Statement of Gregory T. Nojeim

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

Before the House Committee on Armed Services,
Subcommittee on Emerging Threats and Capabilities

On

The Role of the Department of Defense in Cybersecurity

February 11, 2011

Chairman Thornberry, Ranking Member Langevin, 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 for examining the role of the Department of Defense in cybersecurity. Today, I will briefly outline the cybersecurity threat and discuss how to avoid cybersecurity measures that would infringe on privacy or innovation or unintentionally undermine security itself. I will emphasize that private network operators, not the government, should monitor and secure private sector systems, while the Department of Defense secures military systems and the Department of Homeland Security secures civilian government systems. To the extent that DOD entities have information and expertise that would help private sector operators and DHS with their cybersecurity activities, mechanisms must be developed to permit DOD to share that information and expertise. I also will discuss some incremental changes in the law that may enhance information sharing without eroding privacy. Finally, I will discuss the role that identity and authentication measures, if properly designed and deployed, can play in enhancing security while also protecting privacy.

The Cybersecurity Threat

It is clear that the United States faces significant cybersecurity threats from state actors, from private actors motivated by financial greed, and from terrorists. In

[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. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications and public interest organizations, companies and trade associations interested in information privacy and security issues.

2009, 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] Last year, Google revealed that it had been subjected to a major espionage attack originating in China aimed at stealing personal information about human rights activists and Google's own proprietary information.[3] DOD 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. Both offensive and defensive aspects of the issue may have been illustrated by the Stuxnet worm, which, allegedly designed with the involvement of the U.S. government, penetrated the control systems of centrifuges Iran was using to refine uranium, causing hundreds of the centrifuges to spin out of control and damage themselves.[4]

It is also clear that the government's response to this threat has been inadequate. The Department of Homeland Security has been repeatedly criticized[5] for failing to

---

[2] Gorman, Siobhan, Computer Spies Breach Fighter-Jet Project, *The Wall Street Journal,* http://online.wsj.com/article/SB124027491029837401.html, April 21, 2009.

[3] Nakashima, Ellen, Google To Enlist NSA To Help It Ward Off Cyberattacks, *The Washington Post,* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html, February 4, 2010. Information from over 30 other technology, defense, energy and financial firms was also compromised in related attacks.

[4] Broad, William, et al., Israeli Test on Worm Called Crucial in Iran Nuclear Delay, *New York Times,* http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1, January 15, 2011.

[5] *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, before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the House Committee on Homeland Security, September 13, 2006. In 2008, GAO reported that the Department of Homeland Security's U.S. Computer Emergency Readiness Team, 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. In 2009, GAO testified that DHS had yet to comprehensively satisfy its cybersecurity responsibilities: *Cybersecurity, Continued Federal Efforts Are Needed to Protected Critical Systems and Information.* Testimony of GAO's Gregory C. Wilshusen, Director, Information Security Issues, before the Subcommittee on Technology and Innovation of the House Committee on Science and Technology, June 25, 2009. In 2010, GAO found continued shortcomings. *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed*, GAO-11-24, October 6, 2010, http://www.gao.gov/products/GAO-11-24.

develop plans for securing key resources and critical infrastructure, as required in the Homeland Security Act of 2002.[6] President Obama's national security and homeland security advisors completed a cyberspace policy blueprint on April 17, 2009, but implementation of those measures was slowed by the Administration's failure timely to appoint the cybersecurity official in the White House who could drive policy development and coordinate implementation of a government-wide plan.

In the meantime, the Department of Defense has stood up its own cybercommand to oversee the military's efforts to protect its own 15,000 computer networks.[7] Commanded by General Keith Alexander – who also heads the NSA – it is housed at Fort Meade alongside the NSA. It became operational on May 21, 2010, pulling together information operations expertise from components of the Army, Navy and Air Force and launching a program to recruit a cadre of cyberwarriors. In this environment – a plodding DHS and a slowed-down White House, an emergent Cybercommand with expertise, a complex threat environment with many actors and networks that interconnect and that all need to be defended – it is tempting to ask Cybercommand and the NSA to do it all.

We urge you to resist that temptation and instead send a clear message in support of the statement Deputy Secretary of Defense William Lynn, III made last November:

> [Cybercommand] is not intended to be the militarization of cyberspace. It will be responsible for DOD's networks – the dot-mil world. Responsibility for civilian networks – dot-gov – stays with the Department of Homeland Security, and that's exactly how it should be.[8]

In support of this effective allocation of responsibilities, this Subcommittee should encourage DOD entities to share cybersecurity information that would be useful for private sector entities and to support, with limitations, the work of the DHS in defending the civilian government domain. It should also watch out for "mission

---

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

[7] The United States Cybercommand is subordinate to the U.S. Strategic Command and is headquartered in Fort Meade, Maryland where NSA is also headquartered. Its mission statement, from the U.S. Strategic Command Fact Sheet:

> USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

http://www.stratcom.mil/factsheets/Cyber_Command/.

[8] Lynn, William J. III, Deputy Secretary of Defense, speech delivered November 12, 2009 at the Defense Information Technology Acquisition Summit in Washington, D.C. http://www.defense.gov/speeches/speech.aspx?speechid=1399.

creep" that would find Cybercommand and the NSA conducting activities not in support of others that go beyond defense of .mil networks.

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 military government systems, civilian government systems, and systems owned and operated by the private sector. Policy towards government systems, both those in the military domain and those under .gov, 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 open, decentralized and user-controlled nature and its support for innovation, commerce, and free expression – may be put at risk if heavy-handed cybersecurity policies are enacted that apply uniformly to all "critical infrastructure."

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 Internet into the same basket. For example, while it is appropriate to require authentication of a user of an information system that controls a critical element of the electric power grid or of a user of an information system containing classified information, it would not be appropriate to require authentication of ordinary Americans surfing the Internet on their home computers.

In sum, CDT believes that cybersecurity legislation and policy should not treat all critical infrastructure information systems the same. Instead, a sectoral approach is called for. Very careful distinctions – too often lacking in cybersecurity discourse – are needed to ensure that the elements of the Internet critical to new economic models, human development, and civic engagement are not regulated in ways that could stifle innovation, chill free speech or violate privacy.

Network Providers – Not the Government – Should Monitor Privately-Owned Networks for Intrusions

When the White House released the Cyberspace Policy Review on May 29, 2009, President Obama said:

> *"Our pursuit of cybersecurity will not – I repeat, will not – include monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans."*

CDT strongly agrees. No governmental entity – including any element of DOD and DHS – should be involved in monitoring private communications networks as part of a cybersecurity initiative. This is the job of the private sector communications service providers themselves, not of the government. 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 to attacks as necessary to protect their networks, and it is in their business interest to continue to ramp up these defenses. Indeed, providing reliable networks is essential to maintaining their business.

Transparency and the Role of the NSA and Cybercommand in Securing Unclassified Civilian Systems

Some have suggested that the National Security Agency and the Cybercommand should lead or play a central role in the government-wide cybersecurity program. They argue that the NSA has more expertise in monitoring communications networks than any other agency of government and that Cybercommand will be better resourced than DHS to do this work. However, expertise in spying does not necessarily entail superior expertise in all aspects of cybersecurity. The answer to insufficient resources at DHS should be augmentation of those resources, not abdication of its mission. Moreover, there is serious concern that if a DOD entity were to take the lead role in cybersecurity for civilian unclassified systems, it would almost certainly mean less transparency, less trust, and less corporate and public participation, thereby increasing the likelihood of failure and decreasing the effectiveness of the effort even in terms of security.

Over 85% of critical infrastructure information systems are owned and operated by the private sector, which also 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. Private sector operators may hesitate to share this information if they do not know how it will be used and whether it will be shared with competitors. Private sector cooperation with government cybersecurity effort depends on trust. A lack of transparency undermines trust and has hampered cybersecurity efforts to date.

For many reasons, openness is an essential aspect of any national cybersecurity strategy. Without transparency, there is no assurance that cybersecurity measures adequately protect privacy and civil liberties and adhere to Fair Information Practice and due process principles. Transparency is also essential if the public is to hold the government accountable for the effectiveness of its cybersecurity measures and for any abuses that occur.

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. For these reasons, among others, NSA should not be given a

leading role in monitoring the traffic on unclassified 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 smaller. Instead, procedures should be developed for ensuring that whatever expertise and technology NSA has in discerning attacks is made available to a civilian agency.

Likewise, Cybercommand, which will also operate largely in secret, should focus on securing the .mil domain. Mission creep into the .gov domain and the private sector should be guarded against. The lead for cybersecurity operations should stay with the Department of Homeland Security. Maintaining this division of labor will benefit both security and liberty. It will require governmental entities and the private sector to share cybersecurity information, and will require DOD entities to share human resources and expertise with DHS.

-- **Sharing human resources and expertise: the DOD/DHS Cybersecurity MOU**

On September 27, 2010, DHS and DOD signed a Memorandum of Understanding setting forth the terms by which they would provide personnel, equipment and facilities to increase inter-departmental collaboration and support and synchronize each other's cybersecurity operations.[9] Under the agreement, DHS sends teams to the NSA to plan and synchronize cyber-defense, learn about acquisition detection technologies and coordinate on civil liberties protections. NSA sends a team of cryptologists and operations professionals to the DHS network operations center to support DHS operations. NSA experts would work alongside DHS cybersecurity teams to help bring those teams up to speed quickly.

As CDT said when the MOU was made public in October, this kind of arrangement, if of limited duration, might represent the best way to leverage the NSA's defensive expertise domestically without the negatives associated with it being secretive, operating without public oversight, and, when operating abroad, bending and breaking local rules.[10] CDT has long advocated building up the civilian cybersecurity capability by leveraging the expertise of the NSA precisely to reduce the need of DHS to rely directly on NSA. Once DHS has built the necessary expertise, the existing MOU can expire. This Subcommittee could play an important role in overseeing this arrangement to make sure that it is benefitting both security and liberty.

---

[9] Memorandum Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity, effective September 27, 2010, http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

[10] Leslie Harris, President and CEO of the Center for Democracy & Technology in the Huffington Post, October 15, 2010, http://www.huffingtonpost.com/leslie-harris/dhs-nsa-in-cybersecurity_b_764289.html.

-- **Sharing information: Disclosures from the private sector to the government**

Current law gives providers of communications services substantial authority to monitor their own systems and to disclose to military and civilian governmental entities, and to their peers, information about cyberattack incidents for the purpose of protecting their own networks. In particular, the federal Wiretap Act provides that it is lawful for any provider of electronic communications service to intercept, disclose or use communications passing over its network while engaged in any activity that is a necessary incident to the protection of the rights and property of the provider. 18 U.S.C. 2511(2)(a)(i). This includes the authority to disclose communications to the government or to another private entity when doing so is necessary to protect the service provider's network. Likewise, under the Electronic Communications Privacy Act (ECPA), a service provider, when necessary to protect its system, can disclose stored communications (18 U.S.C. 2702(b)(3)) and customer records (18 U.S.C. 2702(c)(5)) to any governmental or private entity.[11] Furthermore, the Wiretap Act provides that it is lawful for a service provider to invite in the government to intercept the communications of a "computer trespasser"[12] if the owner or operator of the computer authorizes the interception and there are reasonable grounds to believe that the communication will be relevant to investigation of the trespass. 18 U.S.C. §2511(2)(i).

These provisions do not, in our view, authorize ongoing or routine disclosure of traffic by the private sector to any governmental entity, including DOD. To interpret them so broadly would destroy the promise of privacy in the Wiretap Act and ECPA. The extent of service provider disclosures to DOD entities for self-defense purposes is not known publicly. We urge the Subcommittee to consider imposing a requirement that the extent of such information sharing be publicly reported, in de-identified form, both to assess the extent to which beneficial information sharing is occurring, and to guard against ongoing or routine disclosure of Internet traffic to DOD entities under the self-defense exception.

There is a widespread perception that cybersecurity information sharing as practiced is inadequate and there is some concern that the provisions of the Wiretap Act and ECPA are impediments to information sharing. This issue must be

[11] Another set of exceptions authorizes disclosure if "the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications [or information] relating to the emergency." 18 U.S.C. 2702(b)(8) and (c)(4).

[12] A "computer trespasser" is someone who accesses a computer used in interstate commerce without authorization. 18 U.S.C. 2510(21).

approached very cautiously, for exceptions intended to promote information sharing could end up severely harming privacy.

First, it should be noted that there has not been sufficient analysis to determine what information should be shared that is not shared currently. Improving information sharing should proceed incrementally. It should start with an understanding of why existing structures, such as the U.S. Computer Emergency Readiness Team ("U.S. CERT")[13] and the public-private partnerships represented by the Information Sharing and Analysis Centers (ISACs)[14] are inadequate. The Government Accountability Office (GAO) has made a series of suggestions for improving the performance of U.S. CERT.[15] The suggestions included giving U.S. CERT 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. All of these suggestions merit attention.

Second, an assessment should be made of whether the newly-established National Cybersecurity and Communications Integration Center (NCCIC) has addressed some of the information sharing issues that have arisen. The NCCIC is a round-the-clock watch and warning center established at DHS. It combines U.S. CERT and the National Coordinating Center for Communications and is designed to provide integrated incident response to protect infrastructure and networks.[16] Industry is

---

[13] U.S. CERT is the operational arm of the Department of Homeland Security's National Cyber Security Division. It helps federal agencies in the .gov space to defend against and respond to cyber attacks. It also supports information sharing and collaboration on cybersecurity with the private sector operators of critical infrastructures and with state and local governments.

[14] Each critical infrastructure industry sector defined in Presidential Decision Directive 63 has established Information Sharing and Analysis Centers (ISACs) to facilitate communication among critical infrastructure industry representatives, a corresponding government agency, and other ISACs about threats, vulnerabilities, and protective strategies. *See* Memorandum from President Bill Clinton on Critical Infrastructure Protection (Presidential Decision Directive/NSC-63) (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. The ISACs are linked through an ISAC Council, and they can play an important role in critical infrastructure protection. *See*, THE ROLE OF INFORMATION SHARING AND ANALYSIS CENTERS (ISACS) IN PRIVATE/PUBLIC SECTOR CRITICAL INFRASTRUCTURE PROTECTION 1 (Jan. 2009), *available at* http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf.

[15] *See* 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.

[16] *See* DHS Press Release announcing opening of the NCCIC, http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm.

now represented at the NCCIC[17] and its presence there should facilitate the sharing of cybersecurity information about incidents.

Third, industry self-interest, rather than government mandate, should be relied on to facilitate information sharing from the private sector to governmental entities. Congress should explore whether additional market-based incentives could be adopted to encourage the private sector to share threat and incident information and solutions. Since such information could be shared with competitors and may be costly to produce, altruism should not be expected, and compensation may be appropriate. Other options would be to provide safe harbors, insurance benefits and/or liability caps to network operators that share information about threats and attacks in cyberspace by terrorists and others.

CDT strongly disagrees with proposals to solve the information-sharing dilemma by simply expanding government power to obtain privately held data. We urge the Congress to steer clear of proposals to give a governmental entity wide-ranging authority to access private sector data that is relevant to cybersecurity threats and vulnerabilities.[18] Such an approach would be dangerous to civil liberties and would undermine the public-private partnership that needs to develop around cybersecurity. Collecting large quantities of sensitive information into a common database can also undermine security because such a database could, itself, become a target for hackers.

While, as noted above, current law authorizes providers to monitor their own systems and to disclose voluntarily communications and records necessary to protect their own systems, we have heard concern that the provisions do not authorize service providers to make disclosures to other service providers or to the government to help protect the systems of those other service providers. Perhaps it should. Many types of attacks could affect multiple providers, and disclosure by one entity about such an attack could be helpful to others. Therefore, there might be a need for a very narrow exception to the Wiretap Act and ECPA that would permit disclosures about specific attacks and malicious code on a voluntary basis, and that would immunize companies against liability for these disclosures. The exception would have to be narrow so that routine disclosure of Internet traffic to the government or other service providers remained clearly prohibited.

---

[17] *See* DHS Press Release announcing that it has agreed with the Information Technology Information Sharing and Analysis Center (IT-ISAC) to embed a full time IT-ISAC analyst at the NCCIC, November 18, 2010, http://www.dhs.gov/ynews/releases/pr_1290115887831.shtm.

[18] For an example of such a proposal, see Section 14 of the Cybersecurity Act of 2009 as introduced in the 111th Congress, S. 773.

Overall, given the risks to privacy, we urge the Congress to take only incremental approaches to information sharing, avoiding more radical approaches, such as permitting or mandating broad sharing of information that may be personally identifiable. In addition, because the existing privacy protections in ECPA have been outpaced by the development of technology, we also urge that any changes to ECPA to facilitate cybersecurity information sharing are counterbalanced with enhanced privacy protections.

-- Sharing information: Disclosures from the government to the private sector

DOD and DHS have legitimate roles, to the extent they have special expertise, in helping the private sector develop effective monitoring systems to be operated by the private sector. Most of the federal government's cybersecurity effort regarding private sector networks should focus on improving information sharing and otherwise strengthening the ability of the private sector to protect private sector networks. This is particularly true for DOD entities such as NSA, which have identified attack signatures that private sector entities may not be aware of. Ways should be found for the NSA to share such information with private sector network operators to help them identify attacks at an early stage, defend in real time against attacks, and secure their networks against future attack. Ideally this sharing would happen through DHS and would help DHS develop its own corresponding capacity.

Much has been said about the problem of sharing classified information with private sector owners and operators of critical information systems. This Subcommittee could make a substantial contribution to cybersecurity by taking steps to ensure that attack signatures are not unnecessarily classified and by working to ensure that providers have personnel who are cleared to receive the attack signatures that must remain classified.

The Government Should Monitor Its Own Networks for Intrusions, But Privacy Concerns Need to Be Addressed

Just as private sector network operators should, and do, monitor their systems for intrusions, the federal government clearly has the responsibility to monitor and protect its own systems. At the same time, such efforts must start with the understanding that exercise of the First Amendment rights of free speech and to petition the government will be chilled if communications between Americans their government are routinely accessed and shared with law enforcement and intelligence agencies. While the Fourth Amendment may not come into play because those communicating with governmental entities necessarily reveal their communications – including content – to the government, the privacy and civil liberties inquiry does not stop there. Protecting privacy in this context is absolutely critical to giving Americans the necessary comfort to communicate with their government.

Another important consideration is the question of how likely it is that private-to-private information may be accessed inadvertently through systems intended to detect intrusions against government computers. While we do not quarrel with the notion that DOD should monitor its own systems for intrusions, the role of intelligence and law enforcement agencies such as the NSA and the FBI in the intrusion detection enterprise with respect to civilian government networks must be carefully considered. Generally, Fair Information Practice principles should be applied to minimize the amount of personally identifiable information collected by the government, to limit its use of this information, and to notify users of this information collection and disposition.[19]

Under current law, all federal departments and agencies must adhere to information security best practices. Generally, these practices include the use of intrusion detection systems.[20] In an effort to improve security, the government has developed and is deploying the Einstein intrusion detection and prevention system. According to a May 19, 2008 Privacy Impact Assessment[21] and a January 9, 2009 opinion of the DOJ Office of Legal Counsel,[22] Einstein 2 is being deployed at participating federal agency Internet Access Points. Einstein 2 assesses network traffic against a pre-defined database of signatures of malicious code and alerts U.S. CERT to malicious computer code in network traffic. While the signatures are not supposed to include personally identifiable information ("PII") as defined by DHS, they do include Internet Protocol addresses, and the alerts that Einstein 2 generates for U.S. CERT may include PII.[23] In addition to using attack signatures, Einstein 2

---

[19] The Department of Homeland Security's Chief Privacy Officer issued a memorandum in late 2008 to describe how DHS would apply FIPS. *Privacy Policy Guidance Memorandum,* issued December 29, 2008 by Hugo Teufel III, Chief Privacy Officer, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[20] Einstein 2 PIA, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf (May 19, 2008), p. 2.

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

[22] Stephen. G. Bradbury, Principal Deputy Assistant Attorney General, *Legal Issues Relating To the Testing, Use and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch,* January 9, 2009, http://www.justice.gov/olc/2009/e2-issues.pdf. The memo concludes that operation of Einstein 2 does not violate the Constitution or surveillance statutes, and an August 14, 2009 opinion from the Obama Justice Department's Office of Legal Counsel affirms that conclusion. http://www.justice.gov/olc/2009/legality-of-e2.pdf.

[23] The PIA for Einstein 2 makes it clear that, for example, Einstein 2 will collect an email address when the source of malicious code it detects is attached to an email address. Moreover any "flow record" (a specialized summary of a suspicious communication) that Einstein routinely generates will generally include IP address and time stamp, which are widely regarded as personally identifiable.

also detects anomalous network traffic on a particular system and alerts U.S. CERT to those anomalies.

A successor, Einstein 3, is being tested with an undisclosed ISP and an undisclosed federal agency. It will have the added capability of intercepting threatening Internet traffic before it reaches a government system. According to the Privacy Impact Assessment DHS issued in connection with these tests,[24] Einstein 3 will use intrusion detection technology developed by the NSA and will adapt threat signatures developed by NSA in the course of its foreign intelligence work and by the DOD in connection with its information assurance mission. It will also use commercially available threat signatures. A key feature of Einstein 3 is that it operates on the network of an ISP providing service to the government instead of on the network of the federal agency that is being protected. One critically important question is whether Einstein can reliably focus on communications with the government to the exclusion of private-to-private communications passing over the ISP's network.

According to the Einstein 3 PIA, the participating federal agency will provide Internet Protocol addresses to the ISP, which will use them to distinguish traffic to or from that agency from other traffic. This is a logical, but by no means fool proof method of identifying the targeted traffic. IP addresses can be re-allocated and become outdated. If Einstein were to analyze private-to-private communications, it would likely be conducting an unlawful interception under the electronic surveillance laws. The Intelligence Authorization Act for FY 2010 requires reports to Congress about the privacy impact of Einstein and any other similar cybersecurity programs as well as information about the legal authorities for the programs and about any audits that have been conducted or are planned for the programs.[25] The Subcommittee should consider whether it would be appropriate for it to conduct oversight to determine the extent to which Einstein information flows back to DOD entities and the uses to which this information is being put.

Other questions about the Einstein intrusion detection system include:

- What personally-identifiable information has Einstein collected so far?
- What have law enforcement and intelligence agencies done with Einstein information that is shared with them, and more to the point, to what extent is the system being used to identify people who should be prosecuted or people who are of intelligence interest, even if that is not its primary purpose?
- To what extent are private sector operators keeping information about communications that appear to match attack signatures?
- How should users be notified that their visits to government websites and

[24] Privacy Impact Assessment for the Initiative Three Exercise, March 18, 2010, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf.

[25] Section 336 of the Intelligence Authorization Act for FY 2010, Pub. L. No. 111-259.

their email communications with government employees are being scanned for security reasons? [26]

The lack of transparency around Einstein highlights a broader concern about the federal government's cybersecurity program: excessive secrecy undermines public trust and communications carrier participation, both of which are essential to the success of the effort. The government needs to publicly disclose sufficient details about Einstein and other programs to be able to assure both the public at large and private sector communications service providers that the confidentially of personal and proprietary communications will be respected.

"Active Defense" and the First Amendment

Some DOD cybersecurity activities are expected to go beyond the kind of monitoring envisioned in the Einstein program. We also urge you to tread carefully in the area of "active defense" in the cybersecurity arena because of the First Amendment concerns raised by some active defense activities. Most cybersecurity measures today involve taking defensive steps, such as using firewalls and protecting sensitive information through authentication and authorization systems.

DOD officials and other experts speak of "active defense" and of offensive measures that would involve reaching out beyond the boundaries of military networks that must be protected and into other networks to hunt for malicious software.[27] For example, General Keith Alexander, head of Cybercommand and of the NSA, reportedly seeks authority to shut down parts of adversaries' computer networks to pre-empt a cyberattack against U.S. targets.[28] The risk here is that attacking computers in one country can unintentionally disrupt communications in another and disrupt the ability of people in the U.S. to legitimately access information that may be housed abroad. Moreover, because attribution is difficult in cyberspace, there is heightened risk that a defensive attack aimed at the source of malware will target another victim of the attack, instead of the attacker itself.

For all of these reasons, we urge you to take great care when considering these measures, and that this Subcommittee exercise its oversight authority over such measures keeping in mind the First Amendment rights of Americans.

---

[26] For a fuller listing of open questions about the Einstein Intrusion Detection System, see Center for Democracy & Technology, *Einstein Intrusion Detection System: Questions That Should Be Addressed*, http://www.cdt.org/security/20090728_einstein_rpt.pdf.

[27] The line between "active defense" and "offensive" cyber operations is a blurry one, and we do not attempt here to delineate what activities fall into each category.

[28] Nakashima, Ellen, Pentagon's Cyber Command Seeks Authority to Expand Its Battlefield, *The Washington Post*, November 6, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/AR2010110507304.html?wprss=rss_world.

Presidential Authority in Cybersecurity Emergencies

Some have proposed that the President or the Department of Homeland Security 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.[29] When the government of Egypt cut off Internet services on January 27, 2011 to much of its population in order to stifle dissent in an uprising, it magnified concerns about extending cybersecurity emergency authority to the U.S. President. It illustrated the First Amendment concerns that would attend use of such authority in the U.S. The authority to shut down or limit communications traffic should extend only to governmental systems (presumably, the government already has the authority to disconnect its own systems from the Internet), but should not extend to those maintained by private sector entities.

To our knowledge, no circumstance has yet arisen that could justify a governmental order to limit or cut off Internet traffic to a particular privately-owned and controlled 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 strong financial incentives to quarantine network elements that need such measures. They already limit or cut off Internet traffic to particular systems when they need to do so. They know better than do government officials whether their system needs to be shut down or isolated.

The list of potential unintended consequences to both the economy and to critical infrastructures themselves from a shut down of Internet traffic is long. It could interfere with the flow of billions of dollars necessary for the daily functioning of the economy. It could deprive doctors of access to medical records. Users of those systems, which may include government personnel, state and local emergency first responders and civilian volunteers, could find themselves with crippled communications capability in a crisis. It could deprive manufacturers of critical supply chain information. It could have world wide effect because much of the world's Internet traffic goes through the United States.

Even if such power over private networks were 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.

Finally, giving the government the power to shut down or limit Internet traffic would also create perverse incentives. Private sector operators will be reluctant to share information if they know the government could use that information to order them to shut them down. Conversely, when private operators do determine that

[29] In the 111th Congress, Section 18 of the Cybersecurity Act of 2009, S. 773 and Section 201 of the Protecting Cyberspace as a National Asset Act, S. 3480 both included such provisions.

shutting down a system would be advisable, they might hesitate to do so without a government order and could lose precious time waiting to be ordered by the government to shut down so that they would less likely be held liable for the damage a shut down could cause others.

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.

Building Privacy into Identity and Authentication Requirements Designed to Thwart or Discourage Malicious Activity

One of the most talked-about approaches to preventing and tracing cyber attacks by terrorists and others is to improve identity and authentication of those who would seek access to the system that must be protected. If an attack cannot be attributed to a particular person because the person cannot be identified, it is difficult to prosecute the perpetrator or deter the attack. However, while identification and authentication will likely play a significant role in securing critical infrastructure, identity and authentication requirements should be applied judiciously to specific high value targets and high-risk activities.

Some have argued for broad authentication mandates across the Internet – including calls for "Internet passports." Mandating strong identity and authentication measures for routine Internet interactions could seriously compromise user privacy, slow on-line interactions and transactions so much that their utility would be impaired, and fundamentally limit the ways in which people use the Internet.

While identity and authentication measures are important elements of cybersecurity, they can either promote privacy or threaten it, depending on how they are designed and implemented. For example, the fact that some transactions or interactions are anonymous may *enhance* the privacy and security of those transactions. Moreover, the right to speak anonymously enjoys constitutional protection.[30] On the other hand, authentication can also enhance privacy. For example, authenticating a party to a transaction may advance a privacy interest by preventing identity fraud. Depending on how the authentication system is designed, disclosing personally identifiable information to facilitate authentication may put privacy at risk or it may increase privacy. For example, it is possible to disclose data to establish trusted credentials that can be used for many on-line transactions, thereby eliminating the need to provide such information for each transaction and to many different entities.[31] Instead of submitting personal information to 10

[30] *McIntyre v. Ohio Elections Comm'n,* 514 U.S. 334 (1995).

[31] Center for Strategic and International Security, *Report of the CSIS Commission on Cybersecurity for the 44th Presidency,*

websites in order to make 10 purchases, the information could be submitted once to a credentialing organization that would perform the authentication necessary to the other transactions. At least for systems used by the private sector, government officials are not well equipped to resolve the complex design and implementation issues that must be addressed to ensure that such a system enhances privacy and security rather than undermining them. Accordingly, policymakers should be hesitant to impose identity mandates on the private sector.

Identity and authentication requirements should adhere to the principles of proportionality and diversity.[32] Under the proportionality principle, if a transaction has high significance and sensitivity and an authentication failure carries with it significant risk, it may be more appropriate to require authentication and the collection of more sensitive information to authenticate. Conversely, certain transactions do not need high degrees of authentication, or any at all. This principle applies in both the private and public sectors, but private sector operators – who know their systems best – are in the best position to decide what level of identity and authentication should be required for their own systems and transactions, depending on the degree of risk posed and the degree of trust that is called for. Private sector operators, such as those in the financial sector, already use various security measures related to online services such as banking and e-commerce. In addition, in light of the federal government's poor historical track record on securing its own systems, it may not be the best entity to put in charge of credentialing or other centralized online security activities.

Under the diversity principle for privacy in identity management schemes, it is better to have multiple identification solutions, because use of a single identifier or credential creates a single target for privacy and security abuses. A single identifier also allows for multiple transactions and interactions to be tied to that identifier, permitting potentially invasive data surveillance. Instead, identification and enrollment options should function like keys on a key ring, with different identities

---

http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf, December, 2008, p. 63. The CSIS report advocates strong authentication of identity for the information and communications technology sector, and the energy, finance and government services sectors. It also recognizes that authentication requirements should be proportional to the risk they pose and that consumers should have choices about the authentication they use.

[32] CDT has outlined these and other Privacy Principles for Identity in the Digital Age. Version 1.4 of the principles, released in December 2007, can be found here: http://www.cdt.org/security/identity/20080108idprinciples.pdf. The privacy principles for identity that extend beyond proportionality and diversity are based on Fair Information Practice principles, and include specifying the purpose for the system being used, limiting the use and the retention period of personal information collected, giving individuals control and choice over identifiers needed to enroll in a system to the extent this is possible, providing notice about collection and use of personally identifiable information, security against misuse of the information provided, accountability, access and data quality.

for different purposes.[33] One model that holds great promise is the "user-centric" identity model, in which the user logs into a Web site through a third party identity provider, who passes on information at the user's request to the Web site in order to authenticate the user.

The White House Cyberspace Policy Review embraced the diversity and proportionality principles by calling for an array of interoperable identity management systems that would be used only for what it called "high value" activities, like certain smart grid functions, and then only on an opt-in basis. It also called for the federal government to build a security-based identity management vision and strategy for the nation, in collaboration with industry and civil liberties groups.

Likewise, the draft National Strategy for Trusted Identities in Cyberspace (NSTIC) envisions an identity eco-system led by various private sector identity providers. It is not a "government ID for the Internet." If such an ID were created, it would not be trusted and would be little used. Instead, NSTIC properly relies on private sector entities to create identities that operate across many platforms. It also accounts for the need to have a range of levels of assurance for interaction on the Internet, ranging from completely anonymous to highly assured.

We urge the Congress to reject sweeping identity mandates and instead support identity initiatives that are led by the private sector and based on the federated model, as recommended in the NSTIC.

Conclusion

Policy makers should distinguish among different types of critical infrastructure when developing cybersecurity policy. One size does not fit all. Effective policies will preserve the open, decentralized, user-controlled, and innovative nature of the Internet and will tailor solutions to the systems that need protection.

Private network operators should monitor their own networks for evidence of intrusion and malicious code. Current law provides adequate authority for such monitoring, but may need to be clarified while ensuring that "self protection" measures do not become backdoors for governmental monitoring of private networks.

The DOD should focus on securing the .mil domain and should provide information and human resources to help DHS to monitor and secure the .gov domain. Intrusion detection and prevention activities should be designed and implemented so as not

[33] *See,* Center for Democracy & Technology, *Privacy Principles for Identity in the Digital Age,* http://www.cdt.org/security/identity/20080108idprinciples.pdf, December 2007.

to chill the right to free speech and the right to petition the government. Intrusion detection/prevention programs such as Einstein should be made more transparent.

Privacy and security are not a zero sum game. Measures intended to increase the security of communications and transactions – such as identity and authentication requirements – need not threaten privacy and indeed may enhance it if properly deployed.