CISA
CYBERSECURITY
ADVISORY
COMMITTEE

REPORT TO THE CISA DIRECTOR

Transforming the Cyber Workforce

June 22, 2022

Introduction:

The Transforming the Cyber Workforce Subcommittee has been asked to develop strategic recommendations to identify and cultivate the best pipelines for talent, expand all forms of diversity, and develop retention efforts to keep CISA's best people. Additionally, the subcommittee has been tasked with identifying creative ways to develop a better-informed digital workforce and inspire the next generation of cyber talent through education of "K through Gray" communities.

The recommendations outlined below focus on (1) Addressing CISA's Workforce Challenges and (2) Building the National Cyber Workforce.

Findings:

The outlined recommendations are informed by meetings which assessed the current state of hiring and onboarding within the agency and the Federal Government to close talent gaps across leadership and rank-and-file employees. The recommendations are also informed by input from industry leaders on innovative approaches to enhance the cyber talent pipeline and mobilize tech talent for the public sector.

Many public and private entities have provided recommendations to address our nation's cybersecurity challenges, but only modest action has been taken. As such, CISA must develop clear benchmarks, metrics, and milestones to track progress and drive traction. Following this initial tranche of recommendations, CISA must develop clear internal Key Performance Indicators (KPIs) to demonstrate progress on the recommended actions over the next 6-18 months. CSAC will also develop KPIs to hold CISA accountable over the same period.

The Office of the National Cyber Director is developing a broader, interagency national cyber workforce strategy that will include CISA. The outlined recommendations align with their initial thinking. The recommendations work to address the identified urgent gaps in CISA's and the nation's mission-critical cybersecurity workforce and promote opportunities for intervention and improvement.

Given CISA's statutory authorities, CSAC would like CISA to identify the recommendation on which they are able to act, and the recommendations that require additional legislation by Congress.

Recommendations:

- Addressing CISA's Workforce Challenges: The ability to recruit and retain professionals with mission-critical cybersecurity skills will be CISA's ongoing challenge and greatest asset. The federal cyber workforce crisis has been repeatedly addressed in previous reports (e.g., the 2012 Department of Homeland Security CyberSkills Task Force report), yet hundreds of federal cybersecurity positions remain unfilled and nearly 600,000 remain unfilled in the United States alone[i]. Addressing the workforce crisis has become a critical national security threat that will require urgent and effective streamlining of current recruiting and retention processes and a radical expansion of the cybersecurity talent pipeline through innovative partnerships with universities, community colleges, private training organizations, industry, and other federal agencies. As CISA builds its infrastructure and workforce, CISA must (1) prioritize strategic workforce development; (2) dramatically improve its talent acquisition process to be more competitive with the private sector; (3) radically expand recruitment efforts to identify candidates across their professional lifecycle; and (4) leverage talent identification and hiring success through interagency collaboration.

- Prioritize Strategic Workforce Development: CISA requires a comprehensive review of its current workforce and talent needs to ensure that it is properly aligned with the agency's strategic goals and future growth. The review should include assessment of CISA's policies and processes to support hiring for those needs while better competing with the private sector. The CSAC recommends that CISA:
  - Move urgently to hire a Chief People Officer responsible for working with the Director and senior leadership to advance a unified approach to talent acquisition, establish workforce development priorities, and ensure alignment with professional career paths. The CSAC strongly supports CISA's current plans to do this.
  - Ensure that agency managers have the necessary training, dedicated time, and support to focus on strategic needs and gaps in the hiring process, including recruiting to maintain alignment and drive progress against talent goals across the agency.
  - Identify and certify recruiters, with demonstrated expertise in strategic focus areas, to support the agency's broader recruiting efforts for specialized hiring needs.
- Dramatically Improve Hiring Goals and Process: While CISA has made some progress toward improving its talent acquisition process, including the launch of the Cyber Talent Management System, CISA must move with far greater speed and urgency to meet the nation's cybersecurity crisis. The process is lengthy and difficult to navigate both internally and externally, and therefore places CISA at a tremendous disadvantage relative to private sector employers for this critical and highly sought-after talent pool. The CSAC recommends that CISA:
  - Set a goal of 90 days from offer to onboarding for cybersecurity candidates. Currently, this process takes an average of 198 days within the agency[ii].
  - Develop a systemic approach to collecting and analyzing data on candidate pools and hiring processes to benchmark, monitor and improve hiring cycles, using an organizational chart to monitor time to fill, time to hire, source of hire, recruitment funnel effectiveness and diversity of candidate slate metrics.
  - Review hiring goals on a regular basis with senior agency leadership, under the guidance of the Chief People Officer and Chief Human Capital Officer, to ensure they remain aligned with the agency's strategy and needs and are properly directed and budgeted to be competitive with private sector employers.
  - Move away from a rigid, inflexible job classification system to a flexible, adaptable, pool-based talent management approach better aligned with organizational needs and career paths for experienced professionals.
- Radically Expand Recruitment Efforts to Identify Candidates Across Their Professional Lifecycle: In order to close CISA's talent gap, the agency's recruitment efforts must reach a broader array of people across the full spectrum of experience. Current recruitment efforts reach only a small portion of the eligible candidates in the nation, limiting the agency's talent acquisition potential. The CSAC recommends that CISA:
  - Expand the recruiting pool by increasing awareness of open roles for internal CISA candidates to other government employees, industry, academia, and cybersecurity training organizations.
  - Establish a standing working group comprised of leaders in the public and private sectors tasked with highlighting leadership opportunities at CISA, advising on cybersecurity recruiting challenges, and ensuring accountability.
  - Partner with universities, community colleges, industry, relevant non-profits, the hacker community, and CISA's network of partners to establish an expanded internship program. These partnerships

        will identify professionals with mission-critical skills that enables CISA to hire full-time employees from a larger pool of candidates.
        - Conduct a thorough review of the interagency security clearing process to identify paths to streamline and speed up this critical path for CISA candidates. The subcommittee heard consistently that the current, unpredictable suitability process is unnecessarily cumbersome and time-consuming, which is a significant obstacle to hiring.
        - Develop a senior leadership specific hiring strategy that uses all resources at CISA's disposal such as Intergovernmental Personnel Act appointments.
    - Leverage Talent Identification and Hiring Success Through Interagency Collaboration: There are currently a number of efforts underway to drive interagency collaboration. By using the information and best practices already uncovered by this work, the agency will be better informed to shape its own talent acquisition process. The CSAC recommends that CISA:
        - Bolster and amplify these ongoing efforts to identify, share, and employ best practices for hiring in cybersecurity.
        - Support the creation of an interagency authority similar to a detailee program to allow CISA to source cybersecurity talent from other agencies and vice versa.
        - Create an internal recruiting tool (e.g., a "LinkedIn for Cyber Talent") that allows CISA and other agencies to tap cyber-skilled Federal personnel and track retention and attrition across agencies.
        - Empower teams leading ongoing interagency collaboration efforts to act with the support of CISA to simplify the sharing and implementation of best hiring and retention practices.

- Building the National Cyber Workforce: In addition to building its own direct workforce, CISA must play a key role in building out the broader national cybersecurity workforce. The agency's future depends on it. There is a significant gap in availability of skilled cybersecurity professionals compared to the rapidly growing need. This challenge is not new, but it is worsening. In May 2021, there were approximately 465,000 open cyber roles in the United States[iii]. In the last year, this number has grown by 29%, leaving us with just under 600,000 currently open roles[iv]. Additional bodies of work have examined similar recommendations, so the CSAC suggest that CISA amplify select recommendations. The recommendations regarding Building the National Cyber Workforce are built on two pillars: Education and Service.
    - Education: It is still difficult for many people to access the educational resources they need to pursue a career in cybersecurity. There is a need for creative new upskilling, reskilling and pipeline development programs designed to lower the barrier to entry to a career in cybersecurity. The CSAC recommends that CISA:
        - Support the establishment of a virtual National Cyber Academy (e.g., a "West Point for Cyber") with a CISA Cadet track leading to a traditional degree and multi-year commitment to CISA.
        - Partner with universities, community colleges and industry-supported cyber education providers to develop a "CISA-approved degree" that enables CISA to quickly tap from a qualified pool of students and professionals and allows recipients to demonstrate their cyber aptitude.
        - Partner with the private sector in working with academia to develop clear, foundational security training credentials to be required by academic institutions.
        - Unify the many existing youth-oriented cyber programs under a single Junior Cyber Corp umbrella to reach younger cohorts (e.g., K-12) with quality learning opportunities to train the next generation of the cybersecurity workforce and deepen our talent pipeline. Bringing these programs together will simplify the educational experience and help ensure a consistent knowledge baseline for students.
        - Develop cyber competitions using the President's Cup as a model to reach universities, community colleges, and key industry events such as Black Hat.

- Service: Today, there are a limited number of broadly available pathways directly into cybersecurity, and even fewer that serve the public interest and evoke a sense of civic responsibility. The development of opportunities that meet these needs will deepen our national cyber talent pipeline, provide critical resources to those without the expertise or funding to bring these to life on their own, as well as increase public understanding that cybersecurity is a shared responsibility. Additionally, The CSAC recommends that CISA:
  - Establish government-sponsored programs that blend public service and cybersecurity education and support the development of similar programs from non-government, private and non-profit organizations.
  - Partner with members of the Joint Cyber Defense Collaborative (JCDC) Alliance to create a tour-of-duty "Cyber Force" pilot program to bridge urgent CISA talent gaps, upskill CISA's workforce and support the agency's strategic priority of public-private collaboration[v]. JCDC members should loan out top security practitioners/volunteers for a one-to-two-year tour of duty before returning to the private sector as designated CISA Liaisons to facilitate ongoing public-private collaboration such as threat sharing, especially during "Shields Up" initiatives and cybersecurity crises. To further incentivize broad participation in this program, the CSAC recommends that CISA support legislation to offer tax credits and other similar benefits to participating organizations.
  - Build a Peace Corps-like cyber program for college graduates and beyond that incorporates education and service to provide domestic cyber development assistance. This would be a broad-based opportunity for early in career professionals to serve their nation while becoming the foundation for the next generation of the Cybersecurity workforce through the development of skills and experiences in cyber.
  - Track the movement of CyberCorps Scholarship for Service recipients through government agencies and set a CISA-specific goal of capturing 50% of scholarship recipients by 2025.
  - Partner with Teach for America to create a cybersecurity program built on their existing platform to increase access to cyber content in communities across the United States.

[i] *Cybersecurity supply and demand heat map*. Cybersecurity Supply and Demand Heat Map. Retrieved May 18, 2022, from https://www.cyberseek.org/heatmap.html

[ii] Cybersecurity and Infrastructure Security Agency, Aggregated Time to Hire Report. https://www.cisa.gov/hiring-process-faqs.

[iii] Morgan, S. (2021, November 11). *Cybersecurity Jobs Report: 3.5 million openings in 2025*. Cybercrime Magazine. Retrieved May 18, 2022, from https://cybersecurityventures.com/jobs/

[iv] *Cybersecurity supply and demand heat map*. Cybersecurity Supply and Demand Heat Map. Retrieved May 18, 2022, from https://www.cyberseek.org/heatmap.html

[v] Using volunteers to fill the cyber workforce gap is not a new concept. The Homeland Security Act of 2002 authorized DHS Secretary to establish a national technology guard, various states have designated Civilian Cyber Corps, and a similar exchange program was a key Cyberspace Solarium Commission recommendation.