usacm ACM US Public Policy Council

RESPONSE TO REQUEST FOR COMMENT
Federal Cybersecurity Research and Development Strategic Plan
77 FR 70483
DOCUMENT NUMBER 2012-28481
U.S. NATIONAL SCIENCE FOUNDATION

RESPONSE FILED BY:
U.S. PUBLIC POLICY COUNCIL OF THE ASSOCIATION FOR COMPUTING MACHINERY

On behalf of the U.S. Public Policy Council (USACM) of the Association for Computing Machinery (ACM) we are submitting the following comments in response to the Request for Comment by the National Science Foundation on the Federal Cybersecurity Research and Development Strategic Plan ("Strategic Plan").

With over 100,000 members, the Association for Computing Machinery (ACM) is the world's oldest and largest educational and scientific computing society. The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology. Our comments are informed by the research experience of our membership. Should you have any questions or need additional information, please contact our Public Policy Office at 212-626-0541 or at acmpo@hq.acm.org.

We appreciate the attention of the National Science Foundation on checking on the progress of the field and mapping that against the Strategic Plan. We recognize the difficulty of coordinating research across so many different agencies, resulting in what many may consider an overly broad plan that could use more specifics. Cybersecurity is much more than a series of technically-oriented research questions, and it is important that strategic plans and the associated research include, among other things:

- Training that integrates the results of research to help the workforce adopt new technologies and practices.
- Human subjects research to understand why the public does (or does not) adopt various cybersecurity technologies and practices.
- Privacy research that addresses both how the public perceives privacy in the context of cybersecurity and how new cybersecurity technologies and practices can integrate privacy.

Answers to specific questions in the RFC

(1) Research Themes of the Strategic Plan

The strategic plan is vague on how its priorities are to be implemented. USACM's assumption is that a goal of the plan is to ensure that the priority areas outlined in the research themes are given due attention by covered agencies. We also assume that the priorities outlined in the plan are not intended to define all necessary research in the field,

and recommend that the plan (and any accompanying guidance) note that the priorities are not intended to exclude computing and information technology research that does not fall under one of the priorities.

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

Most of the research themes outlined in the plan are well-founded and have demonstrated promise in the laboratory and the research literature. However, the theme of Nature-Inspired Solutions is not similarly well founded,[1] and is insufficiently mature to allow for actionable goals in the context of cybersecurity. While some cybersecurity topics have realized a research advantage by identifying natural defenses and porting relevant concepts to cybersecurity solutions, those results apply to narrow niches. Additionally, there is a significant research literature going back nearly two decades that may not have been adequately examined in addressing the current theme.

It is important to ensure that research findings can be communicated to as many people that can use it as possible. However, that need must be balanced against ensuring an appropriate balance amongst short-, medium- and long-term research. Some in the research community have expressed concerns that there can be too much emphasis on transition-to-practice activities.

(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?

While national security is mentioned in the plan, the growth in that sector of cyberspace suggests it could use additional emphasis. For example, there is intense interest, and some cases of implementation, in offensive cyber efforts or cyber retribution against attackers. There is no corresponding basic research to ground such efforts. The ability or limitations in confidently identifying perpetrators; capabilities and limitations in controlling and estimating collateral damage; and economic impacts and liability issues of offensive cyber efforts are just a few of the important basic research questions raised by national security concerns. Research on these questions would have application outside of the national security context. There is increasing attention within the federal government on developing a national doctrine for cyberspace, and should that take shape, it would be useful to have a research foundation to rely on.

Related to the above, we urge that research be directed to efforts to enhance civilian law enforcement related to cybersecurity. Most of the unlawful behavior in cyberspace (past, present, and near future) appears to be non-military in origin, and cybersecurity research and development should be balanced to reflect activity in the field. Finding ways to apply

---

[1] Relevant explorations of the limitations of this approach can be found in section 5 of the unclassified JASON Report "Science of Cyber-Security," November 19, 2010. Accessible at http://www.nitrd.gov/fileupload/files/JSR10102Science_of_cyber20101128.pdf

civilian investigation and law enforcement to acts both large and small, and work with international partners, are needed. There is a distinction between cybersecurity related to law enforcement goals and cybersecurity related to national security goals, and this should be reflected in research priorities.

Additionally, we encourage consideration of privacy issues across the cybersecurity research spectrum. There needs to be attention focused on minimizing exposure and/or derivation of personal and private information in all aspects of information systems research: cloud computing, big data research, mobile computing, data mining and discovery, cyber security, law enforcement, and more. Understanding -- and addressing -- the tensions between enhanced discovery and protecting privacy should be a major focus of research.

(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.

Our members conduct their own research and engagement activities that we cannot effectively capture in these comments. USACM, through the Association for Computing Machinery, is participating as a member of the Identity Ecosystem Steering Group established to implement the National Strategy for Trusted Identities in Cyberspace. While the group is still standing up as an organization, ensuring that there is a way of supporting and communicating relevant research is an important thing that the Steering Group has yet to do.

(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?

One of the best means of sharing knowledge within the computing community, and especially between researchers and practitioners, is the scientific meeting or conference. Given recent Office of Management and Budget guidance that severely curtails agency participation in conferences (and pending legislation that would impose similar restrictions), we are concerned that this important tool could be lost, or at least impaired. We recommend that research agencies like NSF do what they can to demonstrate to OMB and other relevant entities that such conferences are an important part of their mission, and deserve exemption from such conference restrictions.