and, most importantly, Silicon Valley to the Greater Washington, DC area;
- Security policies that can unnecessarily isolate employees from their social and professional networks;

- Lengthy, bureaucratic decisionmaking that can delay testing and implementation of new technology solutions;
- HR policies and institutions that undermine short-term, meaningful work; and
- Poor work environments in aging government buildings.

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 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.

# Solution: A Cyber Workforce Incubator

To harness West Coast cyber technology talent and tap directly into the innovation ecosystem in which it grows, the US Government would benefit from a not-for-profit [501(c)(3)], San Francisco Bay Area-based Cyber Workforce Incubator that provides West Coast technologists with the unique ability to work with select personnel on important, classified national security challenges.

## HOW IT WOULD WORK

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 removing the need for the government to make difficult and highly disruptive internal changes to attract top technical talent, CWI would help reduce the friction that prevents skilled private-sector technologists from working on mission-critical challenges. Several underlying assumptions make CWI uniquely attractive:

1. Participants will not have to relocate;
2. Their work is by definition temporary; and
3. Equipped with a new set of skills, they will return after one or two years to the private sector, where they can continue to work on innovative technologies that will help the US Government in the long run.

Once fully set up, CWI would be housed in its own physical location with both unclassified and classified (SCIF) workspaces. CWI would need authority and support to conduct fast-track clearance reviews—modeled on the Intelligence Community's ability to provide rapid, temporary clearances to VIPs for forums like the Enduring Security Framework—so that CWI's technologists can get a high-level clearance in a matter of 6-12 months.[7] CWI would select incubator participants well before the start of the program to ensure they are able to complete their full clearance process.

By serving the defense, intelligence, and homeland security partners through this new model for public-private engagement, CWI would provide the following significant benefits:

## Relationship To Existing Programs

Although CWI is fundamentally a workforce development innovation, it is not a high-risk endeavor because it borrows from techniques and approaches that are already proven by other organizations that work closely with US cybersecurity communities, including:

**DARPA**

The DARPA innovation model features project managers who come from industry and academia for short periods of time to work on hard, future-oriented technical challenges. When a new manager at DARPA receives an identification badge on Day 1, it also prominently features their last day of work two years later. The message is clear: innovation requires a period of intense focus and appropriate risk, not years of incremental change. **Key Lesson:** Borrowing from the DARPA model, CWI will offer temporary one- or two-year positions to highly talented individuals who wish to work on cybersecurity technology challenges for a set time period.

**IN-Q-TEL**

This not-for-profit venture capital firm has successfully identified promising early-stage technologies for the intelligence community because it stands between the public and private

*continued on page 6*

*Relationship to Existing Programs*
*continued from page 5*

sectors, allowing it to understand what the intelligence community actually needs and translate those needs to start-up companies in clear language. In-Q-Tel solves an important technology innovation supply-chain problem that acquisitions officers cannot fix themselves.

**Key Lesson:** Following the In-Q-Tel model, CWI will be a not-for-profit that will be funded both through the US Government and partnerships with corporations looking for CWI graduates. CWI will also build long-term relationships with government officials who need assistance solving time-sensitive, mission-critical technology challenges.

**Y COMBINATOR**

A funder and seed accelerator, Y Combinator provides the infrastructure, training, and resources necessary for young talent to set up their own technology companies. This firm's approach illustrates a powerful model for addressing the challenge of scouting and developing top technology talent.

**Key Lesson:** Using Y Combinator's example, CWI will foster team-based work, mentor-mentee relationships, and talent development, so that CWI "graduates" return to the workforce with a sophisticated set of marketable skills and experiences.

- Tiger teams capable of working on mission-critical, classified technology challenges;
- Technologists who are able to bring cutting-edge hardware and software solutions to intractable national security technical challenges and who can remain technically current during their CWI service;
- An elite group of private-sector technologists who may wish to work for the government for longer periods of time;
- An engine for improving the US Government's relationships and brand within Silicon Valley and other technology hubs;
- Knowledge and skill transfer from CWI participants to US government personnel, and vice versa;
- An intermediary organization that helps the US Government to better engage with West Coast start-ups and technology companies;
- A reputation for applying ingenious solutions to intractable workforce challenges that are endemic to the military and to civilian government operations;
- Hundreds of innovators and entrepreneurs who will "graduate" from CWI and go on to build hardware and software that benefit the Department of Defense and secure the nation; and
- A workforce innovation that complements and reinforces other types of technology outreach efforts, such as In-Q-Tel and DIUx.

## RELATIONSHIP TO OTHER INITIATIVES

To our knowledge, there are no existing workforce programs that systematically allow the government to leverage top private-sector cybersecurity talent to work directly on actual national security challenges without also forcing those individuals to leave the West Coast and take 'permanent' government, military, or contractor jobs.

Consequently, CWI complements, but does not replicate, several existing efforts to drive workforce improvements in the US Government. For example, the Cyber Mission Force will come online in the medium term and will provide the DOD with cutting-edge

cyber operators from within the four military services. The US Digital Service, soon to be followed by the recently initiated Defense Digital Service, is already demonstrating promise as it matches private-sector technical talent to the general IT needs (e.g., website design) for US agencies. 18F, a federal digital consultancy run out of the General Services Administration (GSA), has already demonstrated value by building modern digital services for federal agencies; 18F successfully operates on a contracting model that allows technologists to work on government projects from offices across the country.[8] DIUx, a DOD initiative that helps bridge the military with the private sector, and In-Q-Tel, a venture capital firm focused on identifying and investing in technologies that will benefit US national security, are well placed to identify and invest in technology for the defense and intelligence communities, respectively.[9]

CWI also complements, but does not replace or overlap traditional military, intelligence, and homeland security agency procurement of academic and private-sector company services. Academics provide deep expertise to the government, but they rarely work on mission-critical projects because they usually lack appropriate clearances, work according to a slower tempo, and must balance their work for the government with other university priorities. Private-sector contractors provide the government with a diversity of unclassified and classified technical services, including some that are core to mission. In many cases, the individuals performing these services are former military or intelligence agency individuals who have spent their whole careers as private-sector government contractors. These employees are often quite effective at solving known technical problems that can be described in a statement of work, but struggle to help the government apply cutting-edge cybersecurity knowledge to ambiguous problems that are hard to disaggregate and even harder to solve. Furthermore, contractors will always have incentives to solve technical problems in ways that generate more government contracting work for their companies.

*Relationship to Existing Programs*
*continued from page 6*

**UNITED STATES DIGITAL SERVICE (USDS)**

The US Digital Service and Innovation Fellowships bring technological talent to the government. Currently in its second year, USDS has been tremendously successful at addressing conventional government IT problems, such as open government, record keeping, website design, and workforce efficiency.

**Key Lesson:** CWI can learn from the US Digital Service's ability to quickly assemble private-sector technologists into teams that are able to effectively solve complex, unclassified technology challenges.

**DIUx**

DIUx operates in and around major technology hubs and works to identify and pilot cutting-edge technologies that meet government mission needs. Today, DIUx is focused on building relationships with technology companies, funding pilots, and facilitating the procurement of promising, quickly deployable technologies.

**Key Lesson:** CWI can leverage the relationships that DIUx is building with technology companies, providing them with a new way to develop and retain their talent. CWI might also benefit from DIUx's physical space at Moffett Field.

# 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 accelerates and the gap between the private- and public-sector 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. Today, some of world's greatest technological talent resides within the West Coast's private-sector innovation ecosystem. CWI will, for the first time, make this talent available to address classified challenges while also conferring long-term strategic benefits to the US Government.

1 This paper focuses primarily on the role a cybersecurity incubator could play in assisting the Department of Defense, Department of Homeland Security, and related intelligence agencies in solving key cybersecurity problems. We encourage the adaption of this policy concept to other agencies' needs — for cybersecurity and beyond.
2 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
3 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." 4 March 2015. http://docs.house.gov/meetings/AS/AS26/20150304/103093/HHRG-114-AS26-Wstate-RogersM-20150304.pdf
4 Maucione, Scott. "CYBERCOM's New Buying Power Now Closer to Reality." Federal News Radio, 23 January 2017. http://federalnewsradio.com/acquisition/2017/01/cybercoms-new-buying-power-now-closer-reality/
5 Sternstein, Aliya. "Trump's hiring freeze blunts rush to recruit cybersecurity talent." Christian Science Monitor Passcode, 25 January 2017. http://www.csmonitor.com/World/Passcode/2017/0125/Trump-s-hiring-freeze-blunts-rush-to-recruit-cybersecurity-talent
6 United States. Department of Defense. "Cyberspace Workforce Strategy." 3 December 2013. http://dodciCWIo.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed(final).pdf
7 The National Guard may also be able to facilitate fast-track clearance reviews through its use of the Defense Support of Civil Authorities (DSCA).
8 News Staff. "What is 18F?" Government Technology, 8 August 2016. http://www.govtech.com/What-is-18F.html
9 Other current efforts, such as the DOD's Force of the Future or the Loaned Executive Program at DHS, may also be instructive.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

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