March 20, 2009

CENTER FOR DEMOCRACY & TECHNOLOGY
Keeping the Internet Open, Innovative and Free

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

Melissa Hathaway
National Security Council
The White House
Sent via e-mail

Dear Ms. Hathaway:

Thank you for meeting with CDT and with other privacy advocates on March 4 and for giving us this opportunity to provide comments for the cybersecurity 60-day review. We were pleased to hear that privacy and civil liberties issues were a core cross-cutting concern for the review team. In order to adequately address these concerns, CDT believes it will be essential to take the steps outlined below. We look forward to discussing these ideas with you in the follow-on meeting we agreed to set up.

Transparency

As a prerequisite for any cybersecurity program to adequately protect privacy and civil liberties, the government would need to offer the public increased information about the measures being taken to protect the relevant networks and how those measures could affect individual users. Fair information practices, due process principles, and the crucial need for public-private cooperation all require openness as an essential element of a national cybersecurity strategy. Transparency, which so far has been woefully lacking, is necessary for ensuring both that the public understands the nature of and justification for any privacy impact and that the public can hold the government accountable for the effectiveness of its efforts and for any abuse of its powers.

CDT does not mean to suggest that every detail of every aspect of the program need be made public. In fact, there are many details that should remain classified to ensure that those attempting to breach sensitive networks are not provided with information that could aid them. For example, information collected by intelligence agencies that describe the attack signatures of foreign adversaries or their capabilities must be handled very carefully. However, the level of secrecy toward cybersecurity displayed by the last Administration put the success of the program at risk by not providing enough information for the public to understand what the government was trying to do, the role of the private sector, and how privacy would be protected.

The private sector operates much of the critical infrastructure that must be protected against attack. And, it provides much of the hardware and software on which government systems rely, including the government's classified systems. The

private sector has valuable information about vulnerabilities, exploits, patches and responses. Its cooperation with this effort depends on trust, and a lack of transparency fosters a lack of trust.

Our experience in tracking the EINSTEIN 2 program demonstrates that a number of potential concerns can be addressed with transparency.[1] We believe that the release of public System of Records Notices and Privacy Impact Assessments along with open and closed Congressional hearings can provide the public with a reasonable starting point in assessing the national cybersecurity strategy and its impact on privacy. Agencies that cannot be transparent through these kinds of public processes should not lead the government cybersecurity initiative.

Lead Agency: DHS

Specifically, there is serious concern that if the NSA were to take the lead role in the cybersecurity initiative, it would almost certainly mean less transparency, less trust, and less corporate and public participation, increasing the likelihood of failure or of ineffectiveness. In part, this distrust relates to the NSA's recent involvement in secret eavesdropping activities that failed to comply with statutory safeguards. The program placed private sector companies asked to assist with the surveillance in an extremely difficult position; those that provided assistance were exposed to massive potential liability. Given NSA's very recent history of acting outside statutory limits, the private sector and the public at large may not trust the NSA with an expanded role in monitoring domestic cybersecurity.

The concerns with NSA go beyond the recent activity. NSA has long had a dual role: it spies on adversaries, cracks their computer networks, and breaks their codes. It also protects U.S. government communications from interception. These two roles tug in opposite directions because the U.S. and its adversaries frequently use the same technology. As a result, if NSA finds security vulnerabilities in a widely used product, it may be inclined to keep the loophole a secret so it can exploit those vulnerabilities against its targets, thereby depriving other government agencies and private entities of information they could use in defending themselves against attack.

Finally, NSA in our view is committed, for otherwise legitimate reasons, to a culture of secrecy that is incompatible with the kind of information sharing necessary for the success of a cybersecurity program.

We urge that the NSA not be given a leading role in monitoring domestic traffic or in making decisions about the cybersecurity initiative as it affects unclassified systems.

---

[1]For example, *see* the NIST Information Security and Privacy Advisory Board December 10 letter to Jim Nussle http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ISPAB_Einstein-letter.pdf.

Instead, means need to be developed for ensuring that whatever expertise NSA has in discerning attacks is made available to a civilian agency.

We believe that, on balance, the lead for cybersecurity should go to DHS. Secretary Napolitano only a few days ago named Philip Reitinger as Deputy Undersecretary of the National Protection & Programs Directorate. Reitinger is the former Chief Trustworthy Infrastructure Strategist at Microsoft, where he helped protect critical networks. He is well-qualified to lead cybersecurity efforts at DHS and to make DHS the government-wide lead. We urge the White House review team to recommend that DHS be unambiguously designated as lead agency in the cybersecurity effort and that Reitinger and his team be given the resources they need to do the job well.

ECPA, the Wiretap Act, and Information Sharing with the Private Sector

Because most of the networks that need to be protected are maintained by the private sector and not by the government, there will need to be exchange of information between the private sector and the government. Private sector operators are already monitoring their systems on a routine basis to detect and respond promptly to any possible attacks. The government has a legitimate role, to the extent it has any special expertise, in helping the private sector develop effective monitoring systems, to be operated by the private sector. The government also should be sharing with private sector network operators the information that they need to determine when they are under attack, to defend in real time against attacks, and to help them secure their networks against future attack. We believe that most of the cybersecurity effort should focus on these forms of interaction with the private sector.

When an attack occurs, or when events suggesting a possible attack are observed, private sector providers may need to share with the government limited information that is <u>necessary</u> to understand possible attacks, respond, and resist further attack. The Wiretap Act and the Electronic Communications Privacy Act already contain "self-defense" provisions that are broad enough to permit the sharing of communications information from the private sector to the government that is necessary to respond to an attack. *See* 18 U.S.C. 2511(2)(a)(i), 18 U.S.C. 2511(i), 18 U.S.C. 2702(b)(5) and 18 U.S.C. 2702(c)(3). We believe that these provisions should be narrowly construed, and we strongly urge that they not be used to justify ongoing or routine disclosure of traffic by the private sector to the government. We would be alarmed if the White House review suggested that these provisions justified ongoing or routine disclosures to the government or that they need to be broadened; rather, we believe that the review should include a recommendation that they be narrowly construed in the cybersecurity context to apply only when a company believes it is or may be under attack or that an attack has occurred.

The White House review should reaffirm that no governmental entity should be involved in monitoring private networks as part of the cybersecurity initiative. This

is the job of the providers themselves, not of the government. Instead, the government should help develop the tools that allow providers to do this in the least intrusive way. Similarly, the review should also reaffirm that good cybersecurity measures will not require that backbone providers give governmental entities access to a significant portion of the communications that flow through their networks. These assurances would go a long way toward addressing the concerns of the privacy community.

Anonymity

CDT agrees with many experts that authentication and reputation have a key role to play in building security online. However, solutions to protect systems that have too heavy a focus on identity management over pseudonymous and anonymous approaches to protecting systems could have the unintended adverse effect of invading privacy, limiting free expression around the world and restricting the openness of the Internet as a means of communication. As founders of the country such as Benjamin Franklin, James Madison and others recognized, anonymity and pseudonymity play an essential role in allowing political views to be aired. The United States should continue our tradition as promoters of anonymous political speech and should insure that it promotes cybersecurity solutions that are not tied to identity.

Promoting Privacy Leadership

As GAO has regularly reported, the federal government as a whole lacks the necessary leadership structure to protect privacy. In order to successfully address privacy and civil liberties under any new cybersecurity leadership structure, privacy leadership at high levels must be created. In particular, we suggest four areas where new privacy efforts could help to protect Americans and build the capacity of privacy programs within the government:

1) Chief Privacy Officer at OMB — We urge the review team to call for the designation of a presidentially-appointed chief privacy officer, housed at OMB, to help develop better privacy protections within the federal government. This officer will need at least a small staff and resources to be effective.
2) Privacy Officers' Council — A separate and funded Council, comprised of the privacy officers of the various agencies, will help the agencies share information about privacy issues and offer a means for the OMB Chief Privacy Officer to work directly with the departments on a regular basis.
3) Privacy Contact in NSC — In order to have real impact, leadership on privacy issues must come from the OMB Chief Privacy Officer. However, having a person responsible for privacy in the NSC could help build trust between the privacy community and the national security leadership. It would be essential that this position have the ability to work with the OMB privacy

officer and the intelligence community and to brief those outside government as much as possible on a non-classified basis.

4) Privacy and Civil Liberties Oversight Board — The PCLOB remains without members or staff. This body would play an important independent role in oversight of privacy and civil liberties. We urge the review team to push for the nomination process to move forward at an accelerated pace.

Scope of CyberSecurity Program Should Be Defined by White House Review To Accommodate Existing Security Efforts

Finally, CDT would like to emphasize the need to provide clear scope of not only what the administration should cover in its cybersecurity efforts, but also what it will not cover. In our first meeting, you suggested that the 60-day White House review would cover broad areas of interest to the administration from health IT to economic security as it relates to networked information. We agree that this broad agenda is important as we move forward, but it is essential that the review recognize the security work that has already been completed in areas such as health IT.[2] It is also important that the new leadership on cybersecurity not become a bottleneck for approving new innovation online. For this public/private partnership to be successful, government must, in most cases, act as a partner and not a barrier, working with industry as industry creates a more secure network.

In conclusion, we would like to thank you again for meeting with us. We appreciate the short time frame that President Obama has given you and your team and we look forward to working with you as you move forward.

Sincerely,

Ari Schwartz
Vice President and Chief Operating Officer

Gregory T. Nojeim
Senior Counsel and Director of CDT's Project on Freedom, Security and Technology

[2] See CDT's May 2008 paper "Comprehensive Privacy and Security: Critical for Health Information Technology" http://www.cdt.org/healthprivacy/20080514HPframe.pdf.