Statement of Gregory T. Nojeim

Senior Counsel and Director,
Project on Freedom, Security & Technology
Center for Democracy & Technology

Before the House Committee on Energy and Commerce,
Subcommittee on Communications, Technology and the Internet

On
Cybersecurity, Civil Liberties and Innovation

May 1, 2009

Chairman Boucher, Ranking Member Stearns and Members of the Subcommittee:

Thank you for the opportunity to testify today on behalf of the Center for Democracy & Technology.[1] We applaud the Subcommittee's leadership and foresight in examining the challenges we face as a nation in addressing cybersecurity issues in a manner that reflects our commitments to liberty and market-driven innovation.

The Cybersecurity Threat

It is clear that the United States faces significant cybersecurity threats. Recently, the *Wall Street Journal* reported that computer hackers had penetrated systems containing designs for a new Air Force fighter jet and had stolen massive amounts of information.[2] U.S. intelligence agencies, which have developed capabilities to launch cyber attacks on adversaries' information systems, have sounded alarms about what a determined adversary could do to critical information systems in the U.S.

It is also clear that the government's response to this threat has been woefully inadequate. The Department of Homeland Security has been repeatedly criticized[3]

---

[1] The Center for Democracy & Technology is a non-profit, public interest organization dedicated to keeping the Internet open, innovative and free. Among our priorities is preserving the balance between security and freedom after September 11, 2001. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications and public interest organizations, companies and associations interested in information privacy and security issues.

[2] Gorman, Siobhan, Computer Spies Breach Fighter-Jet Project, *The Wall Street Journal,* http://online.wsj.com/article/SB124027491029837401.html, April 21, 2009. *See also,* Gorman, Siobhan, Electricity Grid in U.S. Penetrated by Spies, *The Wall Street Journal*, http://online.wsj.com/article/SB123914805204099085.html, April 8, 2009.

[3] *See, e.g.,* Government Accountability Office, *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity* http://www.gao.gov/new.items/d061087t.pdf, Testimony of GAO's David A. Powner, Director, Information Technology Management Issues,

for failing to develop plans for securing key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, and information technology and telecommunications systems, as required in the Homeland Security Act of 2002.[4]

In recognition of these risks and challenges, President Obama ordered his national security and homeland security advisors to examine the cybersecurity issue and develop for him a policy blueprint. Melissa Hathaway headed the 60-day review. The review team reported to the President on April 17, but its recommendations have not yet been made public. The review team solicited input from a wide range of cybersecurity stakeholders, including the privacy and open government communities.[5] The Administration should be commended for its process.

A Careful and Nuanced Approach Is Required for Securing the Internet

In developing a national policy response to cybersecurity challenges, a nuanced approach is critical. It is absolutely essential to draw appropriate distinctions between government systems and systems owned and operated by the private sector. Policy towards government systems can, of course, be much more "top down" and much more prescriptive than policy towards private systems.

With respect to private systems, it is further necessary when developing policy responses to draw appropriate distinctions between the elements of "critical infrastructure" that primarily support free speech and those that do not. The characteristics that have made the Internet such a success – its openness, decentralized and user controlled nature and its support for innovation and free expression – may be put at risk if heavy-handed cybersecurity policies are enacted that apply uniformly to all "critical infrastructure."

Almost 20 years ago, the Commerce Committee played a key role in opening the Internet to commercial traffic. Since then, it has largely promoted a light-handed

---

before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the House Committee on Homeland Security, September 13, 2006. Last year, GAO reported that the Department of Homeland Security's U.S. Computer Emergency Readiness Team ("U.S. CERT"), which has significant responsibilities for protecting private and governmental computer networks, was failing to establish a "truly national capability" to resist cyber attacks. Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, http://www.gao.gov/products/GAO-08-588, July 2008.

[4] P.L. 107-296, Section 201(d)(5).

[5] CDT hosted a meeting among privacy and open government advocates, and Ms. Hathaway and her key staff on March 4. CDT submitted recommendations to the 60-day review team; those recommendations can be found in this March 19 letter to Ms. Hathaway: http://www.cdt.org/security/20090319_cybersecure_comments.pdf.

approach to governmental regulation of the Internet that has helped it become a ubiquitous and valuable part of the American economy and democracy. We ask this Subcommittee in particular to enter the cybersecurity policy debate with this history in mind, and with the mission of protecting the attributes of the Internet that make it so important to free speech. The Internet is different from other critical infrastructures; it is time to say so.

While the Internet is a "network of networks" encompassing at its edges everything from personal computers in the home to servers controlling the operation of nuclear power plants, cybersecurity policy should not sweep all entities that connect to the network into the same basket. For example, while it is appropriate to require authentication of a user of an information system that controls the electric power grid, it would not be appropriate to require authentication of ordinary Americans surfing the Internet on their home computers. Approaches to cybersecurity that would eliminate pseudonymous and anonymous speech online would put privacy at risk, chill free expression and erode the Internet's essential openness. As the founders of our country recognized, anonymity and pseudonymity play essential roles in allowing political views to be aired.

In sum, CDT believes that cybersecurity legislation should not treat all critical infrastructure information systems the same. Very careful distinctions – too often lacking in cybersecurity discourse – are needed to ensure that the elements of the Internet and communications structures critical to new economic models, human development, free speech and privacy are not regulated in ways that could stifle innovation or chill free speech.

Communications Network Providers – Not the Government – Should Monitor Their Networks for Intrusions and Respond To Such Intrusions

Most critical infrastructure computer networks are maintained by the private sector. Private sector operators already monitor those systems on a routine basis to detect and respond promptly to any possible attacks, and it is often in their best business interest to continue to ramp up these defenses.

CDT strongly believes that no governmental entity should be involved in monitoring private networks as part of a 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.

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 information with private sector network operators 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.

Some have proposed that the President ought to be given authority to limit or shut down Internet traffic to a compromised critical infrastructure information system in an emergency, or to disconnect such systems from other networks for reasons of national security.[6] Such extraordinary power should extend only to governmental systems, not to those maintained by private sector entities. Even if such power over private networks was exercised only rarely, its mere existence would pose other risks, enabling a President to coerce costly, questionable – even illegal – conduct by threatening to shut down a system. Any such shut down could also have far-reaching, unintended consequences for the economy and for the critical infrastructures themselves. To our knowledge, no circumstance has yet arisen that could justify a Presidential order to limit or cut off Internet traffic to a particular critical infrastructure system when the operators of that system think it should not be limited or cut off. They already have control over their systems and financial incentives to quarantine network elements that need such measures. We urge you to reject proposals to give the President or another governmental entity power to limit or shut down Internet traffic to privately-held critical infrastructure systems.

Transparency in the Cybersecurity Program Promotes Trust and Industry Participation

So far, the government's cybersecurity efforts have been shrouded in too much secrecy. Openness is necessary for ensuring both that the public understands the nature of and justification for any civil liberties impact and that the public can hold the government accountable for the effectiveness of its efforts and for any abuse of its powers. To protect privacy and civil liberties and to encourage private sector

[6] Section 18 of the Cybersecurity Act of 2009, S. 773.

trust and participation, the government must make public more information about existing threats, the measures being taken to protect the relevant networks, and how those measures could affect individual users.

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 in 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 lack of transparency also undermines trust and cooperation with the private sector entities that operate much of the critical infrastructure that must be protected against attack. Private sector entities also provide much of the hardware and software used by government systems, including classified systems, and are likely to have valuable information about vulnerabilities, exploits, patches and responses. No policy response to encourage a more robust public-private partnership on cybersecurity will be effective unless and until the government brings its cybersecurity efforts out of the shadows.

Promoting Information Sharing Between the Private Sector and the Government

There is widespread agreement that information sharing is an important component of an effective cybersecurity strategy and that information sharing today is inadequate. However, there is no clear consensus on how to improve information sharing. We do not need information sharing merely for the sake of sharing information. It is important that the information that is shared is the information that is actually needed and is actionable, and that adequate standards and privacy protections be put in place when the information to be shared includes personally identifiable information.

Improving information sharing should start with a discussion about exactly what information held by the private sector has not been shared with the government when a specific request for it has been made, and the reasons given for the decision not to share the information. Next, there needs to be an understanding of why existing structures are falling short. These existing structures include the DHS U.S. Computer Emergency Readiness Team ("U.S. CERT"), which already has an information sharing role, and the existing public private partnerships represented by the Information and Analysis Centers ("ISACs").[7] These structures should be

[7] Each critical infrastructure industry defined in Presidential Decision Directive 63 (1998) has established an Information Sharing and Analysis Center to facilitate communication

fixed or eliminated before consideration is given to creating new information sharing structures. The GAO recently made a series of suggestions for improving the performance of U.S. CERT.[8] They included: giving it analytical and technical resources to analyze multiple, simultaneous cyber incidents and to issue more timely and actionable warnings; developing more trusted relationships to encourage information sharing; and providing U.S. CERT sustained leadership within DHS that could make cyber analysis and warning a priority.

Regardless of the structure used, it seems that industry self-interest, rather than government mandate, should be enhanced to facilitate information sharing. Congress should explore whether additional market incentives could be adopted to encourage the private sector to share threat and incident information and solutions. One option would be to compensate companies that share with a clearinghouse the cybersecurity solutions in which they had to invest substantial resources. Since such information could be shared with competitors and may be costly to produce, altruism should not be expected, and compensation may be appropriate. Congress should consider whether an antitrust exemption to facilitate cybersecurity collaboration is also necessary. Other options would be to provide safe harbors, insurance benefits and/or liability caps to network operators that share information.

CDT strongly disagrees with proposals to solve the information sharing dilemma by simply expanding government power to seize privately held data. We urge the Subcommittee to steer clear of a recent proposal to give the Secretary of Commerce unfettered authority to access private sector data that is relevant to cybersecurity threats and vulnerabilities, regardless of whether the information to be accessed is proprietary, privileged or personal and without regard for any law, regulation or policy that governs governmental access, including privacy laws like the Electronic Communications Privacy Act.[9] This approach is dangerous to civil liberties and would undermine the public-private partnership that needs to develop around cybersecurity. We urge you to reject this heavy-handed approach, and to instead favor market-based incentives to facilitate information sharing.

DHS Should Lead, with Augmented Resources and High Level Support

It is widely expected that the President will decide it is necessary to provide greater

---

among critical infrastructure industry representatives, a corresponding government agency, and other ISACs about threats, vulnerabilities, and protective strategies. The ISACs are linked through an ISAC Council, http://www.isaccouncil.org/ and they can play an important role in critical infrastructure protection, as indicated in this white paper from January, 2009. http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf.

[8] Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, http://www.gao.gov/products/GAO-08-588, July 2008.

[9] Section 14 of the Cybersecurity Act of 2009, S. 773.

cybersecurity leadership from the White House and that seems generally appropriate. 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 superior 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.[10]

In part, distrust in the 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.[11] 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 in making decisions about cybersecurity as it affects such systems; and its role in monitoring private sector systems should be even less. Indeed, NSA Director Lt. Gen. Keith Alexander recently renounced any interest in the NSA having a lead role securing non-defense governmental networks.[12] Instead, procedures should be developed for ensuring that whatever expertise NSA has in discerning attacks is made available to a civilian agency.

---

[10] Resignation letter of Rod Beckstrom, former NCSC director, http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf, March 5, 2009.

[11] Commentary by CDT Policy Director Jim Dempsey on Bush Administration cybersecurity initiative, http://is.gd/pINP, May 14, 2008.

[12] Declan McCullagh, NSA Chief Downplays Cybersecurity Power Grab Reports, *CNET News*, http://news.cnet.com/8301-13578_3-10224579-38.html, April 21, 2009.

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.[13]

In thinking through a proper organizational approach, it is helpful to separate responsibility for developing cybersecurity policy from responsibility for cybersecurity operations. In our view, the White House role in cybersecurity should be to set policy and direction, and to budget enough resources for the program. This could be done through a newly established White House office, rather than in one under the National Security Council, whose activity would be shrouded in secrecy.

While some have proposed moving primary responsibilities for cybersecurity operations from the Department of Homeland Security to the Department of Commerce, we do not believe that the case has been made for such a disruptive move. In short, the problems that plague the program won't be fixed by moving them from one governmental box to another.

The lead for cybersecurity operations 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.

Conclusion

Policy makers should distinguish among different types of critical infrastructure when developing cybersecurity policy. One size does not fit all. The key is to acknowledge the substantial differences between the Internet and other critical infrastructure systems, and to tailor solutions to the systems that need protection. Effective cybersecurity measures intended to increase security of the communications infrastructure need not threaten civil liberties. As a general rule, market-based solutions instead of governmental mandates should be favored for private infrastructure systems. The Subcommittee on Communications, Technology and the Internet can play an important role in implementing these approaches to cybersecurity and in keeping the Internet the engine of innovation and robust discourse that is has become.

---

[13] Letter from Senator Susan Collins to DHS Secretary Janet Napolitano http://www.cdt.org/security/20090324_collins_ltr.pdf, March 24, 2009.