7555-01-P

NATIONAL SCIENCE FOUNDATION

Request for Comments (RFC) - Federal Cybersecurity Research and Development Strategic Plan

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

ACTION: Request for Comments (RFC)

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

DATES: To be considered, submissions must be received by December 19, 2012.

SUMMARY: This Request For Comments (RFC) is issued by the Cyber Security and Information Assurance Research and Development Senior Steering Group (SSG) of the Federal Networking and Information Technology Research and Development (NITRD) Program. The SSG is preparing a report to provide an update on technological developments in Federal cybersecurity research and development since the release of the 2011 Federal Cybersecurity Research and Development Strategic Plan (the strategic plan). Also, in light of the ever evolving technological landscape of cybersecurity, and as input to its follow-on report, the SSG seeks comments on the progress over the past year in the research areas identified in the strategic plan, the strategic

plan's impact in orienting private sector cybersecurity research and development activities, the successes and challenges in achieving the technological objectives outlined in the plan, and on any nascent or emerging areas in cybersecurity research and development that warrant further focus. Additionally, the comments will be used by the SSG in its assessment of future needs and directions in Federal cybersecurity research and development. Comments are to be submitted to cybersecurity@nitrd.gov.

SUPPLEMENTARY INFORMATION: Continued cybersecurity research and development is critical to ensuring that we are on track as a Nation to develop innovative tools and capabilities to address cybersecurity threats. In December 2011, the White House Office of Science and Technology Policy (OSTP) released the "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program," a framework for a set of coordinated Federal strategic priorities and objectives for cybersecurity research. (http://www.nitrd.gov/Publications/PublicationDetail.aspx?pubid=39)

The strategic plan was developed under the leadership of the Cyber Security and Information Assurance Research and Development Senior Steering Group (SSG) of the Federal

Networking and Information Technology Research and Development (NITRD) Program. It identifies key cybersecurity research and development themes that are shaping and facilitating a coordinated Federal research and development agenda to engender game-changing technologies. With this overarching template, the federal scientific community has been focusing on a common set of problems. The strategic plan is being executed by all of the agencies conducting and funding Federal cybersecurity research, including DARPA, Department of Homeland Security, Department of Energy, IARPA, National Institute of Standards and Technology, National Security Agency, National Science Foundation, and the Department of Defense. Input from industry, academia, and other stakeholders during the development of the strategic plan contributed greatly to the formulation of Federal research directions in cybersecurity. Guided by this plan, many research activities, initiatives, and solicitations have already been launched by Federal agencies in all areas defined by the plan.

In an effort to continue to evolve Federal strategic directions in cybersecurity research, the SSG seeks comments to gain a better understanding of the plan's impact. Furthermore, the SSG seeks input regarding prospective areas in cybersecurity research and development that might benefit from coordinated support by Federal agencies. To assist with its report, the SSG is requesting that interested parties submit written comments.

We welcome comments from all interested parties, including, but not limited to, academia, private industry, and all levels of government. We seek comments on the following questions in relation to the strategic plan:

1) Research Themes of the Strategic Plan:

(a) Do the research themes need to be refined or enhanced? If so, in what way?

(b) What are the research, development, implementation, transition-to-practice, or other challenges that need to be overcome to achieve the goals under each theme?

(c) Are there areas in cybersecurity research not addressed by the strategic plan that should be? If yes, what are they, why are they important, and what advances in such areas are needed to improve the security, safety, and trustworthiness of cyberspace?

2) Activities that Advance the Strategic Plan:

(d) What activities are you or your organization undertaking that support the objectives of the strategic plan? Please include a brief description of initiatives, use-cases, capabilities, technologies, and/or achievements.

(e) How might your organization utilize the research outcomes?

3) Sustainable Progress:

(f) What interactions, relationships, campaigns, or targeted assistance would support a sustainable process to drive changes envisioned by the research themes?

(g) What engagements among Federal agencies, government labs, industry, and universities are particularly effective in enabling rapid progress in the development of solutions?

To further enhance discussions related to cybersecurity research and this RFC, the Government will webcast a session on Federal cybersecurity research and development during the National Science Foundation's Secure and Trustworthy Cyberspace Principal Investigators Meeting. The session and the webcast will take place on November 27, 2012, from approximately 1:00pm-3:00pm EST. Additional instructions will be available at http://cps-vo.org/group/satc.

SUBMISSION INSTRUCTIONS:

Submission email: submit your comments to cybersecurity@nitrd.gov

Submission deadline: to be considered, submissions must be received by December 19, 2012

To the extent applicable, when addressing a particular question included in this request for comments, comments should reference the relevant number associated with the question. Comments submitted will be made available to the public online or by alternative means. For this reason, do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information. 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 RFC.

Submitted by the National Science Foundation for the National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD) on November 19, 2012.

Suzanne H. Plimpton,

Reports Clearance Officer,

National Science Foundation.

[FR Doc. 2012-28481 Filed 11/23/2012 at 8:45 am; Publication Date: 11/26/2012]