KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of **Leslie Harris**
President and CEO
Center for Democracy & Technology

Before the House Committee on the Judiciary,
Subcommittee on Crime, Terrorism, and Homeland Security and
Subcommittee on Intellectual Property, Competition, and the Internet

on

Cybersecurity: Innovative Solutions to Challenging Problems

May 25, 2011

Chairmen Goodlatte and Sensenbrenner, Ranking Members Scott and Watt, and Members of the Subcommittees:

Thank you for the opportunity to testify today on behalf of the Center for Democracy & Technology.[1] We applaud the Subcommittees for examining proposals to deal with challenging cybersecurity problems. This hearing could not be more timely, coming little more than a week after the White House released its cybersecurity legislative proposal.[2] Critical parts of that legislation implicate matters that are within the jurisdiction of the Judiciary Committee.

Today, I will briefly outline existing threats to our cybersecurity and discuss how to chart a path forward that ensures protection for America's cherished rights of privacy and free expression, continues to encourage innovation, and provides for meaningful improvements in security. I will emphasize that private network operators, not the government, should monitor and secure private sector systems. I will also discuss how to enhance information sharing without eroding privacy. I will examine how the Administration's cybersecurity proposals fit this framework and note areas where they do not. And I will address the issue of

---

[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 a number of working groups, including 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.

[2] Text of the White House cybersecurity legislative proposal: http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf (hereinafter, "White House proposal") Section-by-section analysis of the proposal, prepared by the White House: http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill-Section-by-Section-Analysis.pdf.

Presidential authority to shut down the Internet, an idea that the Administration wisely left *out* of its proposals.

CDT urges the Subcommittees to think carefully about the role of government in enhancing national cybersecurity. Government action is surely required in some areas, but in others government intervention would raise significant civil liberties concerns, could impede innovation, and might be counterproductive from a security standpoint. We urge the Subcommittees to take a careful, nuanced approach when crafting cybersecurity legislation and to avoid overbroad legislation and the attendant unintended consequences to individual rights and technological innovation.

The Cybersecurity Threat

The United States faces significant cybersecurity threats from state actors, from private actors motivated by financial greed, and from terrorists. In 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.[3] Early last year, Google revealed that it had been the subject of a major espionage attack originating in China aimed at stealing personal information about human rights activists and Google's own proprietary information.[4] Later in 2010, the Stuxnet worm, 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.[5] Various criminal organizations have allegedly used malware and other invasive means to defraud U.S. financial institutions of millions of dollars.[6]

The GAO, among others, has repeatedly criticized the federal government for failing to respond adequately to this threat.[7] The scope of the federal response should not be dictated by the need to react to such criticisms, however, but instead by the actual problems that lie behind them.

---

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

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

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

[6] *See, e.g.*, Federal Bureau of Investigation, New York Field Office, Press Release: Manhattan U.S. Attorney Charges 37 Defendants Involved in Global Bank Fraud Schemes that Used "Zeus Trojan" and Other Malware to Steal Millions of Dollars from U.S. Bank Accounts (September 30, 2010), http://www.fbi.gov/newyork/press-releases/2010/nyfo093010.htm.

[7] *See, e.g.,* Testimony of David A. Powner, Director, Information Technology Management Issues, Government Accountability Office, before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the House Committee on Homeland Security, *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity* (September 13, 2006), *http://www.gao.gov/new.items/d061087t.pdf*. 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* (July 2008), http://www.gao.gov/products/GAO-08-588. In 2009, GAO testified that DHS had yet to comprehensively satisfy its cybersecurity responsibilities. Testimony of Gregory C. Wilshusen, Director, Information Security Issues, before the Subcommittee on Technology and Innovation of the House Committee on Science and Technology, Government Accountability Office, *Cybersecurity,*

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. One size does not fit all. There are four important sets of distinctions to be drawn in any attempt to tackle the cybersecurity problem:

- First, a distinction must be drawn between those systems that are government-owned and those that are owned by the private sector.
- Second, distinctions must be drawn based on the degree to which the operation of particular systems is vital to the national well-being.
- Third, systems that support free speech and democratic discourse and those that do not must be distinguished.
- Fourth, threats to systems must be distinguished based on the capabilities and intentions of the originators of those threats.

Keeping these distinctions in mind when tailoring a cybersecurity policy to the needs of various systems is vital.

First, 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.

Second, particularly with respect to private systems, it is important to remember that most networks are not critical infrastructure and should not be designated as such. 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 regulatory 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.

Third, when developing policy responses, appropriate distinctions should be made between the elements of critical infrastructure that primarily support free speech and democratic participation – most prominently the Internet – 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 and free expression – may be put at risk if heavy-handed cybersecurity policies are enacted that apply uniformly to all critical infrastructure. Policies that may be appropriate for the power grid or the banking system may not be appropriate for components of the Internet used for exercising First Amendment rights to speak, associate, and petition the government.

---

*Continued Federal Efforts Are Needed to Protected Critical Systems and Information (*June 25, 2009), http://democrats.science.house.gov/Media/file/Commdocs/hearings/2009/Tech/25jun/Wilshusen_Testimony.pdf. 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.

Fourth, any cybersecurity policy must recognize that networked system security is aimed at countering a broad range of threats, from national-level actors engaging in the theft of state secrets to organized criminals engaged in financial fraud to teenage hackers testing their skills. As one cybersecurity expert has noted, it is important to "break down attacks by attribution and category."[8] Only then can the cybersecurity policy be appropriately tailored to a particular set of threats and not attempt to fit these diverse activities into the same policy framework.

For all these reasons, a sectoral, threat-specific 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 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 owned and maintained by the private sector. Private system operators know their systems best and they already monitor those systems on a routine basis to detect and respond to attacks as necessary to protect their networks; it is in their business interest to continue to ramp up these defenses.

At a top line level, all of the major cybersecurity bills, including the legislation the White House has proposed, honor the Administration's pledge. But government monitoring of private-to-private communications likely will not occur through the front door. Rather, there is a possibility that government monitoring would arise as an indirect result of information sharing between the private and public sectors or as an unintended by-product of programs put in place to monitor communications to or from the government.

Sharing Information Between the Private Sector and the Government

There is widespread agreement that the current level of cybersecurity information sharing, sharing which is essential to a robust cybersecurity program, is inadequate. Private sector network operators and government agencies monitoring their own networks could better respond to threats if they had more information about what other network operators are seeing. How to encourage more robust information sharing without putting privacy at risk is a central

[8] Scott Charney, Rethinking the Cyber Threat: A Framework and a Path Forward 7 (2009) http://download.microsoft.com/download/F/1/3/F139E667-8922-48C0-8F6A-B3632FF86CFA/rethinking-cyber-threat.pdf.

policy challenge that falls to this committee to resolve.

a. The White House Proposal

As a solution to this problem, the White House has proposed a sweeping information sharing regime that would permit any entity to share with DHS any information the entity may have, including communications traffic, no matter how it was acquired and *no matter how use and disclosure of that information would otherwise be restricted by law*, so long as the entity shares it for cybersecurity purposes, makes reasonable efforts to remove irrelevant identifying information, and complies with as-yet-unwritten privacy protections.[9] The provision would permit a vast amount of personal information to flow to and from DHS and would effectively override protections in the Wiretap Act, the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act, the Freedom of Information Act, and the Sherman Antitrust Act – statutes within the jurisdiction of the Judiciary Committee.[10] In contrast, the leading Senate cybersecurity bill explicitly requires information sharing relating to cybersecurity incidents to adhere to the statutory schemes governing electronic surveillance.[11] Communications and other information shared with the DHS by state and local governments and by private entities would be exempt from disclosure under 5 USC 552(b)(3) and comparable state laws.

Importantly, information sharing under the Administration proposal would be voluntary, not mandatory. This is wise because giving a governmental entity mandatory authority to access private sector data that is relevant to cybersecurity[12] would create a huge loophole in electronic surveillance laws and would undermine the public-private partnership that needs to develop around cybersecurity.

In other regards, however, the White House proposal raises serious concerns. Under the White House proposal, DHS could use, retain, or further disclose the communications traffic and other information to private entities and to state and local governmental entities for cybersecurity purposes, and disclose it to law enforcement entities when it is evidence of a crime. Agencies receiving communications, records, and other disclosures from DHS could use them for cybersecurity and law enforcement purposes and could further disclose them to other entities that have merely agreed in writing to use them for cybersecurity and law enforcement purposes and to abide by the as-yet-unwritten privacy protections.

The privacy and civil liberties protections in the proposal are weak and principally center on the purpose limitation: limiting information sharing to cybersecurity and law enforcement purposes. Sharing a vast amount of communications traffic could, however, fall within that broadly defined purpose. In addition, DHS would have substantial discretion about what to include in the privacy and civil liberties policies and procedures. Those policies and procedures would not be subject to notice and comment rulemaking under the Administrative Procedure Act. Importantly, the bill indicates that DHS's policies and procedures must require destruction of communications intercepted or disclosed for cybersecurity purposes that do not appear to be related to

---

[9] White House proposal, proposed Section 245 of the Homeland Security Act.

[10] It also supersedes any state statute that regulates interception, collection, use, and disclosure of communications.

[11] S. 413, Cybersecurity and Internet Freedom Act of 2011, proposed Section 246(c) of the Homeland Security Act.

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

cybersecurity threats. However, there is no effective way for an aggrieved party to enforce compliance with the policies and procedures because there is no private right of action for violations. Knowing and willful violations are misdemeanors that the Department of Justice has discretion to prosecute; they bring no prison time and fines can be no more than $5,000/incident. Companies and state and local governments that violate the law and share communications and other information for inappropriate purposes, or who fail to strip out irrelevant identifying information, or who violate the privacy policies and procedures are immune from civil and criminal liability under *all other laws* if they relied in good faith on their own determination that their conduct was permitted in the proposed statute. Finally, the DOJ – a law enforcement agency – would decide which information could be disclosed for law enforcement purposes.

We urge you to assert jurisdiction over cybersecurity information sharing within the purview of the Committee, and to take a more nuanced approach.

b. An Alternative Approach

First, Congress should determine exactly 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

[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 an Information Sharing and Analysis Center (ISAC) 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), 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 (January 2009), 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* (July 2008), http://www.gao.gov/products/GAO-08-588.

infrastructure and networks.[16] Industry is now represented at the NCCIC[17] and its presence there should facilitate the sharing of cybersecurity information about incidents.

Third, Congress must make a realistic assessment as to whether an information sharing model that puts the government at the center – receiving information, analyzing it, and sharing the resulting analysis with industry – could ever act quickly enough to respond to fast-moving threats. We have serious doubts. An industry-based model, subject to strong privacy protections, might be able to act more quickly and would raise few, if any, of the Fourth Amendment concerns associated with a government-centric model.

Fourth, Congress must account for the significant extent to which current law gives communications service providers authority to monitor their own systems and to disclose to governmental entities, and to their own 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] 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[19] and customer records[20] to any governmental or private entity.[21] 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"[22] 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.[23]

These provisions do not, in our view, authorize ongoing or routine disclosure of traffic by the private sector to any governmental entity. To interpret them so broadly would destroy the promise of privacy in the Wiretap Act and ECPA. Furthermore, the extent of service provider disclosures to the government for self-defense purposes is not known publicly. We urge the Subcommittees 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

---

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

[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] 18 U.S.C. § 2511(2)(a)(i).

[19] 18 U.S.C. § 2702(b)(3).

[20] 18 U.S.C. § 2702(c)(5).

[21] 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).

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

[23] 18 U.S.C. § 2511(2)(i).

traffic to the government under the self-defense exception.

While current law authorizes providers to monitor their own systems and to disclose voluntarily communications and records necessary to protect their own systems, the law does 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. There may be a need for a very narrow exception to the Wiretap Act, ECPA, FISA, and other laws 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. It would need to bar the disclosure to the government of vast streams of communications data, but permit liberal disclosure of carefully defined cyberattack signatures and cyberattack attribution information. It may also need to permit disclosure of communications content that defines a method or the process of a cyberattack. Rather than taking the dangerous step of overriding the surveillance statutes, such a narrow exception could operate within them, limiting the impact of cybersecurity information sharing on personal privacy.

Moreover, we urge the Subcommittees, before making any amendments that weaken the controls and privacy protections of the surveillance laws, to consider counterbalancing such changes with legislation to update ECPA by making its privacy protections more relevant to today's digital environment.[24] We would welcome the opportunity to work with the Subcommittees on such legislation.

The Government Should Monitor Its Own Networks for Intrusions, But Privacy Concerns Must 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 citizens' communication with their government implicates the exercise of the First Amendment rights of free speech and petitioning the government, which will be chilled if communications between Americans and their government are routinely shared with law enforcement and intelligence agencies. While the Fourth Amendment may not be implicated in citizen-to-government communications (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, whether to access services or to criticize government actions.

The White House proposal puts the responsibility to monitor government civilian networks right where it belongs: on the shoulders of the Department of Homeland Security (DHS). Under the bill, DHS is charged broadly with engaging in cybersecurity and information infrastructure

[24] Digital Due Process, a coalition of technology companies, communications service providers, academics, think tanks, and advocacy groups spanning the political spectrum, has proposed updates to ECPA. *See* www.digitaldueprocess.org. The Center for Democracy & Technology is a leading member of DDP.

protection for civilian government systems in what would become new Sections 243 and 244 of the Homeland Security Act. Among other things, DHS would conduct risk assessments of federal systems and maintain a cybersecurity center that would serve as a focal point for cybersecurity information flowing from other governmental agencies at the federal, state, and local level and from the private sector.

We are concerned, though, about the vast scope of the information that could flow to the DHS cybersecurity center from other federal agencies under the White House proposal. The Center would be authorized, notwithstanding any law, to intercept, retain, use, and disclose communications traffic to, from or on any federal system and to deploy countermeasures that block or modify data packets on an automated basis, for cybersecurity purposes.[25] Communications content could be retained, used, and disclosed for cybersecurity purposes when associated with a known or suspected threat, and disclosed to law enforcement when it constitutes evidence of a crime. Users of federal systems would have to be given notice of the monitoring and potential for onward disclosure, but the bill does not indicate how notice would be given. DHS would issue its own privacy and civil liberties policies and procedures in connection with this program, but there would be no independent oversight or auditing to ensure that only traffic to and from government systems is accessed, and that ECPA is not being violated through access to purely private communications. Instead, the Secretary of DHS would annually certify the department's compliance with these provisions. No penalty is specified for violations.

While we recognize the right and responsibility of the federal government to monitor its networks for intrusion, the scope of this authorization and lack of independent oversight give us pause because the legislation appears to authorize significantly more activity than is necessary to facilitate operation of the Einstein intrusion detection and prevention system.[26] At a minimum, Congress should consider requiring information collected by the center to be disposed of after a set period; requiring independent audits to ensure that only communications traffic with the government is acquired, retained, and used; and requiring DHS to provide an assessment of the federal laws that are being overridden to permit this monitoring program.

Designations of Critical Infrastructure Should be Narrowly Targeted

In terms of enhancing the security of private networks and systems, the government may assist the private sector but it should not intrude into the details of the cybersecurity planning process and it should not dictate technology standards. Private sector information technologists typically understand the operation of their own networks better than government regulators, but at the

[25] White House proposal, proposed Section 244(b) of the Homeland Security Act.

[26] The Einstein system is designed to detect and interdict malicious communications traffic to or from federal networks. It assesses network traffic against a pre-defined database of malicious signatures and detects and reports anomalies in network traffic. Einstein operates on the network of an ISP providing service to the government instead of operating on the network of the agency being protected, creating a risk that Einstein could monitor communications traffic that is not to or from a government entity. More about the program can be found in the Einstein 2 Privacy Impact Assessment (PIA) (May 19, 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf, in the PIA for the Einstein Initiative Three Exercise (March 18, 2010), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf, and in legal opinions issued by the Department of Justice concluding that the Einstein program operates lawfully: http://www.justice.gov/olc/2009/e2-issues.pdf (January 9, 2009), and http://www.justice.gov/olc/2009/legality-of-e2.pdf (August 14, 2009).

same time, certain agencies may have unique higher-level insights into burgeoning threats or useful defensive techniques.

First, government should concern itself only with genuinely *critical* infrastructure, and that infrastructure should be narrowly defined. A narrow definition focuses government resources where they are most needed and ensures minimal conflicts with other regulatory regimes. Such a definition also ensures that the burdens of government reporting and regulatory compliance are imposed only on private sector operators who are truly "critical" and limits impact on traditionally non-regulated entities. In this regard, the White House proposal raises very serious concerns. The proposal does little to provide specificity, defining critical infrastructure as those entities whose incapacity or disruption would cause "a debilitating impact."[27] This standard is ambiguous and could sweep vast swaths of U.S. industry into a regulatory fold.

The Senate's Cybersecurity and Internet Freedom Act of 2011 does a better job, and requires that the disruption of any critical infrastructure system would cause "a mass casualty event which includes an extraordinary number of fatalities," "severe economic consequences," ''mass evacuations with a prolonged absence," or ''severe degradation of national security capabilities, including intelligence and defense functions."[28] While more precise that the definition of critical infrastructure than the White House proposal, this definition, too, would benefit from more specificity. It would be useful, for example, for the statute to define the level of economic consequences that should be considered "severe" and the duration and number of evacuations that constitute a "mass evacuation with prolonged absence." DHS has already done this in its definitions of Tier 1 and Tier 2 Critical Infrastructures and Key Resources.

Risk Management Should Target Serious Threats And Eschew Heavy-Handed Mandates

After defining which systems are critical, a risk management regime should further prioritize between levels of criticality. The White House proposal does a good job of addressing this problem by asking DHS to develop risk-based tiers and to assign entities to those tiers based on threats, vulnerabilities, and consequences of an attack.[29]

When setting a risk framework for covered critical infrastructure (recognizing that the government should be setting such frameworks, if at all, only for narrowly defined and prioritized infrastructure components), the government should strive for a consultative process rather than a command-and-control structure. The White House seems to include elements of both approaches, envisioning the government in the role of standards coordinator in consultation with the private sector and respected standards-setting bodies, but also having the power to override private sector decisions about appropriate risk frameworks.[30] DHS would ask representatives of standards-setting organizations and other entities to propose standardized frameworks for assessing risk. Importantly, "frameworks" cannot require the use of particular measures; the

---

[27] White House proposal, proposed Section 3(b)(1)(A) of the Cybersecurity Regulatory Framework for Critical Infrastructure Act.

[28] S.413, Cybersecurity and Internet Freedom Act of 2011, proposed Section 254 of the Homeland Security Act and amendments to Section 210E of the Homeland Security Act.

[29] White House proposal, proposed Section 3(c) of the Cybersecurity Regulatory Framework for Critical Infrastructure Act.

[30] *Id.* at proposed Section 4(b)(4).

decision about measures to employ is left where it belongs: with the entity to which the framework applies. After consulting with those representatives, DHS would consider whether their proposed framework reasonably assesses risks, is cost-effective, has outcome-based metrics, and will sufficiently evaluate performance. If the framework comes up short, DHS can impose its own. While this approach does require DHS consultation with the private sector, it may not give DHS sufficient incentive to consider the private sector solutions before moving on to impose its own plan.

Finally, when seeking to raise standards, the government should generally avoid mandates in favor of transparency requirements and persuasion. Mandates, through which the government directly penalizes actors who fail to meet its specifications, discourage the reporting of security incidents and put the government in the role of adversary rather than partner. Some of the Senate bills have been particularly worrisome in this regard, giving DHS open-ended regulatory powers to approve security plans and to penalize actors who fail to comply with those regulations.[31]

The White House legislative draft is an improvement over those proposals. After DHS has approved or established a risk framework, each covered entity would be required to create a plan to comply with the appropriate framework and retain an independent accredited evaluator to determine its compliance with that plan. In the event of noncompliance on the part of an entity or group of entities, DHS would have the power to demand further consultation with those entities, to issue a public statement alerting citizens to the cybersecurity deficit, or to take other unspecified action, but not to impose fines, penalties, shutdown orders, or injunctive remedies requiring particular action. The bill would also require those entities to report the results of their evaluations within their SEC filings, thus disclosing cybersecurity shortcomings to shareholders and markets. In other words, the proposal uses transparency rather than mandates as a tool to encourage compliance – an approach less likely to have some of the negative impacts on innovation that mandates have.[32]

Transparency and the Role of DOD in Securing Unclassified Civilian Systems

Some have suggested that the National Security Agency (NSA) and the newly minted Cyber Command 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 Cyber Command will be better resourced than DHS to do this work.

However, there is serious concern that if NSA or another 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.

---

[31] S.413, Cybersecurity and Internet Freedom Act of 2011, proposed Section 250(c) of the Homeland Security Act (subjecting violators of Section 248 of the bill, which establishes a risk management regulatory regime, to civil penalties).

[32] The transparency called for would not tip off criminals because only high-level disclosures to the public would be made about the security plan adopted and annual performance evaluations.

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 due process and Fair Information Practice 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 and Cyber Command, for otherwise legitimate reasons, operate in a culture of secrecy that is incompatible with the information sharing necessary for the success of a cybersecurity program. As a result, a DOD entity 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; its role in monitoring private sector systems should be even smaller. Instead, procedures should be developed for ensuring that whatever expertise and technology DOD has in discerning attacks is made available to a civilian agency. The September 27, 2010, Memorandum of Understanding between DHS and DOD 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 is a good step in this direction.[33]

Presidential Authority in Cybersecurity Emergencies

There has been much discussion about whether 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.[34] The White House's implicit rejection of such powers in its legislative proposal should put this dangerous idea to rest.[35]

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. We know of no dispute where a critical infrastructure operator has refused to take appropriate action on its network that would justify the exercise of such a power. Operators have strong financial incentives to quarantine network elements and limit or cut off Internet traffic to particular systems when they need to do so. They know better than do government

[33] 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.

[34] The leading Senate cybersecurity bill, S. 413, the Cybersecurity and Internet Freedom Act, includes such a provision. For an analysis, *see http://www.cdt.org/blogs/greg-nojeim/does-senate-cyber-bill-include-internet-kill-switch.*

[35] Presumably, the government already has the authority to disconnect its own systems from the Internet and CDT does not challenge such authority.

officials whether their systems need to be shut down or isolated.

In contrast, a new Presidential "shut down" power comes with a myriad of unexamined risks. A shut down 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 and cripple communications among first responders in an emergency and would likely have worldwide effect because much of the world's Internet traffic flows through U.S. networks.

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.

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 down. Conversely, when private operators do determine that 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 as to avoid liability for the damage a shutdown could cause others.

Finally, the grant of unfettered "shut down" authority to the President would give aid and comfort to repressive countries around the world. The government of Egypt was widely condemned when it cut off Internet services to much of its population on January 27, 2011, in order to stifle dissent. The U.S. should not now endorse such a power, even if only for cybersecurity purposes, because to do so would set a precedent other countries would cite when shutting down Internet services for other purposes.

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.

Computer Fraud Law Needs Tightening Before Increased Penalties Are Considered

The White House proposal includes various amendments to the Computer Fraud and Abuse Act (CFAA).[36] The White House seeks to further broaden the reach of the CFAA, eliminate its first-time offender provisions, make CFAA violations RICO predicates, impose mandatory minimums for some violations, and add real property to the assets that can be forfeited in civil or criminal proceedings for conduct prohibited in the CFAA.

The CFAA has served as an important component of the online trust framework, giving the federal government authority to pursue cybercrime including hacking and identity theft. However, vague terms in the law have fueled troubling civil actions that have stretched the application of the law well beyond that which Congress intended. That stretching of the law has spread to criminal cases under the CFAA as well, and a number of activities having little to do with the kinds of computer "trespasses" that originally motivated Congress to pass the CFAA are now potential crimes. Before it is further expanded or its penalties increased, the statute needs to be tightened and limited to the type of computer hacking activity it was intended to

[36] 18 U.S.C. § 1030.

penalize so that it more clearly focuses on conduct that threatens cybersecurity. Only then should any expansion of CFAA penalty provisions be considered.

The CFAA imposes liability when a person accesses a computer without authorization or in excess of authorization. Courts have differed significantly on the definitions of "access" and "authorization." Some courts have interpreted unauthorized access so broadly that companies, when setting the terms of service few users will ever read, effectively determine what user conduct is "criminal." In U.S. v. Nosal,[37] the Ninth Circuit held last month that a company's former employee violated the CFAA when he acquired information from the firm's computer network and then repurposed it for his own use, because the employer had not authorized that type of access to information on its network. This prompted one online publication to headline a story about the case "Appeals Court: No Hacking Required to Be Prosecuted as a Hacker."[38] While such activity might constitute theft, or a breach of an employment contract, it is certainly not the kind of conduct that should be addressed in a cybersecurity statute.

Similarly, in the 2008 Lori Drew case, a Missouri mother who impersonated a teenage boy on MySpace in order to taunt her daughter's teenage rival was charged in California under the CFAA after the girl committed suicide. The prosecutor's theory was that Drew exceeded authorized access because the MySpace Terms of Service (TOS) did not allow users to create accounts under a false name. A federal judge overturned Drew's conviction under the CFAA.[39] While Drew's actions were reprehensible, they did not constitute "hacking" in any meaningful sense. Indeed, if violations of TOS were per se violations of the CFAA, literally millions of otherwise law-abiding Americans could be subject to criminal prosecution for signing up for a service using a false name, misrepresenting their ages, or exceeding limits on storage capacity.

Instead of addressing this vexing problem of overbreadth, the White House proposal would enhance CFAA penalties, encouraging more questionable prosecutions. Penalties for first-time offenders would be increased and in some cases more than doubled. A new mandatory minimum three-year sentence would be imposed on those who, as a component of a felonious violation of the CFAA, damage or attempt to damage a critical infrastructure computer, as long as such damage would "substantially impair" the operation of that computer. The CFAA used to have mandatory minimum sentences, but they were repealed in Section 814(f)[40] of the USA PATRIOT Act in a section captioned "Deterrence and Prevention of Cyberterrorism." Before considering new mandatory minimums, an assessment should be made as to why the old ones were repealed.

The White House proposal also makes the CFAA a RICO predicate – adding it to the list of crimes that can be used to demonstrate a "pattern of racketeering activity" to which severe criminal penalties could be applied. Notably, listing a crime under RICO allows civil plaintiffs to

---

[37] C.A. 9, 10-100038, April 28, 2011

[38] David Kravetz, Appeals Court: No Hacking Required to Be Prosecuted as a Hacker, *Wired: Threat Level* (April 29, 2011), http://www.wired.com/threatlevel/2011/04/no-hacking-required.

[39] The brief in which CDT joined in the Lori Drew case can be found here: http://www.eff.org/files/filenode/US_v_Drew/Drew_Amicus.pdf.

[40] This section required the U.S. Sentencing Commission to "amend the Federal sentencing guidelines to ensue that any individual convicted of a violation of [18 U.S.C. § 1030] can be subjected to appropriate penalties, without regard to any mandatory minimum term of punishment." It also increased potential maximum penalties under the CFAA and broadened the conduct to which it applied.

sue for triple damages for violations of that crime.[41] Because of the vagueness of the law, making the CFAA a RICO predicate could have the unintended consequence of making legitimate businesses subject to civil RICO suits for routine and normal activities. While such lawsuits may be legally groundless, their reputational impact and the prospect of treble damages and attorneys fees will often drive legitimate businesses into settling unsustainable charges. Moreover, such lawsuits would intensify the feedback loop between civil and criminal law that has led to the current overbreadth on the criminal side: as civil plaintiffs, newly incentivized to sue under the CFAA, continue to take novel theories to court, the set of activities which are considered criminal will likely continue to expand.

Finally, the proposal adds "real property" to items subject to civil forfeiture, as long as that property was used or was intended to have been used to commit or facilitate the crime. This would subject to forfeiture the house of the parents of a teenage hacker who has used a computer to attempt to break into someone's network if the parents were aware of this conduct.

The conduct constituting a violation of the CFAA must be narrowed before Congress considers legislation to extend the statute and enhance the penalties under it. As Professor Orin Kerr has suggested, clarifying the definition of "authorization" to state that only actions exceeding *code-based* authorization are sufficient to constitute a violation would improve the statute significantly.[42] Clarifying the meaning of "access" and "damage" under the statute would help as well. Even with such changes, however, some of the administration's proposals, such as mandatory minimum sentences for certain CFAA violations, would continue to raise concerns.

White House Data Breach Notification Proposal A Good Starting Point

The White House proposal would require business entities that hold "sensitive personally identifiable information" (SPII) about more than 10,000 people to notify such persons when the business entity suffers a cybersecurity breach that results in disclosure of SPII, unless the breach involves no reasonable risk of harm to the individual. Data breach notification serves cybersecurity purposes by encouraging large business entities that hold personally identifiable information to better protect that information. It also helps defend against the theft of identity, a problem that can undermine cybersecurity in some contexts. Because most states have already adopted data breach notification laws, breach notification is already effectively the law of the land.[43] The White House proposal would pre-empt those laws, which meant that it warrants special scrutiny to protect against eliminating current protections or other unintended consequences. It would wisely permit enforcement by state attorneys general, and includes an innovative provision to authorize the Federal Trade Commission to adjust the categories of SPII it is intended to protect.

Data breach notification, however, is primarily a consumer privacy matter that CDT believes should be part of comprehensive consumer privacy legislation. We urge that you not miss the forest for the trees: what is needed is legislation to protect consumer privacy in the online and offline world that incorporates the full range of Fair Information Practice Principles. The effort to

[41] 18 U.S.C. § 1964(c).

[42] Orin S. Kerr, Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes, 78 *N.Y.U. L. Rev.* pp. 1596- 1668 (November, 2003) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=399740.

[43] *See, e.g.,* http://www.cdt.org/policy/congressional-committee-revives-data-security-legislation.

adopt data breach notification should not undermine the push for baseline consumer privacy legislation. That said, we believe that if Congress does enact federal data breach notification legislation the White House proposal is a good starting point, although it should be improved as outlined below.

Definition of Sensitive Personally Identifiable Information. The definition in the White House proposal of "sensitive personally identifiable information" should include health data tied to a name or another identifier. Unless this change is made, the bill would pre-empt several state breach notice laws – such as California's[44] – that cover health data linked to the individual's name. Further, the provision empowering the FTC to modify the definition of sensitive information in rulemaking should be retained to help keep the statute up to date as technology evolves, new categories of sensitive data are put at risk, and new identifiers are developed.

Preemption. The White House proposal would override any provision of state law relating to notification by a business entity "of a security breach of computerized data," but it only requires notice of a subset of such breaches: breaches of data containing specifically defined "sensitive personally identifiable information." As a result, notice of breaches involving personally identifiable health data appears to be outside the scope of the proposed notice requirement but within the scope of the preemption section. Preemption of state law should be limited to the data covered by the federal law, permitting states to develop their own laws to address breach of information categories not covered under the proposal.

Notification Trigger. Businesses must notify consumers of data breaches involving SPII under the White House proposal unless the business determines that there is "no reasonable risk of harm or fraud to consumers." Some disclosures of personally identifiable information, such as health information, are harmful per se and the legislation should reflect that fact. "Harm" should be construed broadly to include reputational harm or embarrassment; with such a construction, this appears to be an effective trigger, which will avoid notification regarding truly inconsequential data breaches. Under this formulation, notice is the default and must be given *unless* there is an affirmative finding of no risk. We would caution against requiring notification only where harm has occurred or is likely to occur, or only where there was a determination of a significant risk of harm. If a business determines that there is no reasonable risk of harm and that it is not obligated to notify consumers of a breach, the proposal would require the business to submit its risk assessment to the FTC – a critical safeguard for which CDT has advocated.[45]

Delays for Law Enforcement. Under the White House proposal, federal law enforcement agencies can require businesses to delay notification of a breach if the agencies determine that notification would impede a criminal investigation or national security activity. While such a provision is appropriate, it should limit the duration of the periods of delay (e.g., 30 days) and require authorization by a senior law enforcement official.

---

[44] California's data breach law can be found in its Civil Code at Sections 1798.25-1798.29, http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29. The White House proposal could also be modified to include an exception, such as is found in California law, specifying that notification is not required for instances of good faith unauthorized access or acquisition of the data by employees or agents of the data holder, provided the data was not further used or disclosed in an unauthorized manner.

[45] http://www.cdt.org/copyright/20090505_data_p2p.pdf.

Targeted Authentication Requirements, Rather than Broad Attribution Requirements, are the Best Way to Address Identity Issues Online

One of the most talked-about approaches to preventing and tracing cyber attacks by terrorists and others is to make it easier to identify those who access critical systems. 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 will likely play a significant role in securing critical infrastructure, identity requirements should be applied judiciously to specific high-value targets and high-risk activities. Solutions that target high-risk systems and use proven authentication technologies to identify users are more likely to provide significant security benefits and less likely to produce undesirable economic and civil liberties consequences than solutions that attempt to use unproven technologies to identify and track users across the wider Internet.

Proposals to make Internet traffic broadly more attributable by changing IP address allocation standards, putting traceback mechanisms in place at routers, or even requiring the use of "Internet passports" raise serious civil liberties and economic concerns. Mandating increased attributability for routine Internet interactions could seriously compromise user privacy, chill freedom of expression online, and fundamentally limit the ways in which people use the Internet. 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 and must be preserved.[46]

On the other hand, promoting the use of better authentication technologies by the operators of specific targeted critical infrastructure systems can serve similar security requirements without economic and civil liberties harms. The use of authentication requirements should adhere to the principles of proportionality and diversity.[47] 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. Narrowly targeting authentication requirements only to the most critical systems helps ensure that the economic burden of compliance is minimized and that privacy and free speech are protected.

---

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

[47] 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 over and choice about identifiers needed to enroll in a system (to the extent possible), providing notice about the collection and use of personally identifiable information, securing against misuse of the information provided, requiring accountability for data processors, providing users access to their own data, and ensuring data quality.

Under the diversity principle, users should have identification and enrollment options that function like keys on a key ring, with different identities for different purposes.[48] One model that holds great promise is the "user-centric" federated 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 recently released National Strategy for Trusted Identities in Cyberspace (NSTIC) does an excellent job of advancing this model.[49] It envisions an identity eco-system led by various private sector identity providers rather than a "government ID for the Internet." 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.

Conclusion

We appreciate the opportunity to testify about innovative solutions to cybersecurity challenges. The White House proposal raises critical issues that fall squarely within the Judiciary Committee's jurisdiction and within the jurisdiction of the Subcommittees. We urge you to assert jurisdiction where appropriate, and we look forward to working with you to make progress on these important matters, while at the same time protecting the privacy rights of Americans.

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

[49] White House, National Strategy for Trusted Identities in Cyberspace (April 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.