**U.S. Department of Homeland Security**
Cybersecurity & Infrastructure Security Agency
*Cybersecurity Division*
Washington, DC 20528

**Department of Homeland Security (DHS)**
**Cybersecurity and Infrastructure Security Agency (CISA)**
**Requests Insight on Cyber Training and Education Organization Capabilities:**
**An RFI focused on Growing Cyber Talent in Early Education (K-12)**

*THIS IS A REQUEST FOR INFORMATION ONLY. This notice does not constitute a commitment by the Government. Providing a response to this request will not give any advantage to any organization in any subsequent Notice of Funding Opportunity. All information submitted in response to this announcement is voluntary, and the Government will not pay for information requested nor will it compensate any respondent for any cost incurred in developing information provided to the Government.*

## Introduction

The United States continues to face a significant shortfall in cyber talent, with more than 700,000 open positions in cybersecurity. This deficit constitutes a threat to our national and economic security, but it also represents an opportunity to build a future diverse and inclusive workforce starting in the early years of education. To help close this gap now and into the future, we need to ensure that cyber training, education, and career pathways are available and accessible, and create excitement in our youth to pursue a future career in cybersecurity.

DHS' Cybersecurity Education and Training Assistance Program (CETAP) cooperative agreement is designed to equip K-12 educators with curricula and tools to help their students gain a better understanding of cybersecurity.

The intent of this Request for Information (RFI) is to provide an opportunity for a broad array of cyber education and training providers to share their experiences, challenges, approaches, and other information relevant to teaching the K-12 cyber audience critical cybersecurity topics. Responses to this RFI will help CISA ensure that the CETAP cooperative agreement continues to meet its intentions. It may also influence the future requirements specified in the CETAP Notice of Funding Opportunity (NOFO), with the goal of delivering effective and appropriate cyber education and opportunities to K-12 educators and students.

## Questions

Please provide input to any or all the following questions. Respondents are not required to answer every question. Please focus your input to areas in which your organization has specific experience or expertise.

1. What have you experienced as the biggest challenges in educating the K-12 educators in cybersecurity topics? Please provide examples. What recommendations do you have in overcoming these challenges?
2. What training delivery methods/models do you believe will deliver cybersecurity education that will engage a diverse K-12 student audience and how would you execute across elementary, middle, and high schools?

3. What cybersecurity knowledge/content and skills are critical for preparing K-12 students to meet future employer needs? How do you currently execute or propose building this foundation for the skills needed for elementary, middle and high school students?
4. Provide ideas about how you would appeal to elementary, middle and high school students and encourage them to consider and pursue further cybersecurity education and careers?
5. How do you assess and measure the effectiveness of learning gained from K-12 cyber education programs for elementary, middle, and high school students and educators?
    a. How would you assess student impact across K-12?
    b. How would you assess if educators are using resources in the classroom?
    c. How frequently should learning resources be reviewed/updated?
    d. How would you measure impact across diverse/under resources and underrepresented populations?
6. Please provide the following information about your organization:
    a. Type of Organization: Describe your organization's mission and expertise.
    b. Audiences Served: Describe the current audience served by your organization (e.g., cyber professionals, educators, K-12 students)
    c. Content Offered: If you provide cyber training and education, what is the scope of the cyber content and topics offered?
    d. Methods and Platforms: What are the various methods you use to deliver cyber education and training content? (e.g., K-5, 6-8, 9-12 platforms, presentation style training delivery, labs, virtual environments, videos, games, bootcamps, etc.)
    e. Business Model: How would you define your organization?
    f. Years of Relevant Experience: How many years has your organization been providing cyber and/or K-12 education and training?
    g. Do you serve under-represented populations (e.g., race, gender, socio-economic)? If so, how?

**RFI Response Instructions**

This RFI is not for a direct procurement, however, it seeks public and private sector input to help understand challenges and improvements DHS can make in future grants and cooperative agreements that will improve cyber education for K-12 students. We hope that potential respondents will view this RFI as a civic opportunity to help shape the future of educating our youth and developing the Nation's cyber workforce.
For this RFI, the Government intends to follow this approach:

1. **Posting RFI**

The Government has posted this RFI on Grants.gov. We welcome respondents (including, but not limited to, industry, non-profit entities, academic institutions, training and certification providers, and consulting firms) to review and respond to the questions outlined above.

## 2. Submission of Responses to the RFI by Interested Respondents

By 02/08/2023, all interested respondents should submit a written RFI response, in MS Word PDF format, summarizing their recommendations and input (no longer than 10 pages, typed size eleven font) to education@cisa.dhs.gov with the email subject header "K-12 CETAP 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, please include contact information for your organization (POC Name, Title, Phone, Email, Organization Name, and Organization Address).

Question 6, information about your organization, can be included as an appendix and does not count toward total page count.

The written RFI response should address ONLY the topics for which the respondent has expertise and/or hands on experience.

## 3. RFI Review

The Government will complete its review of the RFI responses by MM/DD. RFI responses will help inform future CETAP requirements and the way DHS fulfills its important mission of equipping K-12 educators with curricula and tools to help their students gain a better understanding of cybersecurity. The Government will not provide answers to any questions submitted in response to this request.

At this time, CISA is not seeking technical or cost estimates. Do not submit any proposal / application in response to this RFI. Only the information requested above will be considered. A Notice of Funding Opportunity (NOFO) will be issued at a later date via Grants.gov that will describe the application requirements and process in full.

**Timeline Recap**

**01/18/2023: RFI Distributed and Posted by CISA on Grants.gov**
**02/08/2023: Deadline for Respondent Submissions**