Analysis of S. 773, Cybersecurity Act of 2009

May 2009

The Rockefeller/Snowe Cybersecurity Act of 2009 fails to draw appropriate distinctions between the telecommunications sector and other critical infrastructures, and applies heavy-handed government mandates to both, putting at risk civil liberties and innovation. The bill also includes market-based proposals and measures that could properly enhance the security of critical infrastructure information systems.

On April 1, 2009, Senators John D. Rockefeller (D-WV) and Olympia Snowe (R-ME) introduced legislation designed to promote cybersecurity. CDT applauds the Senators for initiating the Congressional process this year of developing improved policy on one of the most pressing issues facing the nation. The Senators' Cybersecurity Act of 2009 (S. 773) includes a number of concepts that would enhance cybersecurity. However, the bill as introduced also has some extremely troublesome provisions: it would give the President and the Secretary of Commerce enormous power over critical infrastructure information systems maintained by private sector entities, threatening civil liberties and innovation.

The bill fails to draw appropriate distinctions between government systems and systems owned and operated by the private sector. Policy towards government systems can of course be much more "top down" and much more prescriptive than policy towards private systems. With respect to private systems, the bill fails to draw appropriate distinctions between those elements of the communications infrastructure that support free speech and those that do not. The characteristics that have made the Internet such a success – its openness, its 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 any and all infrastructure that may be considered "critical."

The Internet broadly defined is a network of networks encompassing at its edges everything from personal computers in the home to computers controlling the operation of nuclear power plants. Cybersecurity policy could be quite directive as to the systems running the nuclear power plant but should avoid regulating or restricting the "free speech supporting" elements of the Internet.

Sens. Rockefeller and Snowe have made it clear that their bill was put out to spur discussion, and that it is open for revision and improvement. CDT and others have already engaged with the Senators' staff and we look forward to working with all interested parties as legislation moves forward.

Sens. Rockefeller and Snowe introduced a companion bill (S. 778), which would establish a National Cybersecurity Advisor in the White House who would be empowered to assign cybersecurity duties to the heads of Federal entities. S. 778 is likely to be superseded by President Obama's announcement, expected any day now, of his plans for how to organize the Executive Branch, including the White House, for cybersecurity. This analysis focuses primarily on the more comprehensive bill, S. 773, the Cybersecurity Act.

Background

The Rockefeller-Snowe legislation was introduced against a growing consensus that the United States faces significant cybersecurity threats that have not been sufficiently addressed. Recently, the Wall Street Journal reported that computer hackers had penetrated systems containing designs for a new Air Force fighter jet and had stolen massive amounts of information.1 U.S. intelligence agencies, which have developed capabilities to launch cyber attacks on adversaries' information systems, have sounded alarms about what a determined adversary could do to critical information systems in the United States.

The government's response to this threat has been woefully inadequate. The Department of Homeland Security has been repeatedly criticized2 for failing to develop plans for "securing key resources and critical infrastructure of the

---

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

[2] *See, e.g.,* Government Accountability Office, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity,* http://www.gao.gov/new.items/d05827t.pdf, Testimony of GAO's David A. Powner, Director, Information Technology Management Issues, before the Subcommittee on Federal Financial Management, Government Information, and International Security of the Senate Committee on Homeland Security and Governmental Affairs, July 19, 2005. Last year, GAO reported that the Department of Homeland Security's U.S. Computer Emergency Readiness Team ("U.S. CERT"), which has significant responsibilities for protecting private and governmental computer networks, was failing to establish a "truly national capability" to resist cyber attacks. Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, http://www.gao.gov/products/GAO-08-588, July 2008.

United States, including power production, generation, and distribution systems, [and] information technology and telecommunications systems, as required in the Homeland Security Act of 2002."3 Rather than fixing what is wrong with DHS, S. 773 would create duplicative or parallel cybersecurity functions at the Department of Commerce.4

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

The Rockefeller-Snowe legislation attempts to respond to these significant cybersecurity challenges. It sets the stage for the debate over the forthcoming White House proposals. The bill's overall premise is that the federal government must step in, strongly, to protect information systems maintained by critical infrastructure providers because they have failed to protect their own systems.

While strong action is needed, a number of provisions of the bill threaten civil liberties, innovation, and in some cases, security as well. Most fundamentally, the bill fails to draw a distinction between government systems and private sector systems and fails to recognize the special sensitivity of the private sector communications infrastructure. Most of the bill's provisions apply equally to government and private sector critical infrastructure. The bill authorizes the President to designate any infrastructure as "critical." In other cybersecurity contexts, previous Presidents have deemed the communications structure that powers the Internet as "critical infrastructure." But, governmental measures that might be appropriate to secure the air traffic control system might be inappropriate for private sector systems, and measures that might be appropriate for computers at the core of the electric power grid might be inappropriate for the speech-bearing infrastructure at the edges of the Internet.

---

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

[4] S. 773 does not mention DHS despite its extensive cybersecurity role. This was probably to ensure that the Commerce Committee, which Sen. Rockefeller chairs, would have jurisdiction over the bill. As the legislative process unfolds, and as multiple committees take up the issue, it will be necessary to assemble a bill that addresses the responsibilities of agencies across committee jurisdictional lines.

[5] CDT hosted a meeting among privacy and open government advocates, and Ms. Hathaway and her key staff on March 4.

Very careful distinctions – lacking from the bill as introduced – are needed to ensure that the elements of the Internet and communications structures critical to new economic models, human development, free speech and privacy are not regulated in ways that could stifle innovation or hinder free speech.

Presidential power to shut down Internet traffic to critical infrastructure systems is unnecessary and risky: Analysis of Section 18

Two of the most troublesome provisions of the bill are Sections 18(2) and 18(6), both of which, in differing language, give the President the power to limit or shut down Internet traffic to federal government and private critical infrastructure information systems and networks. Section 18(2) permits the President to limit or shut down Internet traffic to and from any compromised critical infrastructure information system or network in an emergency.[6] It permits the President, acting unilaterally, to determine the circumstances that constitute an emergency, and it imposes no time limit on the duration of any shutdown.

Section 18(6) goes further. It gives the President the power to "order the disconnection of any Federal government or United States critical infrastructure information systems or networks in the interest of national security." No emergency is required; the term "national security" probably encompasses an ill-defined array of U.S. economic and political interests, as it has in other contexts; and President would determine what disconnections would serve the national security.

Compounding the breadth of these provisions is Section 23(3)(b) of the bill, which gives the President unfettered discretion to determine which private information systems are part of the critical infrastructure. At a minimum, these information systems include financial and banking systems, transportation systems, and systems that govern the electric power grid, but there is nothing in the bill requiring the President to develop for the computers in a nuclear power plant shut-down approaches that are different from those he might apply to the servers supporting the Google search engine.

Risks: While the President should have clear authority to limit or shut down Internet traffic to and from *governmental* systems in an emergency, exercising

[6] The President is empowered to "declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal government or United States critical infrastructure information system or network." S. 778, Section 18 paragraph (2).

such power over privately-operated systems could have far-reaching unintended consequences for the economy and for the critical infrastructures themselves. Shutting down Internet traffic 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 manufacturers of supply chain information. Even if the power were exercised only rarely, its mere existence poses other risks, enabling a President to coerce costly, questionable – even illegal – conduct by threatening to shut down a system.

No Demonstrable Need: To our knowledge, no circumstance has yet arisen that could justify a Presidential order to limit or cut off Internet traffic to a particular critical infrastructure system when the operators of that system think it should not be limited or cut off. Critical infrastructure information system providers in the private sector already have control over their systems and financial incentives to protect them from cyber attack. We understand that network operators already cooperate to quarantine network elements that seem to be infected. To our knowledge, no example has been cited where the operator refused to shut down a system that clearly needed to be shut down.

No Special Expertise in the Government: An unstated assumption of the Section 18 authority is that someone in government will be in a better position than the operators of private sector systems to determine when a system or component needs to be taken offline. Given the government's abject failure to date to protect its own systems, there is no basis for this assumption. To the extent that the government is in possession of intelligence giving it special insight, it should be developing means to share that information with the private sector system operators through mechanisms such as the DHS United States Computer Emergency Readiness Team (U.S. CERT) and the Information Sharing and Analysis Centers (ISACs).[7] To the extent system operators fail to share with each other information that would help protect their competitors or downstream systems from attack, the focus of policy attention should be on creating additional incentives for information sharing horizontally within the private sector.

---

[7] Each critical infrastructure industry sector defined in Presidential Decision Directive 63 (1998) has established an Information Sharing and Analysis Center to facilitate communication among critical infrastructure industry representatives, a corresponding government agency, and other ISACs about threats, vulnerabilities, and protective strategies. The ISACs are linked through an ISAC Council, http://www.isaccouncil.org/ and they can play an important role in critical infrastructure protection, as indicated in this white paper from January, 2009. http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf.

Perverse Incentives: Granting the President power to shut down networks could discourage desirable private sector activity. It could discourage information sharing. Private sector operators will be reluctant to share vulnerabilities and information about possible attacks if the government could use that information to shut them down. Government shutdown power could discourage private sector initiative in other ways: where speed and agility is desirable, giving the government shutdown power might lead to hesitancy on the part of private sector operators, while they wait to see if the government will act. Fearing liability if it acts on its own, a private sector operator might lose precious time while it waits for the certainty of a government directive.

◪ An effective clearinghouse for sharing information needn't have unfettered authority to seize information: Analysis of Section 14

There is widespread agreement that information sharing is an important component of an effective cybersecurity strategy and that information sharing today is inadequate. Beyond that, there is not a clear consensus on how to improve information sharing. Improving information sharing should proceed from an understanding of why existing structures are inadequate and should either fix or eliminate existing structures before creating new ones. However, probably for the jurisdictional reasons we mentioned above, S. 773 ignores the role of U.S. CERT, which already has an information sharing role, and also ignores the existing public private partnerships represented by the ISACs. Instead, Section 14 of the bill gives the Department of Commerce a new role as a clearinghouse for sharing cybersecurity threat and vulnerability information with the private sector.

It is not clear why a new information sharing structure at Commerce would be any better than DHS or any other entity at interpreting the information it receives and making it useful to governmental and private sector systems operators.

The most troublesome aspect of Section 14(b)(1) is that it gives the Secretary of Commerce the power to override any law, regulation or policy, including privacy laws and laws protecting trade secrets, to gain access to information held by private parties that might be useful to this mission. The bill imposes no limits on the scope of data the Commerce Department would access, or its subsequent use or redisclosure. The only limits would be those set by the Commerce Department itself through a notice and comment procedure.

The bill would authorize the Secretary of Commerce to override a complex set of laws intended to accommodate the dual goals of protecting privacy and providing the government and system operators with the tools they need to protect communications networks and conduct cybercrime investigations. For example, the Wiretap Act and the Stored Communications Act (SCA) already establish rules for governmental access to communications and associated traffic data flowing through information systems that are part of the critical infrastructure. Under the Wiretap Act and the SCA, system operators have authority to monitor their own systems and disclose communications to protect their networks against attack.[8] Moreover, system operators, under the computer trespasser provision,[9] have the authority to invite in the government to monitor their networks. However, if the government wants to intercept communications without a request from the service provider, the government must obtain a court order. The SCA provides similar protection for email and other communications content stored by a communications service provider. Non-content information (e.g., numbers dialed on a telephone) is also protected, but under less exacting standards. If anything, this set of laws should be updated to better protect privacy. In no case, however, is there any need to wholesale eliminate privacy protections in the name of cybersecurity.

Section 14(b)(1) could be interpreted to authorize seizure of constitutionally-protected communications content without a court order based on probable cause, creating serious constitutional concerns. It also authorizes the Commerce Secretary to obtain proprietary information and to share it with other entities – including business competitors – under rules and procedures that the Commerce Secretary would set. This threatens both innovation and competition.

The power to override all laws is unnecessary to facilitate a threat clearinghouse function. It is completely inappropriate for the communications infrastructure. Instead, any new information sharing initiative should be made subject to existing statutes and regulations that protect information, with limited exceptions where both necessary and appropriate to facilitate the sharing of cybersecurity information. Any specified exception should particularly describe the information that would be shared under the exception and should impose statutory protections for the information that is shared with the government – including use limits and restrictions on the circumstances in which it could be shared with other entities in the private sector or with law enforcement and intelligence officials.

---

[8] 18 U.S.C. Section 2511(2)(a)(i) and 18 U.S.C. 2702(b)(5).

[9] 18 U.S.C. Section 2511(2)(i).

The best approach, though, would be to fix the system already established for the sharing of this information. U.S. CERT, housed at the Department of Homeland Security, is responsible for collecting and sharing information relating to cybersecurity threats to governmental and private systems. The GAO recently made a series of suggestions for improving its performance.10 They 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. Moving this function to the Department of Commerce seems unlikely to fix the problems GAO has identified, and is likely to exacerbate some of them.

Regardless of the structure used, it seems that industry self-interest, rather than government mandate, is what needs to be enhanced to facilitate sharing of information. Congress should explore whether additional incentives need to be adopted to encourage the private sector to share threat and incident information and solutions. One option would be to compensate companies that share with the clearinghouse cybersecurity solutions in which they had to invest substantial resources. Since such information could be shared with competitors and may be costly to produce, altruism should not be expected, and compensation may be appropriate. Congress could authorize a study of how such a program would work and whether it would be effective.

Congress should consider, in lieu of giving the Commerce Department virtually unlimited authority to seize information, requiring periodic reporting of significant cybersecurity vulnerability, threat and attack information by critical infrastructure information system operators. The information reported would not include personally identifiable information. Proprietary information that is reported would have to be protected against disclosure by the government. If failure to adequately report would expose a company to fines, Congress would need to take particular care in defining the vulnerability, threat and attack information that would have to be reported. Another option would be to fine operators who fail to adequately secure their networks against specific, particularized threats the government identifies to them and equips them to handle, and to provide safe harbors and/or liability caps for those who do take such steps. Congress should also consider whether an antitrust exemption to facilitate cybersecurity collaboration is necessary.

---

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

NIST should set standards for measuring software security, rather than specifying software configuration: Analysis of Section 6

Section 6 of S. 773 concerns the key issue of standards. It would empower the National Institute of Standards to specify the configuration of software widely used in the Federal government, by government contractors and grantees, and in critical information systems and networks owned by the private sector. It would also empower NIST to establish standard configurations for security settings on operating systems and software utilities widely used in such systems. It would require all software built by or for the entities operating these systems to be tested against these standards, with the results provided to the federal government prior to deployment. Finally, it would empower the Director of NIST to enforce compliance with these NIST standards by software manufacturers, distributors and vendors, and require operators of critical infrastructure information systems to demonstrate their compliance as well.[11]

Section 6 as drafted paints with far too broad a brush, subjecting to the same requirements the computers owned and operated by the federal government, those owned by contractors and grantees, and those solely owned and operated by the private sector. Within the private sector, it makes no distinction between the computer console at a nuclear power plant and the server of a webhosting company serving a hundred small businesses and non-profits. While NIST can, and does, establish software standards for use by the Federal government, imposing mandates on software for systems used in the private sector would stifle innovation. Standardization could actually worsen security because a vulnerability in a standardized system could affect many entities. And the requirement that a governmental entity be provided security testing results for software products used in the private sector could slow deployment of software designed to enhance security.

The question of software configurations for government systems is very important and is an appropriate focus of legislative reform. A key issue is making sure that appropriate configurations are actually adhered to throughout the federal government. That reform should best come by way of amendments strengthening the Federal Information Systems Management Act (FISMA), an overhaul of which is underway. But mandatory software configurations should be limited to government systems and, possibly, to systems of contractors, especially those performing defense or intelligence-related work.

[11] *See* Sections 6(a)(5), (a)(7)(B), and (d).

In terms of the private sector, instead of dictating software configurations, NIST might have a crucial role in providing metrics for measuring the security performance of software for critical infrastructure information systems and determining whether such software meets standards for best practices set by industry, working cooperatively with NIST.

Encouraging ICANN to promote cybersecurity: Analysis of Sections 8 and 9

The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-governmental body that coordinates and oversees some elements of the Internet's Domain Name System (DNS) – the system that translates Internet addresses (e.g. www.cdt.org) into Internet Protocol (IP) numbers understood by computers. It makes it possible for computers to communicate across the Internet and allows users to efficiently navigate the network. ICANN's role is very important to the proper functioning of the Internet, but equally important is keeping that role narrowly defined and free of government interference. S. 773 sends the wrong signal to those countries – far less protective of human rights and openness than the U.S. – seeking greater government control over ICANN.

ICANN was created to move coordination and oversight of the DNS from the United States government to a private, international entity representing the worldwide Internet community. Because it is a global body, ICANN may be vulnerable to interference from foreign governments. ICANN operates under contracts with the U.S. Department of Commerce; those contracts have been vital to ICANN's independence as much for what they do not do as for what they do. So far, despite a few unwise lapses, the U.S. government has not used its limited power over ICANN to interfere with innovation, competition, and the free flow of information over the Internet. Other governments – including those with far less respect for civil liberties and the free flow of information than the U.S. government – have made it clear that they would interfere if they could. Some of those same governments would eagerly point toward any interference by Congress with ICANN to support their arguments that U.S. oversight of ICANN should end because the U.S. promotes its own self-interests, rather than the interests of stakeholders worldwide.[12]

[12] More about the delicate relationship between ICANN and the U.S. government can be found in comments CDT submitted to the Department of Commerce National Telecommunications and Information Administration on January 25, 2008 about the review of the Joint Project Agreement

Sections 8 and 9 of the Cybersecurity Act would give credibility to these international calls for greater international control of ICANN. Section 8 of the bill would subject the contract the U.S. has with ICANN for operating the Internet Assigned Numbers Authority to a national security review by the Cybersecurity Advisory Panel established in the bill. This provision will fuel arguments that the DNS should be wrested from even the "light touch" oversight the U.S. government has exercised to date, with potentially dire consequences for the Internet. It suggests that U.S. national security interests are paramount in the cybersecurity arena. Worldwide problems, like cybersecurity, demand worldwide vision. Section 8 should be dropped from the bill, or, in the alternative, altered to require the Cybersecurity Advisory Panel to make recommendations to ICANN about how to promote cybersecurity worldwide.

Section 9 of the bill would require the Assistant Secretary of Commerce for Communications and Information to develop a strategy to implement a secure domain name addressing system within three years. Such a system, known as DNSSEC, already exists. Using digital signatures and public key encryption, DNSSEC prevents an attacker from altering domain-name-to-IP-address mapping to redirect Internet traffic to the wrong destination. ICANN has not yet comprehensively implemented this system because it would rely on a public encryption key for the root of the domain name structure, and to date, no fair, reliable, trusted and efficient party has yet been identified to control the signing key. However, DNSSEC is being deployed for key domains already, and on a faster schedule than is called for in Section 9. The U.S. government is deploying DNSSEC on the .gov domain this year. Several other countries have deployed DNSSEC on their country-level domains. VeriSign, which operates the .com and .net domains, has indicated it will deploy DNSSEC by January, 2012 for both of these key domains. Other domains are likely to follow. Therefore, this problem, in our estimation, may well be resolved in fewer than three years, making Section 9 unnecessary. In the meantime, ICANN has designed an interim solution, Trust Anchor Repositories, which allow DNSSEC to work without resolving the difficult question of who should control the signing key.

---

between ICANN and the Commerce Department. http://www.cdt.org/dns/icann/20080128_CDT-JPA-comments.pdf.

Promoting market-based and other approaches to cybersecurity over government mandates: Sections 15, 10, 12 and 3.

Many laudable provisions in S. 773 could enhance cybersecurity without threatening civil liberties or innovation. Section 15 would require a study within one year of the feasibility of creating a market for cybersecurity risk management that would include civil liability, insurance and government reinsurance. This market-based approach to cybersecurity could create incentives for industry to increase the level of security implemented by critical structure information systems without imposing mandates that could have unintended consequences for security and liberty. Without even waiting for the study to be completed, the Commerce Committee could explore this approach, holding hearings expeditiously on how the market for cybersecurity risk management could be created. The hearings could include consideration of whether cybersecurity risk is adequately disclosed to shareholders of companies that may be targets of cyber attack – particularly when such attack could cause significant damage to the company.

Section 10 would authorize a cybersecurity awareness campaign focused on the public. Section 12 would authorize cyber scholarships-for-service to recruit and train information technology workers and security managers. Each could yield significant benefits. The Cybersecurity Advisory Panel in Section 3 would bring together representatives of industry, academia, state and local governments and advocacy organizations to advise the President on cybersecurity R & D, education, commercial application and societal and civil liberties concerns. This would wisely involve key stakeholders in promoting a balanced cybersecurity strategy.

Cybersecurity Advisor should provide advise and set cybersecurity strategy: Analysis of S. 778.

S. 778, companion legislation to the Cybersecurity Act, would establish in the White House an Office of the National Cybersecurity Advisor. The President would appoint Cybersecurity Advisor, subject to the advice and consent of the U.S. Senate. The Cybersecurity Advisor would give cybersecurity matters attention that is critically important at the highest level of government. He or she would advise the President on administration of laws relating to cybersecurity and would review and approve all cybersecurity budget requests made to the Office of Management and Budget The Advisor also would be empowered to direct the sponsorship of security clearances.

However, the bill also gives the Cybersecurity Advisor the power to assign cybersecurity duties to the head of any federal agency, department or other so long as they are not inconsistent with the performance of other duties. This seems an unwise delegation of operational power over cybersecurity measures to an office that is not accountable to Congress and that may operate largely in secret. Instead, the Cybersecurity Advisor should focus on giving advice to the President and on setting the general direction of cybersecurity policy government-wide. If the Director of the National Security Agency, or the Attorney General, or the Secretary of the Department of Homeland Security should be directed to do something on cybersecurity, such direction should come from the President.

Conclusion

In our view, the Rockefeller-Snowe legislation has jumpstarted a vital dialogue on the development of a more effective national cybersecurity system. It raises critical issues of information sharing, software assurance and incentives for private sector action. However, the bill as introduced paints with too broad a brush. It vests too much power with governmental entities at the expense of civil liberties and innovation, and fails to recognize the special status of those components of the Internet that have a particularly sensitive role in supporting free speech, economic innovation, and democratic activity. CDT looks forward to working with Senators Rockefeller and Snowe to improve the legislation.

CENTER FOR DEMOCRACY & TECHNOLOGY

FOR MORE INFORMATION

For more information, contact CDT Counsel Gregory T. Nojeim, 202-637-9800 x113, gnojeim@cdt.org.