The Office of the National Cyber Director Requests Insight and Expertise on Cyber Workforce, Training, and Education: An RFI & Virtual Reverse Stakeholder Day Effort

Introduction

The United States continues to face a significant shortfall in cyber talent, with more than 700,000 open positions in cybersecurity.[1] While the cyber workforce deficit constitutes a near- and long-term threat to our national and economic security, it also represents a significant opportunity to employ a more diverse and inclusive workforce in good-paying jobs that offer tremendous opportunity. To help close this gap and maximize the related employment opportunities, we need to ensure that cyber training, education, and career pathways are available to everyone in our society with the passion and potential to do the work.

Even as we grow and strengthen America's cyber workforce, we must also seek systemic reform in the management of cybersecurity risk. We must pursue a future in which Americans are free to be enriched, empowered, and enlivened by digital connectivity rather than burdened or put at risk by it. Too often the responsibility for managing the risk of this ecosystem has devolved down to individuals, small businesses, and local governments. While we seek to redistribute responsibilities more equitably and effectively—to those better equipped to bear them—we must also prepare all users of our digital ecosystem to secure their digital lives while strengthening cybersecurity across the Nation.

With these goals in mind, the Office of the National Cyber Director (ONCD) is developing—in collaboration with our fellow White House and interagency partners—a national strategy that addresses cyber training and education, digital awareness, and the cyber workforce. To kick off this work, ONCD convened a productive Cyber Workforce and Education Summit at the White House in July 2022 with leaders from government, industry, non-profits, and academia. This Request for Information (RFI) represents a continuation of that effort to gather input from a broad array of stakeholders. Responses to the RFI will also be used to inform future meetings with respondents as described in Phase III, below.

Topic List

To inform the development of this strategy, please consider providing input addressing the potential challenges listed below. Instead of responding to every topic, please focus your input on areas where you have special expertise. We are seeking the most impactful best practice insights and recommendations as to how the Federal government can lead, assist, or encourage other key (whole-of-nation) stakeholders to advance progress in the following areas:

1. Area: Cyber Workforce
    a. Sub-Area: Recruitment and Hiring
        i. Attract and grow a diverse cyber talent pool
        ii. Ensure that everyone, regardless of background, has an opportunity to pursue a career in cyber
        iii. Attract people from communities that are underrepresented in cybersecurity and provide them opportunities to join the cyber workforce
        iv. Enable veterans to more easily transition into the cyber workforce

[1] Cyber Seek, "Cybersecurity Supply/Demand Heat Map," https://www.cyberseek.org/heatmap.html, accessed September 29, 2022.

v. Enhance opportunities for entry-level members of the cyber workforce, including new entrants and people pursuing reskilling or upskilling
vi. Improve learning pathways to careers in cybersecurity, including internships, apprenticeships, co-ops, and other work-based learning opportunities
vii. Identify best practices in implementing skills-based assessment as part of the hiring process
viii. Improve recruitment and hiring in State, Local, Tribal, and Territorial (SLTT) governments

b. Sub-Area: Career Development and Retention
i. Develop or align to commonly-accepted work roles and related competency areas (model career pathways)
ii. Improve education and training and the assessment of cyber knowledge and skills
iii. Enable career progression within the cyber workforce, in both the public and private sectors
iv. Ensure opportunities for continuous learning and professional development
v. Identify methods that assist in the retention of cyber talent
vi. Improve career development and retention in SLTT governments

c. Sub-Area: Data
i. Identify promising approaches to attaining greater fidelity in cyber workforce-related data
ii. Measure the success of efforts to advance diversity and inclusion in the cyber workforce

2. Area: Diversity, Equity, Inclusion, and Accessibility (DEIA)
a. Sub-Area: DEIA in the Cyber Workforce
i. Identify best practices and strategies relating to all topics in paragraph 1. (above) that are uniquely applicable to DEIA and a diverse cyber workforce
ii. Address community-wide challenges, including among underrepresented populations, that may inhibit the development of a diverse cyber workforce

b. Sub-Area: DEIA in Cyber Training, Education, and Awareness
i. Identify best practices and strategies relating to all topics in paragraph 3. (below) that are uniquely applicable to underrepresented populations and to veterans
ii. Address community-wide challenges, including among underrepresented populations, that may inhibit cyber education, training, or awareness efforts

3. Area: Training, Education, Awareness
a. Sub-Area: Training and Postsecondary Education
i. Better enable community colleges to prepare talent for the cyber workforce
ii. Identify initiatives and models in training and education that are promising in their potential to scale
iii. Identify characteristics and features of programs that have succeeded in scaling effective cybersecurity skills development
iv. Make a career in cyber an enticing and approachable opportunity for more postsecondary students

v. Enable learners to overcome cost and other barriers to an education and training in cyber and related fields
vi. Increase the number, rigor, and quality of cyber-related educational programs across higher education
vii. Identify solutions to overcome barriers to expanded offerings, including those due to cost of facilities and equipment
viii. Increase the skills and number of faculty needed to expand cyber educational programs
ix. Identify best practices in ensuring graduates of programs in cybersecurity are fully prepared for work in the field
x. Develop and use metrics to assess the value of investments in cyber training and education

b. Sub-Area: K-12 Education
   i. Conduct effective outreach at the K-12 level through curricular offerings, extracurricular activities and programs, and summer camps
   ii. Enable every American with the passion and potential to envision a career in cybersecurity to join the cyber workforce
   iii. Better enable high schools and technical education programs to prepare talent for the cyber workforce
   iv. Identify best practices in connecting skills development and education programs to employer needs
   v. Identify initiatives and models in effective skills development and education systems that are promising in their potential to scale
   vi. Enable state and local education agencies to overcome cost, policy, infrastructure, and other barriers in providing education in cyber and related fields
   vii. Increase the number of teachers needed to expand cyber educational programs and equip teachers with professional development opportunities
   viii. Develop and use metrics to measure the progress of students from education into the workforce
c. Sub-Area: Digital Awareness and Online Safety
   i. Identify and foster the core skills, knowledge, and lifelong learning opportunities all Americans must have to thrive in our digital ecosystem
   ii. Broaden accessibility to, and engagement with, resources for online safety
   iii. Identify successful examples of programs in cybersecurity, or other fields, where public awareness was effectively raised, leading to improved outcomes
   iv. Identify successful approaches that embed cyber safety and awareness into a variety of experiences where users consume technology

In addition to written responses, we are seeking a limited number of innovative speakers who may present a topic, or topics, from the above list to a body directly involved in the formulation of the strategy, including an interagency committee, an associated workshop, or directly to senior government leaders in ONCD and other relevant government entities.

This RFI is *not for a direct procurement*. However, it seeks public and private sector input as Federal leadership develops its strategy and action plan and undertakes initiatives and pilot efforts to strengthen the nation's cyber workforce.

We very much hope that potential respondents will view this RFI as a true *civic opportunity* to help shape the Government's thinking about the national cyber workforce.

Three-Phase RFI and Reverse Stakeholder Day Approach

For this RFI, the Government intends to engage with interested parties in a three-phase approach:

- Phase I: The Government will distribute this RFI, post it on the White House website, and address questions received from potential respondents.
- Phase II: Interested respondents will submit their written responses to this RFI for consideration by the Government no later than November 3, 2022.
- Phase III: The Government will review RFI inputs received, evaluate them, and potentially select some respondents, chosen based on the level of knowledge and expertise demonstrated within the written RFI, to engage with the RFI project team, the interagency working group, an associated workshop, or senior leaders from ONCD and other relevant government entities. The purpose of these sessions would be to engage in Q&A about the material submitted for Phase II and to engage in a dialogue about how the insights might inform the National Cyber Workforce and Education Strategy or related initiatives.

Additional details about the three phases follow below:

Phase I – Gathering Respondent Questions About this RFI

The Federal government has published this RFI document. We ask that potential respondents (including, but not limited to, industry, non-profit entities, academic institutions, training and certification providers, and consulting firms) review this document and the topics outlined above. Please identify any questions you may have about the context of the Government's request, the processes described, or the numbered topics above, by contacting workforce@ncd.eop.gov by October 12, 2022.

By October 19, 2022, after having processed your questions, the Government will post responses to select questions with the RFI on whitehouse.gov/oncd.

Phase II – Submittal of Responses to the RFI by Interested Respondents

By November 3, 2022, all interested respondents should submit a written RFI response, in MS Word PDF format, summarizing their recommendations as to questions on which they have expertise and insights for the Government (no longer than 10 pages typed size eleven font) to workforce@ncd.eop.gov with the email subject header "Cyber Workforce RFI Response" and your organization's name. Title page, cover letter, table of contents, and appendix are not included within the 10-page limit. In the body of the email, also include contact information for your organization (POC Name, Title, Phone, Email, Organization Name, and Organization Address).

The written RFI response should address ONLY the topics for which the respondent has expertise. Inputs that meet most of the following criteria will be considered most valuable:

- **Easy for Executives to Review and Understand:** Content that is modularly organized and presented in such a fashion that it can be readily lifted (by topic area) and shared with relevant executive stakeholders in an easily consumable format.
- **Expert:** The Government, through this effort, is seeking insights to understand current best practices and approaches applicable to the above topics, as well as new and emerging solutions.
- **Clearly worded/not vague:** Clear, descriptive, and concise language is appreciated. Please avoid generalities and vague statements.
- **Actionable:** Please provide enough high-level detail so that we can understand how to apply the information you provide.
- **Cost Effective & Impactful**: Respondents should consider whether their suggestions have a clear return on investment that can be articulated to secure funding and support.
- **Gordian Knot Solutions and Ideas**: Occasionally, challenges that seem to be intractable and overwhelmingly complex can be resolved with a change in perspective that unlocks hidden opportunities and aligns stakeholder interests. We welcome these ideas as well.

An additional appendix of no more than 5 pages long may be also included. This section should only include additional context about you or your organization. If you elect to put forward speakers for any topic, please provide a relevant bio.

Phase III – Virtual Reverse Stakeholder Day Sessions (An Interactive Individual Dialogue with Selected RFI Respondents)

In this third phase, the Government will review the RFI responses submitted for Phase II. This review will be complete by January 6, 2023. Based on that review, will invite selected RFI respondents to participate in a Virtual Reverse Stakeholder Day (VRSD) event.

The VRSD will be conducted as a series of virtual sessions. These sessions will provide the Government with the opportunity to engage in dialogue directly and individually with selected RFI respondents to ask clarifying questions about their submitted RFI responses. During these sessions the respondents may present or share additional relevant information. Each selected respondent will likely be provided up to 30 minutes for presentation and time for an interactive Q&A with the Government.

Virtual participants at these sessions from the Government may include the RFI team, representatives from interested departments and agencies, attendees at associated workshops, or senior government leaders in ONCD and other relevant government entities. Additionally, the Government may invite proposed speakers to present at future Workforce Summits.

Participation, or lack thereof, in this RFI process, including the Virtual Reverse Stakeholder Day, has no bearing on a party's ability or option to choose to participate in or receive an award for any future solicitation or procurement resulting from this or any other activity.

Timeline Recap:

October 3, 2022: RFI Distributed and Posted by ONCD on whitehouse.gov/oncd

October 12, 2022: Deadline for Questions Submitted by Potential Respondents

October 19, 2022: Government RFI Team Posts Answers to Select Questions

November 3, 2022: Deadline for Respondent Submissions

January 6, 2023: Deadline for RFI Team Review of Submissions; VRSD Invitations to Select Respondents

February 3, 2023: Target for Completion of VRSD Sessions