Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket Number 170627596-7596-01]

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development

AGENCY: National Institute of Standards and Technology (NIST), Department of Commerce.

ACTION: Notice; Request for Information (RFI).

SUMMARY: Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (the "Executive Order"), directs the Secretary of Commerce, in conjunction with the Secretary of Homeland Security, and in consultation with other Federal Departments and Agencies, to assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and provide a report to the President with findings and

recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors. The National Institute of Standards and Technology (NIST) is seeking information on the scope and sufficiency of efforts to educate and train the Nation’s cybersecurity workforce and recommendations for ways to support and improve that workforce in both the public and private sectors.

Responses to this RFI—which will be posted at https://nist.gov/nice/cybersecurityworkforce - will inform the assessment and report of the Secretaries of Commerce and Homeland Security to the President.

DATES: Comments must be received by 5 p.m. Eastern time on [INSERT DATE 21 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Online submissions in electronic form may be sent to cybersecurityworkforce@nist.gov. Please include the subject heading of “Cybersecurity Workforce RFI”. Attachments to electronic comments will be accepted in Microsoft Word or Excel, or Adobe PDF formats only. Written comments may be submitted by mail to Cybersecurity Workforce RFI, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899. Comments containing references, studies, research, and other empirical data that are not widely published should include copies or electronic links of the referenced materials.

All submissions, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. Sensitive personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Submissions will not be edited to remove any identifying or contact information. Do not submit confidential business information, or otherwise sensitive or protected information. Please do not submit additional materials. All comments received in response to this RFI will be made available at https://nist.gov/nice/cybersecurityworkforce without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information). Comments that contain profanity, vulgarity, threats, or other inappropriate language will not be posted or considered.

FOR FURTHER INFORMATION CONTACT: For questions about this RFI, contact: Danielle Santos at 301-975-5048 or Danielle.Santos@nist.gov. Please direct media inquiries to the NIST Public Affairs Office at 301-975-2762 or Jennifer.huergo@nist.gov.

SUPPLEMENTARY INFORMATION: Executive Order 13800 of May 11, 2017, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” directs the Secretary of Commerce and the Secretary of Homeland Security to consult with the Secretaries of Defense, Labor, and Education, the Director of the Office of Management and Budget, and other agencies identified jointly by the Secretary of Commerce and the Secretary of Homeland Security, in conducting an assessment and making recommendations regarding the nation’s cybersecurity workforce.[1] Specifically, these departments are to:

(A) “jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and”

(B) “within 120 days of this order, provide a report to the President through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors.”[2]

The Commerce Department’s National Institute of Standards and Technology is soliciting comments from the public that will aid the Department of Commerce (DOC) and the Department of Homeland Security (DHS) in preparing the assessment and report to the President. For the purposes of this RFI, “education and training” of the American cybersecurity workforce does not include general workforce cybersecurity awareness efforts. Rather, “education and training” refers to curriculum- or practicum-based programs to increase the effectiveness of the workforce addressing cybersecurity challenges. As the Executive Order states, comments are sought on the cybersecurity workforce in both the private and public sectors.

[1] Exec. Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 82 FR 22391 (May 16, 2017).
[2] https://www.federalregister.gov/d/2017-10004

NIST may conduct workshops to gain further public input to the assessment and recommendations regarding the cybersecurity workforce. Information will be made available at https://nist.gov/nice/cybersecurityworkforce

This RFI does not address additional aspects of the cybersecurity workforce that are included in the Executive Order.

Request for Information

Given the nature and importance of the Executive Order, NIST requests information from the public about current, planned, or recommended education and training programs aimed at strengthening the U.S. cybersecurity workforce.

Respondents are encouraged – but are not required – to respond to each question and to present their answers after each question. The following questions cover the major areas about which NIST seeks comment. They are not intended to limit the topics that may be addressed. Respondents may address related topics and may organize their submissions in response to this RFI in any manner. Responses may include estimates; please indicate where the response is an estimate.

All responses that comply with the requirements listed in

the DATES and ADDRESSES sections of this RFI will be considered**.**

Comments containing references, studies, research, and other empirical data that are not widely published should include copies or electronic links of the referenced materials. Do not include in comments or otherwise submit proprietary or confidential information, as all comments received in response to this RFI will be made available publicly at https://nist.gov/nice/cybersecurityworkforce. Comments that contain profanity, vulgarity, threats, or other inappropriate language will not be posted or considered.

General Information

1. Are you involved in cybersecurity workforce education or training (e.g., curriculum-based programs)? If so, in what capacity (including, but not limited to: community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)? Note: Providing detailed information, including your specific affiliation is optional and will be made publicly available. Commenters should not include information they do not wish to be posted (e.g., personal or confidential business information) and are strongly encouraged not to include Personally Identifiable Information in their submissions.

Growing and Sustaining the Nation’s Cybersecurity Workforce

1. What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the **collection, organization, and sharing of information** about cybersecurity education, training, and workforce development programs?

2. Is there sufficient understanding and agreement about **workforce categories, specialty areas, work roles, and knowledge/skills/abilities**?
3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?
4. What **types of knowledge or skills do employers need or value** as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (e.g. energy vs financial sectors)?
5. Which are the **most effective cybersecurity education, training, and workforce development programs** being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?
6. What are the **greatest challenges and opportunities** facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?
7. How will **advances in technology** (e.g., artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?
8. What **steps or programs should be continued, modified, discontinued, or introduced** to grow and sustain the Nation’s cybersecurity workforce, taking into account needs and trends? What steps should be taken:

i. At the Federal level?

ii. At the state or local level, including school systems?

iii. By the private sector, including employers?

iv. By education and training providers?

v. By technology providers?

Kevin Kimball
NIST Chief of Staff

[FR Doc. 2017-14553 Filed: 7/11/2017 8:45 am; Publication Date: 7/12/2017]