

Cybersecurity Program Should Be More Transparent, Protect Privacy

March 30, 2009

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts [here](#):

On February 9, President Obama ordered his National Security and Homeland Security Advisors to review the federal government's cybersecurity plan, programs and activities. The 60-day review will culminate in recommendations as to how the new Administration should protect government networks from attack and help the private sector protect key networks, including financial and communications networks. On March 19, CDT provided the White House review team with recommendations on protecting privacy and innovation.

[1\) Cybersecurity Transparency Promotes Trust, Industry Participation](#)

[2\) DHS Should Lead, with Augmented Resources and High Level Support](#)

[3\) Network Providers, Not Government, Should Monitor Networks for Intrusions](#)

[4\) Privacy Leadership Needed](#)

1) Transparency in Cybersecurity Program Promotes Trust, Industry Participation

On February 9, President Obama ordered his National Security and Homeland Security Advisors to review the federal government's cybersecurity plan, programs and activities. The 60-day review will culminate in recommendations as to how the new Administration should protect government networks from attack and help the private sector protect key networks, including financial and communications networks. On March 19, CDT provided the White House review team with recommendations on protecting privacy and innovation.

So far, the government's cybersecurity efforts have been shrouded in too much secrecy. Greater openness 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. Not only to protect privacy and civil liberties but also to encourage private sector trust and participation, the government must make public more 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 need to foster public-private cooperation all require openness as an essential element of a national cybersecurity strategy.

Not every detail of every aspect of the federal cybersecurity program needs to be revealed. In fact, many details should remain classified so 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 the last Administration displayed 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. In addition, it provides much of the hardware and software used by government systems, including 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.

The release of the Privacy Impact Assessment for the DHS EINSTEIN 2 program demonstrates that total obscurity is not a precondition for cybersecurity. It also demonstrates that transparency can expose potential concerns in a cybersecurity program so they can be addressed. For example, the EINSTEIN 2 Privacy Impact Assessment disclosed enough information about the program to allow the Information Security and Privacy Advisory Board to weigh in with suggestions and concerns about the privacy impact of some aspects of the program. System of Records Notices and Privacy Impact Assessments, along with Congressional oversight, can provide the public with a starting point for 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.

[CDT letter](#) [1] to Melissa Hathaway, Head of 60-Day Review Team (March 19, 2009)

[EINSTEIN 2](#) [2] Privacy Impact Assessment (May 19, 2008)

[Letter from ISPAB](#) [3] on EINSTEIN 2 PIA (December 10, 2008)

2) DHS Should Lead, with Augmented Resources and High Level Support

Some have suggested that the DHS National Cyber Security Center (NCSC), which now leads the government-wide cybersecurity program, should be moved to the National Security Agency, which would then oversee the program. They argue that the NSA has more expertise in monitoring communications networks than any other agency of government. However, expertise in spying does not necessarily entail expertise in cybersecurity. Moreover, 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. Citing many of these concerns, as well as a lack of adequate resources, the Director of the NCSC recently resigned in a stinging, public letter.

In part, distrust in NSA emanates from its 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.

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 a security vulnerability in a widely used product, it may be inclined to keep the loophole a secret so it can exploit the vulnerability against its targets. This would deprive other government agencies and private entities of information they could use to defend themselves against attack.

Finally, NSA is committed, for otherwise legitimate reasons, to a culture of secrecy that is incompatible with the information sharing necessary for the success of a cybersecurity program. NSA should not be given a leading role in monitoring the traffic on civilian government systems nor should it be making decisions about cybersecurity as it affects such systems; and its role in monitoring private sector systems should be even less. Instead, means need to be developed for ensuring that whatever expertise NSA has in discerning attacks is made available to a civilian agency.

Some have suggested that a new cybersecurity office should be established in the White House, and that this office should be tasked with overseeing the entire program. They argue that only the White House has the authority to direct agencies to do what needs to be done to protect their own

systems. However, such an approach risks politicizing the cybersecurity program. Moreover, as Senator Susan Collins (R-ME) recently pointed out, putting the cybersecurity program in the White House would mean less Congressional oversight and more secrecy. The White House role in cybersecurity should be to set policy and direction, and to budget enough resources for the program.

The lead for cybersecurity should stay with the Department of Homeland Security, and the NCSC should be provided with additional resources and high-level attention. DHS Secretary Napolitano recently 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.

[Resignation letter from Rod Beckstrom](#) [4], former NCSC director (March 5, 2009)

[Letter from Senator Susan Collins](#) [5] to DHS Secretary Janet Napolitano (March 24, 2009)

[Commentary by CDT Policy Director Jim Dempsey](#) [6] on Bush Administration cybersecurity initiative (May 14, 2008)

3) Network Providers - Not the Government - Should Monitor Their Networks for Intrusions

Because most of the critical computer networks that need to be protected from cyberattack are maintained by the private sector and not by the government, there will need to be exchanges 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 information that will help them identify attacks at an early stage, defend in real time against attacks, and secure their networks against future attack. Most of the federal government's 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 necessary 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). In CDT's view, no new statutory authority is needed to broaden this flow of information; rather, Congress should require public statistical reporting on the use of these provisions. Moreover, these provisions should 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. They cannot justify ongoing or routine disclosure of traffic by the private sector to the government.

No governmental entity should be involved in monitoring private networks as part of the cybersecurity initiative. This is the job of the private sector communications service 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. Effective cybersecurity does not require that backbone providers give governmental entities access to the communications that flow through their networks.

Nor does effective cybersecurity require radical changes in the current practices that permit speakers in some contexts to remain relatively anonymous. While authentication and reputation have a key role to play in building security online, approaches to cybersecurity that would eliminate pseudonymous and anonymous speech could have unintended adverse effects. They could invade

privacy, limit free expression around the world and restrict the openness of the Internet as a means of communication. As the founders of our country recognized, anonymity and pseudonymity play an essential role in allowing political views to be aired. The United States should continue its tradition as promoter of anonymous political speech and should insure that it supports cybersecurity solutions that are not tied to identity.

4) Privacy Leadership Needed

Currently, the federal government as a whole lacks a leadership structure to protect and advocate for privacy. In order to successfully address privacy and civil liberties under any new cybersecurity program, privacy leadership structures must be created at the White House level. Without such leadership, privacy may not receive adequate attention when needed – in the shaping of policy. To build privacy capacity within the federal government, CDT has recommended the following:

- Appointing a Chief Privacy Officer at OMB – CDT has urged President Obama to appoint a 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.
- Creating a Privacy Officers' Council – A CPO Council, comprised of the privacy officers of the various agencies and separate from the existing CIO Council, 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.
- Designating a Privacy Contact in NSC – 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.
- Reconstituting the Privacy and Civil Liberties Oversight Board – The PCLOB remains without members or staff. This body could play an important independent role in oversight of privacy and civil liberties. It needs to be reconstituted quickly. The President should nominate and the Senate should confirm members of the Board promptly.

The copyright © 2013 by the Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL:

<https://www.cdt.org/policy/cybersecurity-program-should-be-more-transparent-protect-privacy>

Links:

[1] http://www.cdt.org/security/20090319_cybersecure_comments.pdf

[2] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf

[3] http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ISPAB_Einstein-letter.pdf

[4] http://blog.wired.com/defense/files/ncsc_directors_resignation1.pdf

[5] http://www.cdt.org/security/20090324_collins_ltr.pdf

[6] http://www.forbes.com/2008/05/14/government-security-privacy-tech-security08-cx_ag_0514govt.html