**REQUEST FOR INFORMATION RESPONSE**

**ONCD Request for Information on Cyber Workforce, Training, and Education**

**November 3, 2022**

## I. INTRODUCTION

In response to the Office of the National Cyber Director's (ONCD) request for insight and expertise on Cyber Workforce, Training, and Education (RFI), CrowdStrike offers the following views.

We welcome the opportunity to provide input on these essential issues and to collaborate with government stakeholders on workforce and talent in the cyber field. The "areas" and "sub-areas" identified in the RFI align with our views about the core issues and opportunities in this space. There are actions that private companies and the government are already taking that can be amplified, along with new creative solutions, to make progress towards both increasing the number of people in the cyber workforce and ensuring the cyber workforce is diverse and inclusive.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

## II. COMMENTS

CrowdStrike hires thousands of cybersecurity professionals per year. Notwithstanding having a visible brand, we are not immune from some of the same workforce challenges and pressures faced by other organizations, including government entities. As such, we have launched a number of initiatives to strengthen our workforce posture – some of which we describe below. We hope details about these efforts can help inform the ONCD as it tackles this challenge at a national level.

## A. Cyber Workforce

Building and retaining a talented cyber workforce goes well beyond hiring experienced talent and requires a comprehensive approach. CrowdStrike's programs that are most relevant to the RFI's cyber workforce section include our: remote-first policy; Return to Work program; military and veterans partnerships; internship program; and employee retention efforts.

*Remote-first culture*. From CrowdStrike's inception over a decade ago, we have placed an emphasis on hiring and maintaining the best talent in the field and that starts with attracting and growing a diverse cyber talent pool. Being a remote-first company ensures CrowdStrike can hire the best people – regardless of their geographic location. Among other benefits, this permits people with family or caretaking obligations to contribute to our mission. While a remote-first environment is not feasible for all parts of the U.S. government, widening the geographic scope of candidates where feasible merits serious consideration. Where fully remote roles are not practical, hybrid remote roles can offer additional flexibility and attract talent who would not have been available or otherwise interested.

*Return to work*. This program specifically promotes consideration of candidates that have gaps in their work histories, such as caretakers or those who have changed careers. We have found that this program attracts people from communities that are underrepresented in cybersecurity and provides them with opportunities to join the cyber workforce. It also presents opportunities for reskilling or upskilling; and improving learning pathways to careers in cybersecurity, including internships and apprenticeships. CrowdStrike has had overwhelming success with this program, and would suggest that the ONCD examine similar efforts within government contexts.

*Military and Veterans program*s. Veterans form a key part of the cybersecurity workforce and CrowdStrike is proud that approximately 6% of our employees have a military service background. CrowdStrike has partnered with American Corporate Partners (ACP), an organization that provides U.S. veterans with career guidance as they transition back to civilian life, addressing the challenge of enabling veterans to more easily transition into the cyber workforce. With the help of professional mentor volunteers, ACP's program offers transitioning veterans important tools for long-term career development and the chance to create a better post-service life. CrowdStrike also partners with Hire Military which helps veterans find careers after retirement and also offers internship opportunities. Additionally, CrowdStrike is a partner with Operation Motorsport which finds educational, mentorship, and industry opportunities for medically retiring Service Members that aid their recovery

and rehabilitation. The U.S. government has many programs aimed to transition veterans to civilian life, and the ONCD could survey those programs and see which ones could feature cyber positions at the forefront of the program. Targeted and dedicated programs for veterans is an effective and proven pathway to widen the aperture of available candidates.

*Internships*. As the cyber workforce currently stands, organizations cannot hire only existing cyber professionals with experience - organizations must recruit earlier in people's careers to boost diversity and to educate those who traditionally would not have thought of a career in cybersecurity. CrowdStrike's Internship program has been highly effective in providing university students a pathway into a career in cybersecurity. Our Internship program is dedicated to attracting and cultivating the next generation of talent in virtually every field. Our program offers paid positions that allow college students and recent graduates to gain real-world experience and develop essential skills from some of the most insightful and accomplished professionals in the field. This program has had an impact on our workforce at large - in this current class, we had over 250 interns, 40% of which are women, and this has led to 70% of interns being converted into full time professional roles across multiple functions at the company.

*Retention*. CrowdStrike has both formal and informal programs designed to retain talented cyber professionals. Burnout is a significant problem in the field, particularly among incident responders and others with 24x7, high-operational-tempo responsibilities. Further, insufficient retention magnifies recruitment challenges, particularly for mid- and senior-level roles. An example of a formal program we use is CrowdStrike Alignment Reviews (CARs). This effort is designed to allow for managers and employees to easily discuss performance and developmental goals and how to achieve success in their roles. Whatever the specific mechanism(s), we strongly recommend organizations adopt a structured approach to facilitating conversations around performance and career development or advancement.

### B. Diversity, Equity, Inclusion, and Accessibility (DEIA)

CrowdStrike's approach to DEIA includes multiple lines of effort. From our point of view the most impactful elements include the following:

*Recruitment*. With significant effort and experimentation, we are finding success with two key initiatives to broaden the talent pool:

- *Position language and characterization*. We have worked to reduce jargon and inscrutable language in our position descriptions, as well as eliminating unnecessary requirements. Our Human Resource teams continue to identify best practices, but

several departments have already reported stronger outcomes. For example, CrowdStrike's threat intelligence team has grown to be comprised of 35% women since the language on job postings has been updated. We believe much of the team's success is due to their ability to attract a broader set of candidates.

- *Diversity sourcers*. CrowdStrike has invested in diversity sourcers whose sole focus is to bring diverse candidates into our candidate pools. They focus on recruiting through specific job boards which target under-represented minority groups, or from certain universities or career fairs which are also focused on diversity. Diversity sourcers currently make up roughly a third of our sourcing team.

*Training*. Further, CrowdStrike has implemented unconscious bias training for recruiters and hiring managers. Beyond improvements in the hiring process itself, our hope is that the training carries over to help our staff be more inclusive managers, run inclusive meetings, and be thoughtful of inclusivity in everyday process and practice. The U.S. government has similar training programs. The ONCD's national strategy could amplify unconscious bias programs that are showing positive results.

*Culture*. CrowdStrike is a mission-focused organization: we feel passionately that our core responsibility is to stop breaches. Every day, we prevent foreign nation-state threat actors, as well as criminal groups and hacktivists, from attacking customers and others throughout the ecosystem. In addition to government organizations and key critical infrastructure organizations, we regularly defend NGOs, political or policy organizations, persecuted religious or minority rights advocacy organizations, and other sensitive or marginalized groups. All culture at the company ultimately flows from prioritization of this mission. Government organizations and others—from nonprofits to large businesses—can benefit from emphasizing how good cybersecurity practices contribute to their own missions.

Further, as a team, we strive to provide tools that help employees connect with each other, celebrate common causes, and share ideas, perspectives, experiences, and approaches. Through employee resource groups, internal development programs, allyship training, speaker series, networking opportunities, and more, employees can come together to create a workplace that reflects the diverse communities around us. CrowdStrike aims to create the space for open conversations.

### C. Training, Education, Awareness

CrowdStrike is examining ways to reach individuals earlier in their education careers. More outreach to high school and middle school students will help students envision a career in cybersecurity, build relevant skills, and see the potential to join the cyber workforce.

Development of talent at the earliest career phases can help grow a diverse cyber workforce. CrowdStrike mainly facilitates this through our broader internship program. Our goal is to make a career in cyber an enticing and approachable opportunity for more postsecondary students. We seek to provide participants the opportunity to work on meaningful and valuable assignments that support our mission to make the digital world a safer place to live and work. Our hope is by assigning interns meaningful projects that make a difference, and exposing them to different teams, they come away with a positive experience that translates to a career in cyber.

Additionally, CrowdStrike established its NextGen Scholarship Program to support the development of the next generation of talent and leadership in cybersecurity and artificial intelligence (AI). NextGen Scholarships provide financial assistance to select undergraduate and graduate students studying cybersecurity and/or AI. Scholarship applicants are evaluated on a range of criteria and if selected, awarded $10,000 to help fund their educational pursuits.

From exploratory conversations, we have found that some prospective cyber professionals have difficulty envisioning career pathways in cybersecurity. Part of this challenge is that the field evolves quickly. Another issue is clearly communicating opportunities for less-technical entrants. CrowdStrike is always working on building narratives that show different career paths such as engineering, sales, customer support, and intelligence so individuals interested in cybersecurity can develop a better understanding of paths outside of purely technical roles. We believe there are many ways one can contribute to the cause of stopping breaches. The ONCD could expand efforts along these lines. Additionally, we recommend the ONCD continue the approach of evaluating the whole lifecycle of careers in cybersecurity when drafting the national strategy.

Beyond explicit steps to build and strengthen the cybersecurity workforce, we encourage the ONCD to drive conversations about alternate approaches to strengthening security posture. Organizations should periodically reassess their needs, and determine whether emerging solutions may drive better security outcomes. For example, a senior-level risk manager working with the support of a Managed Security Service Provider (MSSP) might be able to do the work of a cybersecurity-focused person on-site. (Or, a mid-level cybersecurity professional augmented by an MSSP might in some contexts be a suitable substitute for a more senior-level professional.) More broadly, reimagining roles within the broader risk, compliance, security, and cybersecurity space may create opportunities for additional candidates. But these tradeoffs can operate differently within different types or

sizes of organizations. Continued experimentation and documentation of success stories will help.

## III. CONCLUSION

The ONCD's RFI on cyber workforce represents a desire to address a complex problem. This RFI is a meaningful continuation of the efforts outlined at the Cyber Workforce and Education Summit in July 2022, in which we were delighted to participate. As the drafting of the national strategy on workforce continues, we encourage continued engagement with stakeholders. CrowdStrike will continue to support ongoing initiatives. Thank you for your consideration.

## IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance, and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

## V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

**J.C. Herrera**
Chief Human Resources Officer

**Drew Bagley CIPP/E**
VP & Counsel, Privacy and Cyber Policy

Email: policy@crowdstrike.com

***