



7555-01-P

## **NATIONAL SCIENCE FOUNDATION**

### **Request for Information on Update to the 2016 Federal Cybersecurity Research and Development Strategic Plan**

**AGENCY:** National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD); submitted by the National Science Foundation.

**ACTION:** Notice of Request for Information.

**SUMMARY:** Pursuant to the Cybersecurity Enhancement Act of 2014, Federal agencies must update the Federal cybersecurity research and development (R&D) strategic plan every four years. The NITRD NCO seeks public input for the 2019 update of the Federal cybersecurity R&D strategic plan. The updated plan will be used to guide and coordinate federally funded research in cybersecurity, including cybersecurity education and workforce development, and the development of consensus-based standards and best practices in cybersecurity.

**DATES:** To be considered, submissions must be received on or before 11:59 p.m. (ET) on January 15, 2019.

**ADDRESSES:** Submissions to this notice may be sent by any of the following methods:

(a) Email: [cybersecurity@nitrd.gov](mailto:cybersecurity@nitrd.gov). Submissions should include "RFI Response: Federal Cybersecurity R&D Strategic Plan" in the subject line of the message.

(b) Fax: 202-459-9673, Attn: Tomas Vagoun.

(c) Mail: NCO/NITRD, Attn: Tomas Vagoun, 2415 Eisenhower Avenue, Alexandria, VA 22314, USA.

**INSTRUCTIONS:** Response to this RFI is voluntary. Submissions must not exceed 25 pages in 12-point or larger font, with a page number provided on each page. Responses should include the name of the person(s) or organization(s) providing the submission.

Responses to this RFI may be posted online at <http://www.nitrd.gov>. Therefore, we request that no business-proprietary information, copyrighted information, or personally identifiable information be submitted in response to this RFI.

In accordance with FAR 15.202(3), responses to this notice are not offers and cannot be accepted by the Federal Government to form a binding contract. Responders are solely responsible for all expenses associated with responding to this RFI.

**FOR FURTHER INFORMATION, CONTACT:** Tomas Vagoun at [cybersecurity@nitrd.gov](mailto:cybersecurity@nitrd.gov) or 202-459-9674, or by mailing to NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314, USA. Individuals who use a telecommunications device for the deaf (TDD) may call the Federal Information Relay Service (FIRS) at 1-800-877-8339 between 8 a.m. and 8 p.m., Eastern time, Monday through Friday.

**SUPPLEMENTARY INFORMATION:** The Cybersecurity Enhancement Act of 2014 (<https://www.gpo.gov/fdsys/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf>) requires that every four years the applicable Federal agencies, working through the National Science and Technology Council and the Networking and Information Technology R&D (NITRD) program, develop and update a Federal cybersecurity research and development strategic plan.

The most recent version of the strategic plan was released in February 2016 (<https://www.nitrd.gov/pubs/2016-Federal-Cybersecurity-Research-and-Development->

Strategic-Plan.pdf). This strategic plan identifies four categories of defensive capabilities (deter, protect, detect, adapt) and six critical dependent areas (scientific foundations, risk management, human aspects, transition to practice, workforce development, and infrastructure for research) as the structure for focusing and coordinating Federal cybersecurity R&D activities. The quadrennial strategic plan update (to be released by end of 2019) will leverage this structure.

On behalf of Federal agencies and the NITRD Cyber Security and Information Assurance Interagency Working Group, the NCO for NITRD seeks public input on Federal priorities in cybersecurity R&D. Responders should consider a 10-year time frame when characterizing the challenges, prospective research activities, and desired outcomes. Responders are asked to answer one or more of the following questions:

1. What innovative, transformational technologies have the potential to greatly enhance the security, reliability, resiliency, and trustworthiness of the digital infrastructure, and to protect consumer privacy?

2. What progress has been made against the goals of the 2016 Federal Cybersecurity R&D Strategic Plan? Are there mature private-sector solutions that address the deficiencies raised in the 2016 Strategic Plan? What areas of research or topics of the 2016 Strategic Plan no longer need to be prioritized for federally funded basic research?

3. What areas of research or topics of the 2016 Strategic Plan should continue to be a priority for federally funded research and require continued Federal R&D investments?

4. What challenges or objectives not included in the 2016 Strategic Plan should be strategic priorities for federally funded R&D in cybersecurity? Discuss what new capabilities would be desired, what objectives should guide such research, and why those capabilities and objectives should be strategic priorities.

5. What changes to cybersecurity education and workforce development, at all levels of education, should be considered to prepare students, faculty, and the workforce in the next decade for emerging cybersecurity challenges, such as the implications of artificial intelligence, quantum computing, and the Internet of Things on cybersecurity?

6. What other research and development strategies, plans, or activities, domestic or in other countries, should inform the U.S. Federal cybersecurity R&D strategic plan?

Following the receipt of comments, the NITRD Cyber Security and Information Assurance Interagency Working Group under the National Science and Technology Council will consider the input provided when updating the Federal cybersecurity R&D strategic plan.

Submitted by the National Science Foundation on behalf of the Networking and Information Technology Research and Development (NITRD) National Coordination Office (NCO) on November 7, 2018.

**Suzanne H. Plimpton,**

*Reports Clearance Officer,*

*National Science Foundation*

[FR Doc. 2018-24668 Filed: 11/9/2018 8:45 am; Publication Date: 11/13/2018]