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 Gregory T. Nojeim
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology

Before the House Committee on Homeland Security,
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

on

Draft Legislative Proposal on Cybersecurity

December 6, 2011

Chairman Lungren, Ranking Member Clarke and members of the Subcommittee:

Thank you for the opportunity to testify today on behalf of the Center for Democracy & Technology.[1] We applaud the Subcommittee for holding a hearing on draft legislation to address significant cybersecurity challenges. Clearly, cybersecurity is a growing problem that Congress needs to address, but with a careful, nuanced, and incremental approach in order to minimize the unintended consequences, such inhibiting innovation, diminishing privacy or damaging civil liberties.

We believe that the legislation you are considering is a good start in many ways and that it could use some improvements in key areas:

- The draft bill has a light regulatory touch, generally relying on market incentives rather than government mandates to increase cybersecurity performance. This approach, which we favor, encourages companies to enhance their cyber defenses without forcing compliance with government-imposed standards that could discourage security innovation.
- The regulation that the draft bill would impose extends primarily to owners and operators of critical infrastructure systems, so it is important to carefully define those systems.
- The draft bill wisely cements the role of the Department of Homeland Security as the lead federal agency for cybersecurity for the civilian government and private sectors, instead of putting an element of the Defense Department in this role.

[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.

- The draft bill appropriately avoids giving the government authority to shut down or limit Internet traffic in a "cybersecurity emergency."
- We are concerned about the information sharing provisions of the draft bill and the impact that they could have on privacy. We will share our suggested changes to those provisions.

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

One of the most important things to get right about cybersecurity – for civil liberties and for effectiveness – is to ensure that the private sector remains responsible for monitoring and protecting its own networks and that monitoring authority not be transferred, directly or indirectly, to the government. When the White House released the Cyberspace Policy Review on May 29, 2009, President Obama embraced this principle, stating:

> *"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, government monitoring would most likely grow 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. For that reason, we focus extensively here on the information sharing provisions of the draft bill. We conclude that they have benefits over the language in both the Administration bill and the Cyber Intelligence Sharing and Protection Act reported by the House Intelligence Committee on December 1 (H.R. 3523), but we also see areas that need to be clarified or otherwise improved.

Sharing Information Between the Private Sector and the Government

There is widespread agreement that the current level of cybersecurity information sharing 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 policy challenge that falls to Congress to resolve.

Preferred approach to information sharing:

CDT strongly recommends an incremental approach to the information sharing problem. First, Congress should determine exactly what information should be shared that is not shared currently, and why it is not being shared. We believe that what is most important to share is attack signatures, information describing other exploits and information identifying the source or attribution of attacks or probes. The assessment of current practices should start with an understanding of why existing structures, such as the U.S. Computer Emergency Readiness Team ("U.S. CERT")[2] and the public-private partnerships represented by the Information Sharing and Analysis Centers (ISACs),[3] are inadequate. The Government Accountability Office (GAO) has made a series of suggestions for improving the performance of U.S. CERT.[4] The suggestions include giving U.S. CERT analytical and technical resources to analyze multiple, simultaneous cyber incidents and to issue more timely and actionable warnings; developing more trusted relationships to encourage information sharing; and providing U.S. CERT sustained leadership within DHS that could make cyber analysis and warning a priority. All of these suggestions merit attention.

Second, an assessment should be made of whether the newly-established National Cybersecurity and Communications Integration Center (NCCIC) has addressed some of the information sharing issues that have arisen. The NCCIC is a round-the-clock watch and warning center established at DHS. It combines U.S. CERT and the National Coordinating Center for Communications and is designed to provide integrated incident response to protect infrastructure and networks.[5] Industry is now represented at the NCCIC[6] 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. Though the White House cybersecurity proposal[7] and the lead Senate bill, the

---

[2] 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.

[3] 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.

[4] *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.

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

[6] *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.

[7] The text and an analysis of the White House proposal are at http://www.whitehouse.gov/omb/legislative_letters.

Cybersecurity and Internet Freedom Act, (S. 413) adopt the government-centric approach, we have serious concerns about it. An industry-based model, subject to strong privacy protections, would 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 authority current law gives providers of communications service authority to monitor their own systems and to disclose to governmental entities in formation about cyberattack incidents for the purpose of protecting their own networks. In particular, the federal Wiretap Act already 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.[8] 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[9] and customer records[10] to any governmental or private entity.[11] Furthermore, the Wiretap Act provides that it is lawful for a service provider to invite in the government to intercept the communications of a "computer trespasser"[12] if the owner or operator of the computer authorizes the interception and there are reasonable grounds to believe that the communication will be relevant to investigation of the trespass.[13] These provisions do not, in our view, authorize ongoing or routine disclosure of traffic by the private sector to governmental entities but, rather, go a long way to authorizing the type of targeted information sharing that we believe is needed.

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. We believe it probably 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 be narrow so that routine disclosure of Internet traffic to the government or other entities remains clearly prohibited. It would 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.

---

[8] 18 U.S.C. § 2511(2)(a)(i).

[9] 18 U.S.C. § 2702(b)(3).

[10] 18 U.S.C. § 2702(c)(5).

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

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

[13] 18 U.S.C. § 2511(2)(i).

Information sharing in the draft bill.[14]

The draft bill establishes[15] the National Information Sharing Organization (NISO), a non-profit, quasi-governmental organization to serve as a national clearinghouse for the exchange of undefined "cyber threat information" – including information derived from intelligence collection – among owners and operators of critical and non-critical networks and systems in the private sector, the federal government, state and local governments, and educational institutions. One of its goals would be to create a "common operating picture" by combining network and cyber threat warning information shared with the federal government and with NISO members designated by its board of directors. NISO would be required by law to ensure that information exchanged is stripped of all information that identifies the submitting entity, but it would not be required by law to minimize personally identifiable information that is shared. Threat and vulnerability information derived from intelligence collection could only be shared with cleared NISO members.

DHS would select NISO's initial board of directors. That board would set procedures for future board elections and criteria for membership in NISO by non-federal entities. It would establish a governing charter setting information sharing rules for NISO and its members, including the treatment of intellectual property, limitations on liability, measures to mitigate anti-trust concerns, and protections of privacy and civil liberties. NISO would determine the extent to which its own activities would be transparent to the public – information submitted to and exchanged through NISO would be exempt from disclosure under FOIA and information it shares with state and local governments would be exempt from disclosure under state law.

Participation in NISO would be mandatory for the Departments of Energy, Defense, and Homeland Security and the FBI. Other entities such as companies, state and local governments, and academic institutions would participate voluntarily by becoming members under criteria established by the NISO board of directors and by paying membership fees determined by the board.[16] Industry representatives would dominate its board of directors, which would include representatives of small business, seven critical infrastructure sectors, DHS, the Department of Defense, the Department of Justice, the intelligence community and the privacy and civil liberties community.[17]

---

[14] In addition to the information sharing entity discussed at length below, the draft bill calls on DHS to facilitate information sharing and interactions and collaborations among federal agencies, state and local governments and academic and international partners, to disseminate timely and actionable cybersecurity threat, vulnerability and mitigation information, to compile and analyze risks and incidents regarding threats to federal systems and critical infrastructure information systems, and to provide incident detection, analysis, mitigation and response information to federal agencies and to private entities and other governmental entities that own or operate critical infrastructure. This is consistent with its duties today.

[15] It is not clear whether NISO is a newly-established non-profit, or whether an existing non-profit, or existing non-profits, would become NISO. This should be clarified.

[16] Up to 15% of NISO's annual expenses would come out of the DHS budget.

[17] Industry representatives would outnumber governmental representatives by 2-1 and would outnumber privacy and civil liberties community representatives by 5-1.

Evaluation of the proposed information sharing regime.

At a top-line level, NISO would be something of a "super ISAC." Like an ISAC, it would be convened by the government, devoted to cybersecurity information sharing, and dominated and paid for by industry. It would partner with the same governmental and private organizations that an effective ISAC would. The largest differences are that NISO is not sector specific, thus facilitating information sharing across sectors, that some of its information sharing rules are guided by statute instead of being set by its members or governing board, and its enabling statute removes any doubt that classified cybersecurity information could be shared with participating entities cleared to receive it. Whether NISO will be effective or not seems to turn on whether it addresses deficiencies in the current ISAC/U.S. CERT structures. We suggest that you measure NISO against any identified shortcomings in these existing structures to ensure that the bill does not establish a redundant information sharing entity.

We would make a number of suggestions to protect privacy and promote efficacy if the Committee determines to move forward with NISO:[18]

1. *Carefully define, with reference to existing law, the cyber threat information that can be shared with or through NISO.* It is not necessary to run a bulldozer through existing laws that protect privacy and other societal values with a provision permitting the sharing of broadly defined cyber threat information "notwithstanding any law." Such an open-ended exception would be damaging to privacy and would likely have adverse unintended effects. Both the White House information sharing proposal and the House Intelligence Committee's Cyber Intelligence Sharing and Protection Act, H.R. 3523, have this defect.[19] In contrast, CIFA, the lead Senate bill, explicitly provides that cyberattack reporting must comply with the surveillance statutes, rather than override them.[20]

2. *Restrict the purpose and use of the information being shared to cybersecurity.* Cybersecurity should not become a back door for the flow of information to the government for law enforcement purposes, or to the private sector to help it target advertising or for other commercial purposes unrelated to cybersecurity. The draft bill falls short in this area, permitting government participants in NISO to use information shared to prosecute any crime,[21] and permitting industry participants to use the information for any commercial purpose, including commercial purposes that might be at odds with the interests of the party submitting the information. While the bill permits entities submitting information to NISO to impose use and disclosure restrictions on the information when it is disclosed to officials of the U.S. government, this provides little comfort to the computer user to whom the disclosed information may pertain and whose

[18] The NISO provisions are very much a work in progress and we will be suggesting some technical clarifications to staff that are not outlined here.

[19] The House Intelligence Committee's bill defines cyber threat information so broadly that it would permit carriers to share all of the communications traffic they scan to protect their networks, and to share that traffic with the FBI, NSA and other governmental agencies. Our analysis of the bill can be found at http://www.cdt.org/blogs/greg-nojeim/112cyber-intelligence-bill-threatens-privacy-and-civilian-control.

[20] S. 413, the Cybersecurity and Internet Freedom Act of 2011, proposed Section 246(c)(1)(A)(ii) to the Homeland Security Act.

[21] Since the prosecution of cybersecurity crimes serves a cybersecurity purpose, cyber threat information shared through the NISO could be used to prosecute such crimes, including violations of the Computer Fraud and Abuse Act.

interests may not align with those of the company submitting the information. We are particularly concerned about the degree to which personally identifiable information and communications content would flow to governmental entities through the NISO. These issues should be addressed by law; rules and procedures the NISO board adopts will not be sufficient.

3. *Make the restrictions on information sharing enforceable by people and entities aggrieved by violations.* Companies that share carefully defined cyber threat information through NISO should be insulated against liability for doing so. However, if they break the rules, there should be consequences. The current draft makes it a misdemeanor for an employee of the federal government to knowingly disclose without authorization cyber threat information protected against disclosure. There are no penalties if a state or local official or an employee of a company participating in the NISO makes a similar disclosure. The bill's penalties should apply to intentional violations by state or local officials or private sector employees.

4. *Require that information sharing to and from the NISO minimize the personally identifiable information and communications content that is shared.* When cyber threat information includes PII or communications content that is not necessary to identify and respond to the threat, such information need not, and should not be shared, and the bill should so provide. Like the White House bill, it should require destruction of communications intercepted or disclosed for cybersecurity purposes that do not appear to be related to cybersecurity threats.

5. *Ensure that information sharing by NISO members is voluntary.* We assume that the bill does not intend to mandate information sharing, but proposed Section 248 in the draft bill, entitled "Voluntary Information Sharing," does not actually specify that information sharing be voluntary. Instead, the bill permits the NISO board to set the information sharing rules, which could be misread as permitting the Board to adopt a rule that would require members to share information as a condition of membership. The enabling statute should prohibit the NISO board from adopting any such rule.

6. *Enhance transparency with audits and Inspector General Reports.* DHS Inspector General should be required to issue an annual report that evaluates the efficacy of NISO's information sharing activities and their impact on privacy. These reports should be public, but may have a classified annex. The bill could also require publicly-reported independent audits to ensure that information sharing though NISO comports with statutory requirements and rules and procedures adopted by the NISO board.

7. *Consider whether information sharing through NISO should be complemented* by efforts to enhance information sharing directly within industry, subject to audits, reporting and other privacy controls. While it may have disadvantages, a distributed information sharing system may be more nimble than a centralized, hub-and-spoke model.

Cybersecurity Role of the Department of Homeland Security and of DOD Entities

The draft bill would firmly establish DHS as lead federal agency responsible for improving the security of civilian federal systems and for working with the private sector to improve the security of civilian critical infrastructure systems. Under the bill, DHS cybersecurity activities would include: conducting risk assessments of federal systems and, upon request, of privately-owned critical infrastructure information systems; facilitating adoption of new cybersecurity policies and practices; becoming a focal point within the federal government for protecting federal systems and critical infrastructure systems; coordinating among federal agencies and state and local governments, academia and international partners on cybersecurity; developing a cybersecurity incident response plan; sharing information about cyber threats and vulnerabilities and mitigation strategies with governmental agencies and with owners and operators of critical infrastructure information systems; and a host of other cybersecurity activities.

Putting DHS in the lead is the right approach, and in this regard the draft bill is superior to other proposals that could put an element of the Department of Defense – the National Security Agency or Cyber Command – formally or *de facto* at the head of civilian cybersecurity efforts. Some have suggested that these military entities be given a lead role because of their expertise and resources. We believe that to be most effective, the government's cybersecurity program should harness the expertise and resources of the DOD, but a civilian agency must remain in control of the overall program in order to ensure transparency and thereby instill trust of the private sector and the public. Less transparency means less trust, less corporate participation, and less effectiveness of the government's cybersecurity program.

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. In addition, 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, operate, understandably, in a culture of secrecy that is incompatible with the information sharing necessary for the success of a civilian 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. We applaud steps taken in this direction, such as the September 27, 2010 MOU between DHS and DOD setting forth the terms by which each agency provides personnel, equipment, and facilities to increase collaboration and support and synchronize each other's cybersecurity operations.[22]

[22] Memorandum Agreement Between DHS and DOD Regarding Cybersecurity, effective September 27, 2010, http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

Designations of Critical Infrastructure Should be Narrowly Targeted

DHS should concern itself only with genuinely *critical* infrastructure, and that infrastructure should be narrowly defined. A narrow definition focuses agency 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 network operators who are truly "critical" and limits impact on traditionally non-regulated entities.

In this regard, other cybersecurity proposals raise very serious concerns. The May 12, 2011 White House proposal does little to provide specificity, defining critical infrastructure as those entities whose incapacity or disruption would cause "a debilitating impact."[23] This standard is ambiguous and could sweep vast swaths of U.S. industry into a regulatory fold. The Senate's CIFA bill 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.''[24]

The draft bill does better than either the Administration proposal or the Senate bill. It defines covered critical infrastructure as a facility or function which, if destroyed, disrupted or accessed without authorization, through exploitation of a cyber vulnerability, would result in: (i) loss of thousands of lives; (ii) major economic disruption, including disruption or failure of financial markets; (iii) mass evacuation of a major metropolitan area for longer than 30 days; or (iv) severe degradation of national security or non-military defense functions. While more precise than the definition of critical infrastructure in either the White House proposal or in CIFA, this definition, too, would benefit from more specificity.

It would be useful, for example, for the statute to define the level of economic disruption and of lives lost that would trigger coverage as "critical infrastructure." DHS has already drawn these lines in its definitions of Tier 1 and Tier 2 Critical Infrastructures and Key Resources, and DHS uses these more precise definitions to allocate resources used to protect critical assets. If the draft bill becomes law as written, DHS would have discretion in specifying what is critical and what is not. It could draw those lines as it already has or it could draw new lines. The question for the Committee is whether Congress draws the lines that determine what assets are subject to DHS regulation or whether to leave that decision to DHS. We favor Congress drawing those lines in a transparent, precise and measureable way. We also suggest that the draft bill be amended to include a meaningful appeal process companies could trigger when they believe an asset of theirs has been incorrectly designated as "critical infrastructure."

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

[24] 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.

Incentivizing Risk-Based Conduct to Secure Critical Infrastructure

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 private sector cybersecurity planning processes and it should not dictate technology standards. Certain agencies may have unique insights into burgeoning threats, specific attack signatures, or useful defensive techniques, but private sector information technologists typically understand the operation of their own networks better than government regulators. The goal should be to enhance the capability of the private sector, not to transfer it to the government. Furthermore, when it comes to securing critical infrastructure, one size does not fit all. Existing regulatory regimes reflect this reality: the regime governing operation of a nuclear power plant is much more prescriptive that the regulatory regime governing most information technology. Cybersecurity measures should build on this insight.

The draft bill would authorize DHS, in coordination with federal agencies and owners and operators of critical infrastructure, to assess cybersecurity risks to critical infrastructure and the harms that could result from disruption, destruction or unauthorized use of critical infrastructure information systems. DHS would also catalogue internationally recognized consensus-developed risk-based performance standards and develop unspecified market-based incentives designed to encourage use of those standards. It would then coordinate with the relevant regulatory agencies and private sector entities to work to include the risk-based performance standards in the regulatory regimes applicable to the covered critical infrastructure. This approach helps ensure alignment between existing regulatory regimes and performance standards DHS has identified. In cases where there is no existing risk-based security performance standard, DHS would work with the owners and operators of critical infrastructure to mitigate identified risks and would coordinate with international bodies to develop and strengthen standards to address the identified risks.

We believe this consultative, risk-based approach will contribute to cybersecurity without inhibiting innovation. It gives DHS flexibility to draw distinctions between different types of critical infrastructure and to work with industry to identify appropriate risk based performance standards for each.

For the sake of privacy, innovation, *and* effectiveness, government efforts to improve private sector cybersecurity should adhere to several overarching principles. The government should generally avoid technical mandates. DHS in particular should not have the power to dictate technical standards or to override a company's decisions about how to best protect its information systems. Nor should DHS have any enforcement power with respect to the performance-based standards it identifies. Instead, enforcement and oversight should occur through existing regulatory schemes. When trying to raise standards, the government should generally avoid punitive measures. Penalizing companies that fall short of some standard will discourage the reporting of security incidents and will put the government in the role of adversary rather than partner.

As we understand the section of the draft bill adding a new Section 227 to the Homeland Security Act, it adheres to these principles. In contrast, 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.[25] Under the draft bill, existing regulatory regimes that already authorize a governmental agency (other than DHS) to dictate technical standards for an industry or to override decisions of a particular company would remain in place. This seems appropriate – it would leave enforcement with those agencies already set up to regulate a given sector, most of which have already been addressing cybersecurity, sometimes for years. The draft bill seeks to empower those regulators with additional knowledge about risk-based performance standards. It would encourage DHS to play a consultative, rather than a directive role, and to work with industry rather than against it. We believe the bill is intended to leave decisions about the measures a company should take to reach the necessary level of performance where those decisions belong, with the people who know those systems best - the owners and operators of critical infrastructure information systems and the regulators who intimately know the industry. It might be appropriate to amend the bill to make the foregoing more explicit, as the White House did in its own legislative proposal. [26]

For companies that operate critical infrastructure in sectors that do not have an existing regulatory regime, the bill includes no mechanism to promote the adoption of internationally recognized, consensus-driven risk-based performance standards, other than market-based incentives and the existing authority of the Federal Trade Commission, which has brought cases against companies engaging in inappropriate security practices involving consumers' personal data. While this seems to leave a gap in oversight and enforcement, we believe that there is relatively little critical infrastructure that does not fall within an existing regulatory scheme. To the extent that there are such critical infrastructure systems that do not fall within an existing scheme (other than the FTC's overarching Section 5 authority), the Committee to might consider whether it would be appropriate to require some level of transparency for companies of a certain size so that the public and/or Congress is made aware of when such companies fail to adopt and adhere to relevant standards. Any transparency requirement should not mandate disclosure of information that would tip off hackers to particular vulnerabilities.

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 or over a privately-owned[27] critical infrastructure information system in an emergency or to disconnect such systems from other networks for reasons of national security.[28] Through omission, both the draft bill, and the White House legislative package implicitly reject this dangerous idea, and we urge you to oppose any efforts that may be made to include it in any cybersecurity legislation.

---

[25] S.413, Cybersecurity and Internet Freedom Act of 2011, proposed Section 250(c) of the Homeland Security Act (civil authorizing penalties for violators of Section 248, as added by the bill, which establishes a risk management regulatory regime).

[26] White House proposal, proposed Section 4(b)(5) of the Cybersecurity Regulatory Framework for Critical Infrastructure Act.

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

[28] 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.*

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 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. These and other consequences could 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.

Conclusion

We appreciate the opportunity to testify about the draft legislative proposal that is before the Committee. We believe the legislation is in many ways a good start and that its light regulatory touch would enhance cybersecurity without stifling innovation. The bill would benefit from some substantial tightening of the information sharing provisions, and we have suggested a number of changes. We look forward to working with you on those changes and on other provisions of the draft legislation as it moves through the legislative process.