ASPEN TECH POLICY HUB

aspen institute

Dear Office of the National Cyber Director (ONCD),

The Aspen Institute's Tech Policy Hub – a component of Aspen Digital – is an incubator training cybersecurity professionals and other technologists how to get involved in policy. We have now trained nearly 200 technologists. Many of our alumni now work in the government on cybersecurity issues, including at the White House and the Cybersecurity & Infrastructure Security Agency. We also regularly author reports on Diversity, Equity, and Inclusion (DEI) issues, including on cybersecurity and climate change.

In the below short memo, we propose:

- (Areas 1 and 2) That ONCD should take concrete actions to improve its DEIA work in cybersecurity recruitment, hiring, career development, and retention. For instance, ONCD should:
    - Rewrite federal job descriptions to remove jargon;
    - Reconsider whether the current criminal background check process is unfairly excluding candidates for federal positions;
    - Work with the private sector to improve their DEIA practices; and
    - Study effective DEIA mentorship models.
- (Area 3) That ONCD should give more emphasis to nontraditional pathways to federal cybersecurity jobs, such as certification programs;
- (Area 3) That ONCD should create pathways for new and existing cybersecurity professionals in government to receive policy training; and
- (Area 3) That ONCD should also consider the importance of training policy professionals to better understand cybersecurity.

Thank you for your consideration and work on these important issues.

Betsy Cooper, Director
Mai Sistla, Deputy Director

Aspen Tech Policy Hub
The Aspen Institute
aspentechpolicyhub@aspeninstitute.org

—----------

AREA 1: CYBER WORKFORCE AND AREA 2: DIVERSITY, EQUITY, INCLUSION, AND ACCESSIBILITY (DEIA)

In 2020 and 2021, Aspen Digital and the Aspen Tech Policy Hub – with support from the Hewlett Foundation and convener Camille Stewart Gloster, now Deputy National Cyber Director at ONCD – hosted two workshops on diversity, equity, and inclusion (DEI) in cybersecurity with an intergenerational, multidisciplinary, and multicultural group of cybersecurity professionals from across the private and public sector. In a subsequent report by lead authors Mai Sistla and Meha Ahluwalia, the group proposed a number of priority approaches for achieving better DEI in cybersecurity.

The full report can be found here. The following summarizes key recommendations that ONCD can deploy to better incorporate DEIA into its cybersecurity workforce efforts. More details on each of these points can be found in the report.

Subarea A: Recruitment and Hiring

To attract and grow a diverse cyber pool, ONCD should establish a group of pro bono experts to help federal government cybersecurity employers to rewrite their job descriptions without jargon and focus on the skills required. Currently, many cybersecurity job descriptions are filled with industry-specific terms that can be confusing even to professionals within the field. Moreover, existing job descriptions rarely include broader skill sets like problem solving and critical thinking that are essential for successful employees. In order to recruit a more diverse workforce, a group of pro bono cybersecurity and human resources experts should provide guidance for cybersecurity employers to rewrite their job descriptions. These experts could also publish best practice guides for writing job descriptions and recruiting diverse talent.

To attract people from communities that are underrepresented in cybersecurity, ONCD should work with OPM to reconsider whether the current criminal background check process is appropriate, fair, and equitable. Cybersecurity jobs are often subject to strenuous background checks which can impede diverse candidates from completing the hiring process. A task force should reconsider whether background check requirements can be eliminated or streamlined, so as to reduce biases in the hiring process caused by the disparate impact of law enforcement and the broader criminal justice system on persons of color.

To attract and grow a diverse cyber pool, ONCD should encourage companies to collect and share anonymous data about the diversity of characteristics that prove useful for successful hiring of cybersecurity jobs, and should itself collect such data on federal government hires. It is often difficult to identify characteristics of successful job hires, which makes it difficult to replicate success in making diverse hires. A public data repository containing example profiles of successful hires from a wide diversity of experiential, educational, and cultural backgrounds could help hiring managers adjust job requirements and hone in on the skills new hires actually need. ONCD could convene a group of companies to encourage such information-sharing, and/or could host such a public data repository itself.

Subarea B: Career Development and Retention

To assist in the retention of cyber talent, ONCD should encourage private sector DEIA work by establishing a task force to track C-suite executives' commitments to DEIA initiatives related to cybersecurity professionals within companies. Over the past year, numerous technology and cybersecurity CEOs have made public statements regarding improving DEI within their organizations. Yet, there are no real mechanisms to hold CEOs accountable for their commitments. A publicly-available tracking system creates some accountability and may incentivize these companies to make progress on their specific DEIA goals. A task force of DEIA experts could track C-suite executive commitments to improving diversity and inclusion within their companies and look into whether their companies actually achieve their DEIA goals over time.

To assist in the retention of cyber talent, ONCD should develop a coalition to determine DEIA mentorship models for cybersecurity organizations of all types. Mentorship models are a common tool for fostering DEIA in organizations. However, there is little data on what types of mentorship models work in the cybersecurity space, and whether mentorship models need to be tailored to different types of organizations. A coalition of experts across industry, academia, non-profit organizations, and government could publish a "best practices" guide to determine the most effective DEIA mentorship models for different types of organizations.

Subarea C: Data

Please see point 1 under Subarea A, which speaks to data collection on hiring practices. In addition, we note that adequate data collection will be extremely important to achieve the other goals noted above.

AREA 3.A: TRAINING, EDUCATION, AWARENESS: TRAINING AND POSTSECONDARY EDUCATION

Training Outside Traditional Education Pathways

First, we note that this section of the Request for Information focuses primarily on traditional schooling paths to cybersecurity jobs: post-secondary education and K-12 education. However, increasingly there are other paths to working in cybersecurity, including certifications and training programs such as the one we run at the Aspen Tech Policy Hub. These programs are extremely important in enabling underrepresented communities to join the cyber workforce.

In particular, our DEI in Cybersecurity report recommends that ONCD organize a coalition to assess the value of certifications in developing quality candidates for cybersecurity jobs. Over the past decade, numerous cybersecurity certification programs have emerged in attempts to close the cybersecurity skills gap and allow for non-traditional candidates to enter the field. However, there is little evidence of the efficacy of these programs in recruiting high quality and diverse cybersecurity professionals. Moreover, there are barriers associated with their costs. A

coalition should drive research to assess the efficacy of these certification programs across the field and use this data to influence the industry on its continuing use of certification to evaluate candidates.

Importance of Policy Training

Second, in thinking about the skills that effective cybersecurity professionals need to do their work, especially in the federal government, we recommend that ONCD consider policy training an essential part of that work. Problems that seem to be about technology or cybersecurity often end up being about policy. For instance, two of our former fellows sought to improve the Department of Defense's Vulnerability Disclosure Programs. They uncovered that there were no technical obstacles to such an expansion, but that the Secretary of Defense would need to sign off on a policy change to implement the expansion. Using the skills that the fellows gained in our Aspen Tech Policy Hub fellowship, they succeeded in getting the policy changed. As noted earlier, we now have a number of alumni in cybersecurity roles in the federal government.

Too often we fail to set government leaders up for success because we assume that the only skills they need are technical. Successful federal government employees also need to be able to identify policy obstacles to their work and have the skills to navigate policy change. We hope ONCD considers this skillset as an essential element in preparing new government employees for cybersecurity roles. The Aspen Tech Policy Hub would be delighted to talk with ONCD about how we can work together to scale policy training for cybersecurity professionals in and entering government.

Importance of Training Policymakers on Cybersecurity

Finally, we too often also assume that the burden in establishing new skills should be placed on the cybersecurity employees. However, one reason that cybersecurity employees struggle to accomplish their goals is that the policymakers who need to approve changes or who control the purse strings often do not understand cybersecurity in the first place. ONCD should invest in cybersecurity training programs to train policymakers on the essentials of cybersecurity. The Aspen Tech Policy Hub is considering future opportunities to expand training in this area.