November 1, 2022

RFI Response: Cyber Workforce, Training, and Education
The Office of the National Cyber Director

The Center for Security and Emerging Technology (CSET) offers the following submission for consideration by the Office of the National Cyber Director. CSET is a policy research organization within Georgetown University's Walsh School of Foreign Service. We produce data-driven, nonpartisan research and analysis at the intersection of national security and technology. We have organized our response as general recommendations concerning the topics mentioned in the Request for Information and more specific feedback according to sub-areas. We appreciate the opportunity to offer these comments, and we look forward to continued engagement with the ONCD.

We offer the following recommendations related to specific questions in the RFI:

1. **To conduct effective outreach through educational programming, cybersecurity competitions are an effective yet underutilized tool for students to access and engage with tools and education.** Generally, competitions are an opportunity to incentivize growth, exploration, or knowledge advancement in a particular area.[1] Major national K-12 cybersecurity competitions promote cyber education through competitive challenges and encourage students to pursue extracurricular study of cybersecurity.[2] Students have the opportunity to gain or develop practical and industry-relevant cyber skills outside of the classroom in more realistic situations. Supporting cyber competitions at the K-12 and postsecondary levels can improve learning pathways to careers, increase the number of cyber-related educational programs across higher education, and easily scale outreach initiatives. One known limitation is the availability of trained teachers and mentors. The government's strategy must address a national shortage in qualified and prepared K-12 educators.[3]

2. **Professional certifications are a critical component of the modern cyber skillset and should be incorporated into the national cyber education and training strategy.** On the workforce supply side, certifications allow workers to demonstrate skill competency to potential employers and are often necessary to progress in a cyber career. On the demand side, they serve as important credentials that employers use to assess candidates' qualifications. However, the certification landscape is expansive, training and preparation can be expensive and time-consuming, and job seekers often lack information about which certifications are most valuable to their career development. The strategy should take these factors into account when evaluating certifications

[1] Ali Crawford and Ido Wulkan, "Federal Prize Competitions" (Center for Security and Emerging Technology, November 2021). https://doi.org/10.51593/2021CA002
[2] Kayla Goode, Ali Crawford, and Christopher Back, "U.S. High School Cybersecurity Competitions: Building Cyber Talent Through Extracurricular Activities" (Center for Security and Emerging Technology, July 2022). https://doi.org/10.51593/2021CA012
[3] Computer Science Teachers Association, "The Computer Science Teacher Landscape: Results From a Nationwide Teacher Survey," 2020, https://csteachers.org/documents/en-us/e1d6ac1e-3ae1-4ac1-983d-aaffdacd03c1/1/

as an educational and professional training tool. Future in-depth cyber workforce research is also necessary to examine the role of certifications as hiring credentials and how they can serve as both a bridge into the cyber workforce and a potential barrier to entry.

3. **The forthcoming national strategy should prioritize the funding and promotion of cyber workforce data initiatives that complement existing projects such as CyberSeek.** Comprehensive public-facing cyber workforce data remains elusive, resulting in knowledge gaps on the part of both employers and workers. CyberSeek, a National Initiative for Cybersecurity Education (NICE) initiative in collaboration with Lightcast and CompTIA,[4] is a positive outlier because it is publicly accessible and brings together data about current workforce statistics, job openings, requested credentials, career pathways, skills, and education providers. The recent CHIPS and Science Act of 2022 calls for the establishment of a cyber workforce data initiative led by the National Institute of Standards and Technology (NIST)[5]—which funds CyberSeek—and the National Center for Science and Engineering Statistics (NCSES). CyberSeek can serve as a model for this and future data initiatives, and new cyber workforce data collection should complement CyberSeek's access to private sector data.

4. **The National Centers of Academic Excellence in Cyber (NCAE-C) are leading efforts to produce cyber talent, but there are gaps in opportunity.** NCAE-C institutions are recognized as leaders in promoting higher education in cyber and related fields. Not only does this consortium of NSA-accredited institutions graduate cyber talent, but it also prioritizes additional initiatives such as K-12 curriculum and pathway development, faculty professional development, regional hubs, and scholarship programs. However, in the absence of legislation specifying support, the NCAE-C does not receive annual funding for these broader initiatives. Advocacy with Congress for annual funding will ensure the NCAE-C can continue its efforts to improve education and training, scale effective cyber skills development, and increase faculty skills.

5. **The National Science Foundation's CyberCorps program should expand its efforts to attract, recruit, and retain cyber talent.** Federal cyber scholarship-for-service programs, like the National Science Foundation's CyberCorps, create critical talent pipelines to the federal, state, local, and tribal government cyber workforce. However, this program is not active in all U.S. states and territories, nor is it active at every NCAE-C institution. To improve recruitment, hiring, and retention, the national strategy should encourage and prioritize program expansion while identifying and amplifying others like it. Furthermore, data from this program is not widely public or comprehensive. At a minimum, data should include demographic information, award amount per student, specific fields and programs of study, student types (undergraduate, graduate, etc.), obligation fulfillments, and retention so that better metrics can be developed to assess the

[4] CyberSeek homepage, accessed 21 October 2022, https://www.cyberseek.org/.

[5] U.S. Congress, House, Research and Development, Competition, and Innovation Act of 2022, HR 4346, 117th Cong., 2nd sess, https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf.

value of financial investments in cyber training and education. The Cyber Solarium Commision 2.0 also has made these recommendations.[6]

For more detail, please refer to the following sections based on the RFI topic list:

1. Area: Cyber Workforce

a. Sub-Area: Recruitment and Hiring

v. Enhance opportunities for entry-level members of the cyber workforce, including new entrants and people pursuing reskilling or upskilling

- Certification providers often present entry-level cyber certification training as an opportunity to change careers or break into the cyber workforce from an adjacent field such as Information Technology (IT). The strategy should advocate that potential employers consider relevant certifications alongside traditional degrees or apprenticeship programs as a potential avenue into the cyber workforce.

vii. Identify best practices in implementing skills-based assessment as part of the hiring process

- Employers often require certifications in job descriptions, but there is often also a mismatch between the level of the certification required and the actual job role. Certifications (and their associated examinations) can be an extremely useful proxy for employers trying to assess candidates' skills, but potential employers may screen out qualified candidates because of misaligned certification requirements. We recommend requesting clarification about how employers use certifications to assess skills, whether or not certifications are in fact testing candidates for relevant cyber skills, and how workers can best use certifications to demonstrate their qualifications during the hiring process.

viii. Improve recruitment and hiring in State, Local, Tribal, and Territorial (SLTT) governments:

- Expand the CyberCorps program to ensure that all states within the U.S. have at least one active scholarship program to attract and retain cyber talent at the state, local, tribal, and territorial levels. Expansion should also include additional financial support for institutions to award more scholarships to increase the supply of cyber talent.

1. Area: Cyber Workforce

b. Sub-Area: Career Development and Retention

i. Develop or align to commonly-accepted work roles and related competency areas (model career pathways)

---

[6] Cyber Solarium Commission 2.0, Workforce Development Agenda for the National Cyber Director," p.9, June 2022, https://cybersolarium.org/wp-content/uploads/2022/05/CSC2.0_Report_WorkforceDevelopmentAgenda_FullText.pdf

- Education and training providers should examine their offerings to ensure that they are fully aligned with the latest version of the NICE Framework. Many prominent cyber certification bodies and education providers already align their offerings to the current version of the NICE Framework and provide some guidance on how their certifications can help learners obtain relevant knowledge, skills, and abilities.

ii. Improve education and training and the assessment of cyber knowledge and skills

- Commonly-required certifications can serve as proxies for standardized cyber skills assessments, as certification exam topics are publicly available and the certifying bodies often offer their own official training courses. Aligning employers' needs and job descriptions with the skills tested by required certifications will help clarify certifications' usefulness to job seekers and improve transparency in the hiring process.

iii. Enable career progression within the cyber workforce, in both the public and private sectors

- Employer demand for certifications serves as an incentive for workers to continually refresh their qualifications. Career progression strategic planning should therefore take into account the role that certifications currently play in cyber career progression and whether or not supply and demand patterns for certain in-demand certifications such as CISSP create a bottleneck that prevents qualified candidates from being hired into entry- or mid-level cyber roles.

iv. Ensure opportunities for continuous learning and professional development

- See response above to 1-b-iii.

v. Identify methods that assist in the retention of cyber talent:

- The Department of Defense (DOD) administers a scholarship-for-service program called the Cyber Scholarship Program (CySP) that offers both recruitment and retention scholarships. The latter program awards scholarships to DOD civilians, military officers, and enlisted personnel to pursue Masters and Doctoral degrees in cyber and related fields. The CyberCorps program could expand to offer a similar retention program. Furthermore, the DOD requires colleges and universities participating in the Cyber Scholarship Program (CySP) to submit an annual report that explains their use of CySP funds. In regards to 1-c-ii, this data could be aggregated for public use to attain greater fidelity in cyber workforce-related data.

vi. Improve career development and retention in SLTT governments:

- CyberCorps should be expanded to all 50 states. Each state should have at least one accredited institution to administer scholarships for service to cultivate and attract home-

grown talent. This has the added benefit of diversifying the cyber talent pipeline geographically and socioeconomically. Also see response to 1-b-v.

1. Area: Cyber Workforce
c. Sub-Area: Data

i. Identify promising approaches to attaining greater fidelity in cyber workforce-related data

- CyberSeek is particularly valuable because it aggregates different data sources, providing a more complete picture of the cybersecurity workforce than would otherwise be available from individual organizations. NICE and its collaborators should consider promoting CyberSeek more heavily and encouraging the use of the data for workforce development research.
    - CyberSeek also demonstrates the importance of public-private partnerships in workforce data collection, as detailed data about certifications and other non-degree qualifications are often not publicly accessible or are only published annually via industry surveys such as (ISC)^2's annual workforce study.[7]
- More publicly available data is needed to further cyber workforce research. To supplement demand-side workforce data such as Lightcast's job posting dataset, CSET is currently working on a cyber jobs classification project based on data from LinkedIn that is intended to provide a (supply-side) snapshot of the current cyber workforce. More data—much of it held by private sector organizations or otherwise not currently public—is necessary in order to interrogate current assumptions about the cyber talent gap, answer key workforce development questions, and guide data-driven strategic planning.

ii. Measure the success of efforts to advance diversity and inclusion in the cyber workforce:

- Data from federal cyber scholarship for service programs should be public, comprehensive, and accessible. This data can highlight potential areas where efforts are failing to meet standards or goals for the cyber workforce.

3. Area: Training, Education, Awareness
a. Sub-Area: Training and Postsecondary Education

ii. Identify initiatives and models in training and education that are promising in their potential to scale:

---

[7] "A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)^2 Cybersecurity Workforce Study, 2021," International Information System Security Certification Consortium, 2021, accessed 20 October 2022, https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

- See response below to 3-b-iv.

iii. Identify characteristics and features of programs that have succeeded in scaling effective cybersecurity skills development:

- See response below to 3-b-v.

iv. Make a career in cyber an enticing and approachable opportunity for more postsecondary students:

- Making cyber more approachable as a field of study or career must start at the K-12 level. This includes foundational learning at the K-8 level so that students are interested in and prepared to interact with cyber and computer science topics by the time they reach high school. There is significant overlap between computer science and cybersecurity curriculum which provides important early educational opportunities for those considering future cyber careers

- Adoption of more uniform computer science education policy and curriculum can improve access and opportunity:

    - Presently only half of U.S. high schools offer at least one computer science course and only 27 states require that schools offer relevant coursework.[8] Adoption of curriculum standards and policy is not uniform perpetuating disparities in access. Rural, urban, and schools with high populations of economically disadvantaged students are less likely to offer computer science.

    - For cyber, less than half of a 900-respondent survey report that their district or school offers cybersecurity classes.[9] This survey also reports that providing cybersecurity education through extracurriculars such as clubs, competitions, or camps may spark a deeper interest in pursuing cybersecurity as a career.

vi. Increase the number, rigor, and quality of cyber-related educational programs across higher education

- Each U.S. state should have at least one accredited public four-year and accredited public two-year NCAE-C institution. Accreditation indicates that a particular institution meets rigorous curriculum and faculty standards and is committed to training and preparing the next generation of the cyber workforce.

---

[8] Code.org, "State of Computer Science Education," 2022, https://advocacy.code.org/2022_state_of_cs.pdf

[9] Cyber.org, "The State of Cybersecurity Education in K-12 Schools: Results of a National Survey," June 2020, https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf

- High quality cyber-related educational programs at the K-12 level are already available. Non-profits in this space, such as code.org and teachcyber.org, are doing important work to connect schools, districts, and states with the programming and professional development that schools and teachers need to be equipped and prepared to teach cybersecurity. The challenge to making this content more widely available is an over-saturation of these program offerings in schools coupled with a critical shortage of qualified teachers. Funding for such initiatives, particularly at the state level, should remain a priority.

viii. Increase the skills and number of faculty needed to expand cyber educational programs:

- The workforce strategy should encourage expansion of the CyberCorps program to allow more recipients to return to teaching, given a critical shortage of K-12 computer science teachers.[10] Currently, the CyberCorps program encourages recipients to fulfill workforce obligations in federal, state, local, or tribal government positions. In some cases, recipients are allowed to fulfill their workforce obligations at a U.S. National Laboratory or recipients can return to NCAE-C institutions as instructors or professors. As a further measure the program could expand to include education majors who have the intention to study and teach computer science at the K-12 level.

ix. Identify best practices in ensuring graduates of programs in cybersecurity are fully prepared for work in the field:

- Congressional grants in 2020 and 2021 funded coalitions of NCAE-designated schools that provide resources to the CAE-C community, as well as delivering K-12 cyber educational programming and outreach, career pathway creation, faculty professional development, community and workforce development initiatives, and other programs. Continued support of the NCAE-C will ensure that graduates of programs in cybersecurity are fully prepared for work in the field. This is also a recommendation shared by the Cyber Solarium Commission.[11]

x. Develop and use metrics to assess the value of investments in cyber training and education

- See response to 3-b-viii.

3. Area: Training, Education, Awareness
b. Sub-Area: K-12 Education

[10] Ali Crawford and Ido Wulkan, "Federal Prize Competitions"

[11] Cyber Solarium Commission 2.0, Workforce Development Agenda for the National Cyber Director," p.10, June 2022,

i. Conduct effective outreach at the K-12 level through curricular offerings, extracurricular activities and programs, and summer camps:

- Prioritize the development of education and training program catalogs that align with the NICE Framework, similar to the CSET's AI Education Catalog.[12] This catalog provides easily accessible information on AI-related programs available to students and educators and informs AI education and workforce policy. Other catalogs could be developed to correspond with NICE categories, experience level, source of funding, cost, or type. While the federal government is not in the position to endorse or recommend particular programs or opportunities, it could catalog programs or opportunities that already receive federal funding or sponsorship, like NCAE-C institutions, or highlight pathways or avenues into the federal cyber workforce, like CyberCorps and CySP. Such a resource could help interested Americans navigate the vast array of government programs and pathways to cybersecurity careers.

iii. Better enable high schools and technical education programs to prepare talent for the cyber workforce:

- See response to 3-b-vii.

iv. Identify best practices in connecting skills development and education programs to employer needs:

- Cyber competitions allow students to gain practical and industry-relevant cyber skills in realistic settings outside of the classroom. Some major cyber competitions, like the National Cyber League, structure their challenges to align with the NICE Workforce Framework. This structure allows students to actively demonstrate skills in areas of cybersecurity most desired by industry.

v. Identify initiatives and models in effective skills development and education systems that are promising in their potential to scale:

- National cybersecurity competitions have positively impacted thousands of students and they have several beneficial features. First, major national cyber competitions, like the Air Force Association's CyberPatriot, prioritizes education through its challenges by providing training materials and resources for both students and educators. This accessible format of cybersecurity education can reach more diverse communities, schools, and states that lack access to cybersecurity education or the necessary human capital, like qualified educators. Second, CyberPatriot is funded and sponsored by influential partners such as the Department of Homeland Security, the Northrop

[12] Original CSET Data Visualization, "AI Education Catalog," Center for Security and Emerging Technology, October 2021, https://aieducatalog.cset.tech/

Grumman Foundation, Boeing, and Facebook.[13] Such sponsorship creates legitimacy and national prestige, which is a motivating factor for student and school participation. Third, cyber competitions generally have a low barrier to participation. Moderate hardware and software requirements allow virtually any student or school to participate and engage with cybersecurity topics with little financial or hardware investment.[14]

vii. Increase the number of teachers needed to expand cyber educational programs and equip teachers with professional development opportunities:

- The forthcoming strategy must address a national shortage in qualified and prepared K-12 educators.[15] Previous CSET work found that prior exposure to cybersecurity or computer science education is not necessarily a factor in success in cyber competitions. Instead, access to qualified and invested teachers or mentors is critical. A shortage of K-12 CS teachers may be the biggest hurdle to expanding participation and success in cybersecurity competitions and enabling high schools and technical education programs to prepare cyber talent. Supportive schools and district administrations can also make a difference.

viii. Develop and use metrics to measure the progress of students from education into the workforce:

- Presently, important data on the federal scholarship for service programs is not publicly available. At a minimum, data should include demographic information, award amount per student, specific fields and programs of study, student types (undergraduate, graduate, etc.), obligation fulfillments, and retention. This data would assist in the development of metrics to assess the value of federal financial investments in cyber training and education for the federal cyber workforce.

Thank you for considering our insight on these issues and our recommendations for building and supporting the cyber workforce. If you have any questions or would like clarification on our comments, please contact **Ali Crawford** at ac2213@georgetown.edu and **Jessica Ji** at jj950@georgetown.edu.

---

[13] Air Force Association's CyberPatriot, "Sponsors," accessed 24 October 2022, https://www.uscyberpatriot.org/Pages/About/Sponsors.aspx

[14] Kayla Goode, Ali Crawford, and Christopher Back, "U.S. High School Cybersecurity Competitions: Building Cyber Talent Through Extracurricular Activities"

[15] Computer Science Teachers Association, "The Computer Science Teacher Landscape: Results From a Nationwide Teacher Survey," 2020, https://csteachers.org/documents/en-us/e1d6ac1e-3ae1-4ac1-983d-aaffdacd03c1/1/