May 12, 2010

Howard A. Schmidt
Special Assistant to the President and
Cybersecurity Coordinator
Eisenhower Executive Office Building
1650 Pennsylvania Avenue, NW
Washington, DC 20500

Dear Mr. Schmidt,

We the undersigned organizations write to request a meeting with you to discuss our interests in the nation's plans for cybersecurity. We share President Obama's concerns regarding the security of the Internet and our electrical and technology infrastructure, yet we believe that the right approach to enhanced cybersecurity must incorporate protections of our basic freedoms and constitutional rights.

First, cybersecurity initiatives should be designed in a manner that does not discourage lawful, constitutionally protected activity. Overreaching cybersecurity measures may deter individuals and organizations that rely on the Internet from engaging in First Amendment protected activity such as research, accessing information, collaboration, political participation, fundraising, coalition building, campaigns, advocacy, organized dissent, political speech, watchdog actions against government and businesses, freedom of expression, dissemination of information or outreach to constituencies, and more.

Protecting freedom of expression and association should be a paramount concern as our nation develops a cybersecurity policy, and care should be taken to ensure that new policies do not have a chilling effect on the expression of a wide diversity of ideas and points of view or association with others via the Internet. The Internet is a vital source of information for a large and growing number of citizens and is one of the primary platforms for the democratic discussion and debate necessary for a free society. We believe, moreover, that First Amendment rights such as these are integrally connected to privacy, due process, equal protection, and indeed the rights and values protected by the entire Bill of Rights. We would like to discuss these concerns with you, and in particular how they relate to the activities of libraries, independent media, membership organizations, and advocacy groups with an online presence.

For example, we are aware of EINSTEIN 3, an effort led by the Department of Homeland Security and with the assistance of the National Security Agency to secure civilian- federal government computer networks from cyber-attacks. All Internet traffic to government agency websites could be subject to EINSTEIN 3. The Privacy Impact Assessment for EINSTEIN 3 states the following surveillance:

> The goal of EINSTEIN 3 is to identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness and security response. It will have the ability to automatically detect and respond appropriately to cyber threats before harm is done, providing an intrusion prevention system supporting dynamic defense.

How will 'cybersecurity' and 'malicious threats' be defined? What is the legal basis for the government to undertake this program? Who will determine what information will be acquired by the government and under what standard? Will the government be prevented from accessing expressive and associational information unless it is evidence of a crime? Will additional protections be granted for sensitive personal information? Will the program respect the right to anonymous speech? Who will have access to the information once it is collected, and how will it be used and disseminated? Also, how will the information be stored, by whom, and for how long? How will due process rights be established? And how might the evolution of the Internet impact cybersecurity and privacy? The answers to these questions will determine whether the government's cybersecurity initiatives chill protected First Amendment activities, offend due process, or otherwise infringe on rights.

Second, cybersecurity programs must apply strong Fair Information Practices so that users of digital communications receive robust and effective protections under laws such as the Privacy Act. Information about these initiatives should also be available to the public and subject to the Freedom of Information Act. These and other relevant federal laws should extend to government contractors involved in federal government cybersecurity.

Finally, cybersecurity activity undertaken by the federal government must be carefully monitored. Any policies should be subject to the independent oversight of an empowered and effective Privacy and Civil Liberties Oversight Board. This body must be funded sufficiently. And it is critically important that it be staffed with a diverse group of technical, policy, and legal experts to take on the challenges of monitoring federal government activity related to cybersecurity by both civilian and military authority. Cybersecurity efforts should also be subject to rigorous public and congressional reporting.

We believe that President Obama's commitment to privacy and freedom in his statements regarding cybersecurity reflects the values we express in this letter.[1] We are committed to the benefits that a safe, secure, and free Internet have provided to us in meeting the needs of our constituents. A successful cybersecurity effort will be enhanced by practical implementation of these values and collaboration with our organizations to educate online users about strategies to

---

[1] http://www.c-span.org/Watch/Media/2009/05/29/HP/R/19192/Pres+Obama+announces+cyber+security+policy.aspx

make surfing, shopping, texting, organizing, and engaging in digital communications more secure. Therefore, we are ready and willing to participate in a dialogue with you on these issues at your earliest convenience.

In discussing these issues with you, we seek three things: (1) greater transparency in cybersecurity decision-making, (2) a role in the decision-making process for advocacy organizations that rely on the Internet, and (3) legal constraints on when, where, and how information may be acquired or viewed in cybersecurity-related activities.

To indicate your availability for a meeting with the groups listed below, please contact Lillie Coney, who coordinates the Privacy Coalition, an Electronic Privacy Information Center (EPIC) project in cooperation with organizations including the undersigned. She can be reached at 202-483-1140 x 111 or by email at coney@epic.org.

Thank you for your consideration of this request. We look forward to a meeting with you on the matters outlined in this letter.

Sincerely,

1. American Civil Liberties Union
2. American Library Association
3. Association of Research Libraries
4. Bill of Rights Defense Committee
5. Center for Financial Privacy and Human Rights
6. Center for Media and Democracy
7. Citizens for Responsibility and Ethics in Washington
8. Consumer Action
9. Council on American-Islamic Relations
10. Cyber Privacy Project
11. Defending Dissent Foundation
12. Electronic Privacy Information Center
13. Government Accountability Project
14. Internet Collaboration Coalition
15. JustHealth
16. Lawyers' Committee for Civil Rights Under Law
17. Liberty Coalition
18. Media Alliance
19. The Multiracial Activist
20. NAACP
21. National Coalition Against Censorship
22. National Lawyers Guild, National Office
23. OpenTheGovernment.org
24. Peace Action
25. Privacy International

26. Privacy Rights Clearinghouse
27. Progressive Librarians Guild
28. Reporters Without Borders (RSF)
29. Rutherford Institute
30. Special Libraries Association
31. The Special Libraries Association
32. UNITED SIKHS
33. U.S. Bill of Rights Foundation
34. World Organization for Human Rights USA

EPIC Board/Advisory Board Members/Others

Bruce Schneier, EPIC Board Member
Pablo Molina, EPIC Board Member
Stefan Brands, EPIC Advisory Board Member
Christine Borgman, EPIC Board Member
Alessandro Acquisti, EPIC Advisory Board Member
David Chaum, EPIC Advisory Board Members
Chip Pitts, EPIC Advisory Board Member
Pamela J. Harbour, EPIC Advisory Board Member
Grayson Barber, EPIC Advisory Board Member
Mary Minow, EPIC Board Member
Former Congressman Bob Barr