COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE CYBER SECURITY AND INFORMATION ASSURANCE RESEARCH AND DEVELOPMENT SENIOR STEERING GROUP OF THE FEDERAL NETWORKING AND INFROMATION TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM

"Request for comments regarding Federal Cybersecurity Research and Development Strategic Plan"

December 19, 2012

By notice published on November 26, 2012, 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 announced a request for comments on the progress of the 2011 Federal Cybersecurity Research and Development Strategic Plan ("Strategic Plan").[1] The Strategic Plan was developed by NITRD agencies in an effort to create a new cybersecurity strategy based on a coordinated set of research priorities characterized by four strategic goals: (1) Inducing Change; (2) Developing Scientific Foundations; (3) Maximizing Research Impact; and (4) Accelerating Transition to Practice.

EPIC supports various efforts of the Strategic Plan. Specifically, EPIC supports efforts to anonymize data to protect the privacy of users as researchers work towards better data models of cyber economic incentives.[2] These measures minimize risks to privacy resulting from the misuse of personally identifiable information. We also support the

[1] 77 Fed. Reg. 70483 (Nov. 26, 2012).
[2] *See, e.g.*, Executive Office of the President National Science and Technology Council, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*, 10 (Dec. 2011) [hereinafter *Strategic Plan*].

preservation of anonymous web access within Trusted Tailored Spaces.[3] This technique allows individuals to obtain access to information without the risk of tracking and profiling. In addition, EPIC backs the Strategic Plan's call to promote privacy and focus on privacy-enhancing technologies within the context of "trusted identities."[4] EPIC has additional recommendations to improve the Strategic Plan to better protect privacy and civil liberties.

Pursuant to this request, the Electronic Privacy Information Center ("EPIC") recommends that the SSG incorporate the following recommendations into the Strategic Plan: (1) narrowly define "threat"; (2) fully adhere to the Privacy Act of 1974 and the Freedom of Information Act; (3) actively incorporate genuine privacy-enhancing technologies ("PETs") into new technologies and protocols; and (4) acknowledge the OECD Security Guidelines.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus on emerging civil liberties issues and protecting privacy, the First Amendment, and constitutional values. EPIC has a long history of promoting transparency and accountability for cybersecurity and government data collection programs, specifically through the enforcement of the Privacy Act and the Freedom of Information Act.[5] Transparent cybersecurity programs are crucial to the public's ability to monitor the government's national security efforts and ensure that federal agencies respect privacy

[3] *Id*. at 7-8.
[4] *Id*. at 12-13.
[5] *See EPIC v. NSA*, 678 F.3d 926 (D.C. Cir. 2012); EPIC, Cybersecurity Privacy Practical Implications, http://epic.org/privacy/cybersecurity/; EPIC, *EPIC v. NSA – Cybersecurity Authority*, http://epic.org/privacy/nsa/epic_v_nsa.html; EPIC, Comments of the Elec. Privacy Info. Ctr. to the Cyber Security and Information Assurance Research and Development Senior Steering Group of the Federal Networking and Information Technology Research and Development Program: Request for Comments, Dec. 19, 2012, *available at* http://epic.org/privacy/cybersecurity/EPIC-DOD-Cyber-Security-Comments.pdf.

rights and comply with their obligations under the Privacy Act. EPIC further supports techniques that improve both privacy and security.

I. The Strategic Plan Should Narrowly Define "Threat"

The Strategic Plan makes numerous references to "threats" without fully identifying what constitutes a threat.[6] The Strategic Plan references the "Fiscal Year 2010 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002" as a resource for "further data on the size and nature of threats,"[7] yet even this document fails to adequately define and narrow the term "threats." Such an open-ended and broad use of the word "threat" does not properly narrow the Strategic Plan's cybersecurity research objectives to relevant cybersecurity problems. EPIC objects to these particularly broad usages because they increase the risk of innocuous online activities being classified as "threats"—thereby providing the pretext for the collection of user data. Therefore, SSG needs to refine and clarify the definition of cyber "threat"

II. There is a Considerable Public Interest in the Transparency of Government Cybersecurity Activities

The challenges of cybersecurity touch upon a number of critical areas including healthcare, energy, financial services, and defense; and the efforts by the government to increase cybersecurity affect every citizen in the United States.

[6] *See, e.g.*, *Strategic Plan* at 1-4, 7, 9-10, 13-14.
[7] *Strategic Plan* at 2 n.3.

On May 29, 2009, President Barack Obama announced the Administration's plan to address the growing issue of digital information security.[8] Discussing the plan in 2010, Cybersecurity Coordinator Howard Schmidt emphasized the importance of transparency:

> Transparency is particularly vital in areas, such as the [Comprehensive National Cybersecurity Initiative], where there have been legitimate questions about sensitive topics like the role of the intelligence community in cybersecurity. Transparency provides the American people with the ability to partner with government and participate meaningfully in the discussion about how we can use the extraordinary resources and expertise of the intelligence community with proper oversight for the protection of privacy and civil liberties.[9]

Transparency and accountability in cybersecurity research, development, and implementation will allow the public to participate in the ongoing cybersecurity debate as it develops and encourage government agencies to be mindful of the privacy and civil liberties of citizens of the United States.

III. The 2011 Federal Cybersecurity Research and Development Strategic Plan Should Fully Adhere to the Privacy Act and Freedom of Information Act

The Strategic Plan provides an overarching set of coordinated research priorities for a number of federal agencies including the Department of Homeland Security, National Security Agency, and Defense Advanced Research Projects Agency. Many of these agencies, through their agency work, collect various personal information on individuals that is subject to the Privacy Act of 1974.

---

[8] *See, e.g.*, Data Accountability and Trust Act (DATA), H.R. 1707, 112th Cong. (2011) (introduced by Rep. Rush (D-IL)); Secure and Fortify Electronic Data Act (SAFE Data Act) H.R. 2577, 112th Cong. (2011) (introduced by Rep. Bono Mack (R-DA)).

[9] Howard A. Schmidt, *Transparency Cybersecurity*, NAT'L SEC. COUNCIL (Mar. 2, 2010), http://www.whitehouse.gov/blog/2010/03/02/transparent-cybersecurity.

The Privacy Act of 1974 places extensive obligations on federal agencies that collect and use personal information.[10] Research and Development ("R&D") under the Strategic Plan that may collect and use personal information should not be exempted from the obligations under the Privacy Act of 1974. In addition to the Privacy Act, participants in the Strategic Plan should fully adhere to the openness requirements of the Freedom of Information Act ("FOIA"). EPIC emphasizes that FOIA's purpose is to facilitate transparency by providing public oversight of government operations. Therefore participants in the Strategic Plan should only apply FOIA exemptions when they are absolutely necessary.

IV. Privacy Protections are Vital to Cybersecurity

The incorporation of privacy safeguards is vital to cybersecurity. Robust privacy protections promote cybersecurity in a number of ways. Proper privacy protections, including adequate data protection and avoiding unnecessary sharing of personal information, limit exposure to a cyberattack or other type of breach and minimize the risk to individuals when such attacks occur.

Protecting individual's privacy keeps cybersecurity efforts focused on robust efforts to secure cyberspace, prevent attacks, and minimize damage and disruption when attacks do occur. As noted, EPIC supports the Strategic Plan's commitment to anonymity and privacy and emphasizes the need for the development of genuine privacy-enhancing technologies that minimize or eliminate the collection of personally identifiable information where possible. Furthermore, in an effort to protect personal privacy and maintain the open and free flow of information, EPIC recommends the Strategic Plan

[10] 5 U.S.C. § 552a (2006).

acknowledge the Organisation for Economic Co-operation Development ("OECD") Security Guidelines.[11] These principles include:

- Awareness;
- Responsibility;
- Response;
- Ethics;
- Democracy;
- Risk Assessment;
- Security Design and Implementation;
- Security Management and;
- Reassessment.[12]

In particular, EPIC emphasizes the need for recognition of the Democracy Principle, which states "[t]he security of information systems and networks should be compatible with essential values of a democratic society."[13]

V. Conclusion

As the Strategic Plan moves forward, the agencies involved in the plan must uphold their obligations under the Privacy Act and the Freedom of Information Act. EPIC urges the National Coordination Office for Networking Information Technology Research and Development to adopt the recommendations to the Strategic Plan suggested above.

Respectfully Submitted,

Marc Rotenberg
EPIC Executive Director

Khaliah Barnes
EPIC Administrative Law Counsel

Jeramie D. Scott
EPIC National Security Fellow

[11] Organisation for Economic Co-operation Development, *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002), *available at* http://www.oecd.org/internet/interneteconomy/15582260.pdf.
[12] *Id*.
[13] *Id*.