Statement of Gregory T. Nojeim
Senior Counsel and Director,
Project on Freedom, Security & Technology
Center for Democracy & Technology

Before the Senate Committee on the Judiciary,
Subcommittee on Terrorism and Homeland Security

Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace

November 17, 2009

Chairman Cardin, Ranking Member Kyl 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 preventing terrorist attacks in cyberspace in a manner that also protects privacy and civil liberties. Today, I will briefly outline the cybersecurity threat and explain why measures appropriate for securing some critical infrastructure systems would be inappropriate for others. I will emphasize that private network operators, not the government, should monitor and secure private sector systems, while the government should monitor and secure its networks. I 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.

---

[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 trade associations interested in information privacy and security issues.

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. Just last week, the news magazine *60 Minutes* brought the cybersecurity threat into Americans' living rooms, reporting that cyber thieves had stolen millions of dollars from banks and key secrets from the government.[2] Earlier this year, 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.[3] 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. While we welcome the leadership of Secretary Napolitano and Deputy Undersecretary Reitinger, the Department of Homeland Security has been repeatedly criticized[4] for failing to develop plans for securing key resources and critical infrastructure, as required in the Homeland Security Act of 2002.[5] President Obama's national security and homeland security advisors completed a cyberspace policy blueprint on April 17, making many useful

---

[2] http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml.

[3] 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.

[4] *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. Last year, 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.

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

recommendations, but implementation of those measures has been slowed by the Administration's failure to appoint the cybersecurity official in the White House who could drive policy development and coordinate implementation of a government-wide plan.

The Subcommittee can play an important role in addressing some of the gaps in cybersecurity policy.

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 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 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.

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 and communications structures critical to new economic models, human development, free speech and privacy 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, 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 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 and 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.

Current law gives these service providers substantial authority to monitor their own systems and to disclose to the government and to their peers information about cyberattack incidents for the purpose of protecting their own networks. Appropriately, the law does not authorize ongoing, routine disclosure of traffic. 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.[6] 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

[6] 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).

trespasser"[7] 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). The subcommittee should explore with service providers how they interpret and apply these provisions in the cybersecurity context.

These provisions do not, in our view, authorize ongoing or routine disclosure of traffic by the private sector to the government. To interpret them so broadly would destroy the promise of privacy in the Wiretap Act and ECPA. Should the Subcommittee find that there is any confusion or ambiguity about this, it should consider amending these provisions to make it clear that they permit, in regards to cybersecurity, disclosure only of information relating to a suspected attack or other particular cybersecurity threat. The Subcommittee should also consider requiring public, statistical reporting on the use of these provisions to assure the public that these authorities do not devolve into a backdoor governmental monitoring system.

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. We urge the Subcommittee to approach this issue 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")[8] and the public-private partnerships represented by the Information Sharing and Analysis Centers (ISACs)[9] are

---

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

[8] 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.

[9] 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

inadequate. The Government Accountability Office (GAO) recently made a series of suggestions for improving the performance of U.S. CERT.[10] 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.

Secondly, it seems that industry self-interest, rather than government mandate, should be relied on to facilitate information sharing. The Subcommittee 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. One option, therefore, would be to compensate companies that share with a clearinghouse the cybersecurity solutions in which they have invested substantial resources. The Subcommittee might also consider whether an antitrust exemption to facilitate cybersecurity collaboration is necessary. 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 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.[11] Such

---

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.

[10] *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.

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

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 such 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.

Overall, given the risks to privacy, we urge the Subcommittee 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 urge the Subcommittee to ensure that any changes to the statute to facilitate cybersecurity measures are counterbalanced with enhanced privacy protections.

The government also 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 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 regarding private sector networks should focus on improving information sharing and otherwise strengthening the ability of the private sector to protect private sector networks.

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.[12] Such extraordinary power 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. 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 have far-reaching, unintended consequences for the economy, for the critical infrastructures themselves, and for users of those systems, which may include government personnel, state and local emergency personnel, first responders, and civilian volunteers. It could even discourage private sector operators from quickly shutting down their own networks when they should out of fear of liability for doing so, as they wait to see whether the President will order the shut down. 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.

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 responsibility to monitor and protect its own systems. At the same time, such efforts must start with the understanding that if communications Americans have with the government are routinely accessed and often shared with law enforcement and intelligence agencies, this will chill the exercise of the First Amendment rights of free speech and to petition the government. Some methods of detecting intrusions raise more privacy concerns than do others. 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.

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

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. The role of intelligence and law enforcement agencies such as the NSA and the FBI in the intrusion detection enterprise must be carefully considered. Generally, the principles of Fair Information Practices 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 the information collection and disposition.[13]

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.[14] In an effort to improve security, the government has developed and is deploying a new intrusion detection system called "Einstein 2." According to a May 19, 2008 Privacy Impact Assessment,[15] and to a January 9, 2009 opinion of the DOJ Office of Legal Counsel,[16] Einstein 2 will be deployed at participating federal agency Internet Access Points.[17] Its first full implementation was at the Department of Homeland Security. Five other federal

---

[13] 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.

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

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

[16] 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.

[17] It is unclear whether this means that Einstein 2 operates on privately owned and operated equipment or on government equipment. More importantly, it is unclear whether the network points at which Einstein is deployed handle only government traffic or could carry both government and private-to-private traffic.

agencies were supposed to begin using it by June 2009.[18] Einstein 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 IP addresses, and the alerts that Einstein 2 generates for U.S. CERT may include PII.[19] In addition to using attack signatures, Einstein 2 also detects anomalies from the norm in network traffic on a particular system and alerts U.S. CERT to those anomalies.

Press reports in the *Washington Post*[20] and *Wall Street Journal*[21] indicate that the federal government is developing a successor intrusion detection system, dubbed "Einstein 3." This new system will also rely on pre-defined signatures of malicious code that may contain PII. However, while Einstein 2 merely detected and reported malicious code, Einstein 3 is to have the capability of intercepting threatening Internet traffic before it reaches a government system, raising additional concerns.

Given these capabilities, a key question is where Einstein operates – on network elements that carry only government traffic or on elements where it might scan private-to-private communications – and how likely it is to scan private-to-private communications. According to press accounts, Einstein 3 will operate inside the networks of the telecoms. Thus, one critically important question is whether Einstein can reliably focus on communications with the government to the exclusion of private-to-private communications. If Einstein were to analyze private-to-private communications, that would likely be an interception under the electronic surveillance laws, requiring a court order. The Subcommittee may

---

[18] http://democrats.science.house.gov/Media/file/Commdocs/hearings/2009/Tech/16jun/Fonash_Testimony.pdf, p. 5.

[19] 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.

[20] http://www.washingtonpost.com/wp-dyn/content/article/2009/07/02/AR2009070202771_pf.html.

[21] http://online.wsj.com/article/SB124657680388089139.html#printMode.

want to consider legislation that would require that an independent audit mechanism be put in place as part of Einstein 3 or any similar system to ensure that no private-to-private communications are scrutinized, and require a report to Congress if they are.

Other questions about the Einstein intrusion detection system include:

- What personally-identifiable information that Einstein 2 has 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 their email communications with government employees are being scanned for security reasons? [22]

The Senate version of the Intelligence Authorization Act for FY 2010 seeks answers to similar questions. It calls for 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.[23] At any rate, the Department of Homeland Security should, of its own initiative, publish an unclassified Privacy Impact Assessment of Einstein 3, as it did for Einstein 2.

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

---

[22] 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.

[23] S. 1494 as passed by the Senate on September 16, 2009 http://intelligence.senate.gov/090722/s1494.pdf. *See* Section 340. The Senate Select Committee on Intelligence Report on the bill, 111-55, can be found here: http://intelligence.senate.gov/090722/2010report.pdf. *See* p. 22. The House version of the bill does not include a similar provision.

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.

Role of the NSA in Securing Unclassified Civilian Systems

Some have suggested that the National Security Agency 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. 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 cybersecurity for civilian unclassified systems, it would almost certainly mean less transparency, less trust, and less corporate and public participation, increasing the likelihood of failure or of ineffectiveness.

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 less. Instead, procedures should be developed for ensuring that whatever expertise and technology NSA has in discerning attacks is made available to a civilian agency.[24]

The lead for cybersecurity operations should stay with the Department of Homeland Security, and DHS's National Cyber Security Center (NCSC) should be provided with the necessary resources.

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

[24] CDT does not quarrel with the role the NSA Chief has been given as commander of the new United States Cyber Command in the Department of Defense. Securing military systems seems a proper role for the NSA.

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. 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 a transaction or interaction cannot be traced to an identifiable individual may enhance privacy and security. Moreover, the right to speak anonymously enjoys constitutional protection.[25] 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.[26] Instead of submitting personal information to 10 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. Huge design and implementation issues must be addressed to ensure that such a system enhances privacy and security rather than undermining them.

---

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

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

Identity and authentication requirements should adhere to the principles of proportionality and diversity.[27] 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, if any. 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.

The Office of Management and Budget E-Authentication Guidance for Federal Agencies[28] explained in 2003 how federal agencies should incorporate the proportionality principle into their operations in connection with government services accessed on-line. The Guidance directs federal agencies to organize their on-line transactions and interactions with the public into four risk levels that reflect the degree of harm that could flow from an authentication failure and the likelihood of such harm. For example, according the Guidance, "Level 1" interactions require no authentication and include activities such as participating by name in an online discussion on the whitehouse.gov website. In

---

[27] 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 Principles of Fair Information Practices, 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.

[28] Joshua R. Bolten, Director, Office of Management and Budget, *E-Authentication Guidance for Federal Agencies*, December 16, 2003, http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf.

contrast, a Level 3 interaction would require a much stronger level of authentication; examples might include a patent attorney submitting confidential patent information to the Patent and Trademark Office which, if improperly disclosed, would give competitors an advantage. The Guidance, of course, applies only to interactions with government systems, as is appropriate; many operators of critical systems in the private sector calready make similar risk assessments for their own unique systems and interactions and impose authentication requirements accordingly.

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 would function like keys on a key ring, with different identities for different purposes.[29] 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.

Recently, the General Services Administration took a major step in this direction by announcing three pilot programs for using user-centric identity management to improve access to government information while leveraging existing credentials for users. It has begun to set conditions that must be met by the identity credentials providers to ensure that identity providers are reliable and responsible.[30] Because the federal government is a leader in the provision of on-line services, this initiative could influence heavily the authentication and

---

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

[30] http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf. CDT's recent analysis of this initiative and of the policy issues it raises can be found here: http://www.cdt.org/privacy/Issues_for_Responsible_UCI.pdf.

identification measures adopted by the private sector, including by critical infrastructure providers.

Those who call for broad identity and authentication mandates across the Internet find no support in either the White House Cyberspace Policy Review or in the GSA initiative. We urge the Subcommittee to reject sweeping identity mandates and instead support and monitor more focused identity initiatives like the GSA's.

Conclusion

Policy makers should distinguish among different types of critical infrastructure when developing cybersecurity policy. One size does not fit all. Effective solutions 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 to ensure that "self protection" measures do not become backdoors for governmental monitoring of private networks. The Subcommittee should consider whether to craft a narrow exception from current surveillance statutes that would specifically permit communications service providers to share cyber attack information with each other and with the government to help defend other providers.

Likewise, the government should monitor its own networks for intrusion, but account for the chill to free speech and the right to petition the government that invasive monitoring could cause. Intrusion detection 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.

FOR MORE INFORMATION

Please contact: Greg Nojeim, (202) 637-9800 x 113, gnojeim@cdt.org