7555-01-P

NATIONAL SCIENCE FOUNDATION

Request for Information (RFI) – Federal Cybersecurity R&D Strategic Plan

AGENCY: The National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD).

ACTION: Request for Information (RFI)

FOR FURTHER INFORMATION, CONTACT: Tomas Vagoun at vagoun@nitrd.gov or (703) 292-4873.

DATES: To be considered, submissions must be received no later than June 19, 2015.

SUMMARY:

In response to the Cybersecurity Enhancement Act of 2014, federal agencies are developing a Federal cybersecurity research and development strategic plan. On behalf of the agencies, the Cyber Security and Information Assurance Research and Development Senior Steering Group seeks public input on research objectives for the strategic plan. The strategic plan will be used to guide and coordinate federally-funded cybersecurity research.

SUPPLEMENTARY INFORMATION:

The Cybersecurity Enhancement Act of 2014 (https://www.congress.gov/bill/113th-congress/senate-bill/1353) requires that the applicable federal agencies, working through the National Science and Technology Council (NSTC) and the Networking and Information Technology R&D (NITRD) Program, develop a Federal cybersecurity research and development strategic plan. The strategic plan is to be delivered to Congress by the end of 2015.

On behalf of NITRD, the Cyber Security and Information Assurance Research and Development Senior Steering Group (CSIA R&D SSG) seeks public input in several areas identified by the Act and regarding the current federal priorities in cybersecurity research and development (R&D). Responders are asked to answer one or more of the following questions:

Questions related to the Cybersecurity Enhancement Act of 2014:

1. Section 201 (a) (1) of the Act identifies a number of cybersecurity objectives. What scientific, technological, or implementation gaps are indicated by those objectives? What research goals, for both basic and applied research, could serve as guidance for a federally-funded, multi-agency portfolio of R&D activities to close those gaps?

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

3. Discuss how the Federal government can foster the rapid transfer of R&D results into new cybersecurity technologies and applications for the timely benefit of society and the national interest.

4. Discuss how the current research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems could be improved, including how the access by academic researchers to this infrastructure and related data could be improved.

In 2011, the Government released "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program" (http://www.nitrd.gov/subcommittee/csia/fed_cybersecurity_rd_strategic_plan_2011.pdf) outlining objectives for federally-funded research to fundamentally improve the security, safety, and trustworthiness of the nation's digital infrastructure. The 2011 Strategic Plan defined five promising areas where research could make fundamental, game-changing advances in improving the security and trustworthiness of cyberspace: Tailored Trustworthy Spaces, Moving Target, Cyber Economic Incentives, Designed-In Security, and Science of Security. The challenges and objectives described in the 2011 Strategic Plan remain pertinent and will be incorporated into the new Strategic Plan. The following questions are directed at the 2011 Strategic Plan:

5. What areas of research or topics of the 2011 Strategic Plan do not need to be prioritized anymore for federally-funded research (because, for example, solutions are now sufficiently mature, or the private sector is now significantly invested in addressing the deficiencies)?

6. What areas of research or topics of the 2011 Strategic Plan should continue to be a priority for federally-funded research and need continued federal R&D investments?

7. What challenges or objectives not included in the 2011 Strategic Plan should be a strategic priority for federally-funded R&D in cybersecurity? Discuss what new capabilities would be desired, what objectives should guide such research, and why those objectives should be a strategic priority.

Submission Instructions:

Page limitation: submissions must be 25 pages or less.

Comments can be submitted by any of the following methods:

(a) Email: cybersecurity@nitrd.gov

(b) Fax: (703) 292-9097, Attn: Cybersecurity Research and Development

(c) Mail: Attn: Cybersecurity Research and Development, NCO, Suite II-405, 4201 Wilson Blvd., Arlington, VA 22230

Deadline for submission under this RFI is June 19, 2015.

Responses to this RFI may be posted online at http://www.nitrd.gov. The CSIA R&D SSG therefore requests that no business proprietary information or copyrighted 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 Government to form a binding contract. Responders are solely responsible for all expenses associated with responding to this RFI.

Submitted by the National Science Foundation in support of the Networking and Information Technology Research and Development (NITRD) National Coordination Office (NCO) on April 22, 2015.

Suzanne H. Plimpton,

Reports Clearance Officer,

National Science Foundation.

[FR Doc. 2015-09697 Filed: 4/24/2015 08:45 am; Publication Date: 4/27/2015]