# Cybersecurity and Freedom on the Internet

Gregory T. Nojeim*

> *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.*[1]

Cybersecurity has become a national imperative and a government priority. Increased cybersecurity will help protect consumers and businesses, ensure the availability of critical infrastructures on which our economy depends, and strengthen national security. However, cybersecurity efforts must be carefully tailored in order to preserve privacy, liberty, innovation, and the open nature of the Internet.[2] To design an effective and balanced cybersecurity strategy, each part of the country's critical infrastructure[3] must be considered separately. Solutions that may be appropriate for the power grid or financial networks may not be suitable for securing the public portions of the Internet that constitute the very architecture for free speech essential to our democracy. Policy toward government systems can be much more prescriptive than policy toward private systems. 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 policies are enacted

---

* Senior Counsel and Director of the Project on Freedom, Security and Technology at the Center for Democracy & Technology (CDT), a nonprofit organization dedicated to keeping the Internet open, innovative, and free. He handles much of CDT's work on electronic surveillance, the USA PATRIOT Act, and cybersecurity, and also sits on the Coordinating Committee on National Security and Civil Liberties of the American Bar Association's Section on Individual Rights and Responsibilities. The author extends his gratitude to colleague James X. Dempsey, who provided valuable assistance and guidance in the development of this article.

1. President Barack Obama, Remarks at Release of White House Cyberspace Policy Review (May 29, 2009), *available at* http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

2. *See Cybersecurity, Civil Liberties and Innovation: Hearing Before H. Comm. on Energy and Com.,* 111th Cong. (2009) (statement of Gregory T. Nojeim), *available at* http://www.cdt.org/security/20090501_cybersecurity.pdf; *Cybersecurity: Preventing Terrorist Attacks and Protecting Cyberspace: Hearing Before S. Comm. on the Judiciary, Subcomm. on Terrorism and Homeland Security,* 111th Cong. (2009), *available* at http://www.cdt.org/files/pdfs/20091117_senate_cybersec_testimony.pdf.

3. While there is no definitive list of critical infrastructure sectors, they include: energy (electrical, nuclear, gas, oil, and dams), agriculture, food, water, transportation (air, road, rail, port, waterways), information and telecommunications, banking and finance, the chemical industry, the defense industry, postal and shipping, and national monuments and icons. *See* John Moteff & Paul Parfomak, *Critical Infrastructure and Key Assets: Definition and Identification* (Cong. Res. Serv. RL32631), Oct. 1, 2004, *available at* http://www.fas.org/sgp/crs/RL32631.pdf.

that apply uniformly to any and all infrastructure that may be considered "critical."

Some cybersecurity proposals take a "one-size-fits-all" approach that ignores these nuances. This article analyzes those proposed cybersecurity measures from a civil liberties perspective. It suggests alternative approaches that would protect the privacy and liberty of Internet users and promote – rather than stifle – innovation. The article concludes that:

- Cybersecurity solutions that favor industry standards over government technology mandates will enhance security more efficiently and flexibly than those that do not.
- "Self-defense" provisions in current law already authorize communications companies to share incident information with the government in order to gain assistance in responding to a cyber attack. Instead of empowering the government to seize such information from companies or monitor private networks for attacks, incentives should be developed to encourage companies to share this information.
- Identification and authentication requirements should focus on particularly sensitive transactions and interactions, thereby preserving user anonymity for political speech and protecting the free flow of information on the Internet.
- Transparency in the cybersecurity program will build the confidence and trust that is essential to industry and public support for cybersecurity measures.

## I. THE CYBERSECURITY THREAT IS GROWING AND IS INADEQUATELY ADDRESSED

The United States faces significant, increasing cybersecurity threats. *The Wall Street Journal* has reported that computer hackers have penetrated systems containing designs for a new Air Force fighter jet and stolen massive amounts of information.[4] The *Journal* has also reported that spies have penetrated the electric power grid and left behind malicious computer code.[5] 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.[6]

---

4. *See* Siobhan Gorman et al., *Computer Spies Breach Fighter-Jet Project*, WALL ST. J., Apr. 21, 2009, at A1.

5. *See* Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, WALL ST. J., Apr. 8, 2009, at A1.

6. *See generally* NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (William A.

The government's response to this threat has been woefully inadequate. The Department of Homeland Security (DHS), which is required by statute to develop plans for "securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems" and "information technology and telecommunications systems,"[7] has been criticized repeatedly for failing to develop the required plans and for otherwise failing to develop the necessary capacity for responding to the cybersecurity challenge.[8]

In recognition of these risks and challenges, President Obama ordered his national security and homeland security advisors to examine the cybersecurity issue and develop a policy blueprint. The review team reported to the President on April 17, 2009, and its recommendations were made public on May 28, 2009.[9] While the Cyberspace Policy Review (referred to as the Review) made many useful recommendations – some of which are discussed below – their implementation seems to have been slowed by the Administration's delay in appointing an official responsible for overseeing cybersecurity implementation.[10]

## II. MEASURES TO ADDRESS THE THREAT

Cybersecurity measures can be broken down roughly into three processes, each of which poses its own special challenges: (1) learning about cybersecurity threats and intrusions; (2) hardening threat targets; and (3) responding to attacks. Policy initiatives to deal with each are discussed below.

---

Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009).

7. Homeland Security Act of 2002, Pub. L. 107-296, §201(d)(5), 116 Stat. 2135, 2146 (2002).

8. *See, e.g.*, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity*, *Hearing Before a Subcomm. of the S. Comm. on Homeland Sec. and Gov. Affairs* (Gov't Accountability Office GAO-05-827T), July 19, 2005 (statement of David A. Powner, Dir., Info. Tech. Mgmt. Issues, GAO.), *available at* http://www.gao.gov/new.items/d05827t.pdf. Last year, the Government Accountability Office (GAO) reported that the DHS's U.S. Computer Emergency Readiness Team (U.S. CERT), which has significant responsibilities for protecting private and government computer networks, was failing to establish a "truly national capability" to resist cyber attacks. *See* GOV'T ACCT. OFF., CYBER ANALYSIS AND WARNING: DHS FACES CHALLENGES IN ESTABLISHING A COMPREHENSIVE NATIONAL CAPABILITY 1 (2008), *available at* http://www.gao.gov/products/GAO-08-588.

9. CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 1 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

10. On December 22, 2009, President Obama appointed Howard Schmidt as Cybersecurity Coordinator. Schmidt had formerly served as Special Advisor for Cyberspace Security for the Bush administration and as Chief Security Strategist at both Ebay and Microsoft. *See* Ellen Nakashima & Debbi Wilgoren, *Obama To Name Former Bush, Microsoft Official as Cyber-Czar*, WASH. POST, Dec. 22, 2009, at A04.

### *A. Learning About Threats and Intrusions*

So far, government entities attempting to learn about cyber threats and intrusions have wisely and appropriately distinguished between government systems and those operated by the private sector. As an owner and operator of important computer systems and networks, the government monitors its own systems in order to develop an awareness of intrusions into those systems. In addition, if the government is to play a role in helping private sector critical infrastructure operators improve their security, it must also develop a level of understanding about those systems and the types of threats and intrusions they face. However, as President Obama has pledged, a clear line should be drawn so that the government is not in the business of monitoring traffic on private networks.

#### *1. Threats and Intrusions on Government Systems: The Einstein Intrusion Detection and Prevention System*

While the government clearly has responsibility to protect its own systems, some methods of detecting intrusions raise more privacy concerns than others. The Fourth Amendment may not come into play because those communicating with government entities necessarily reveal their communications – including content – to the government and therefore may not have a claim that they have a reasonable expectation of privacy. However, the privacy inquiry does not stop there.

Even when the government is focused on protecting its own systems, privacy issues may be raised. Most important is the question of how likely is it that private-to-private information may be accessed inadvertently through the systems intended to detect intrusions into government computers. A related question is whether there are adequate measures to ensure that the communications carriers who play an essential role in the system do not misuse their access to communications. The role of intelligence and law enforcement agencies such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) in the intrusion detection enterprise must be carefully considered. Generally, the principles of Fair Information Practices should be applied to minimize the amount of personally identifiable information collected, limit the use of this information, and notify users of the information collection and disposition.[11]

Under current law, all federal departments and agencies must adhere to information security best practices. Generally, these practices include the

11. The DHS's Chief Privacy Officer issued a memorandum in late 2008 describing how the DHS would apply principles of Fair Information Practices. *See* Memorandum from Hugo Teufel III, Chief Privacy Officer, Dept. of Homeland Sec., The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (Dec. 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policy guide_2008-01.pdf.

use of intrusion detection systems.[12] In an effort to improve security, the government has developed and is deploying a new intrusion detection system called "Einstein 2."[13] Einstein 2 will be deployed at participating federal agency Internet access points.[14] The first full implementation was at the DHS.[15] As of March 15, 2010, nine other agencies and the Executive Office of the President were also using Einstein 2.[16]

Einstein assesses network traffic against a pre-defined database of signatures of malicious code and alerts the U.S. Computer Emergency Readiness Team (U.S. CERT)[17] to malicious computer code in network traffic. While the signatures are not supposed to include personally identifiable information, as defined by the DHS, they do include Internet Protocol (IP) addresses, and the alerts that Einstein 2 generates for U.S. CERT may include personally identifiable information.[18] Einstein 2 cannot detect previously unknown attack signatures. Even a tiny change in a signature can evade the system. As a result, a new attack gets through the system until the database of attack signatures is updated. In addition to

12. *See* DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT: EINSTEIN 2, at 1, 2 (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ einstein2.pdf.

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

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

15. *See Hearing Before the Subcomm. on Tech. and Innovation of the H. Comm. on Sci. and Tech.*, 111th Cong., at 1, 5 (June 16, 2009) (statement of Dr. Peter Fonash, Acting Dir., Nat'l Cybersecurity Div., DHS), *available at* http://democrats.science.house.gov/Media/file/Commdocs/hearings/2009/Tech/16jun/Fonash_Testimony.pdf.

16. Agencies using Einstein 2 include the Departments of State, Agriculture, Education, Interior, Treasury, and Transportation, and Veterans Affairs, as well as the Securities and Exchange Commission, and the Office of Personnel Management. Correspondence between the author and Peter Sand, Director of Privacy Technology, Privacy Office, Dept. of Homeland Sec. (March 15, 2010).

17. U.S. CERT is the operational arm of the DHS's National Cyber Security Division. It helps federal agencies in the top-level "gov" domain 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.

18. Einstein 2 will collect an email address when the source of malicious code it detects is attached to an email address. *See* DEPT. OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT, *supra* note 12. Moreover any "flow record" (a specialized summary of a suspicious communication) that Einstein routinely generates will generally include IP address and time stamp, which are widely regarded as personally identifiable. *Id.*

using attack signatures, Einstein 2 also detects anomalies in network traffic on a particular system and alerts U.S. CERT to those anomalies.

The federal government is developing a successor to Einstein 2. Like its predecessor, Einstein 3 will rely on pre-defined signatures of malicious code that may contain personally identifiable information.[19] But while Einstein 2 merely detected and reported malicious code, Einstein 3 will also have the ability to intercept threatening Internet traffic before it reaches government systems. This new capability raises new concerns.

The key questions are: where does Einstein operate – on network elements that carry only government traffic or on elements that might scan private-to-private communications – and how likely is it to scan private communications? According to the DHS, Einstein 3 will operate inside the networks of private telecommunications companies.[20] Thus, another important question is whether Einstein can reliably focus on communications with the government to the exclusion of private-to-private communications. To distinguish communications to or from the government from private-to-private communications, Einstein 3 will rely on IP addresses. If communications are to or from IP addresses assigned to a government agency using the Einstein 3 system, Einstein 3 will scan them. Sometimes – but rarely – IP address allocation information can be out of date; a federal agency may think it can assign an IP address that is actually allocated to a private entity. If Einstein were to analyze private-to-private communications, it would likely be considered an interception under the electronic surveillance laws, which require a court order. An independent audit mechanism should be put in place to ensure that private-to-private communications are not scrutinized.

Already in 2010, the DHS and the Department of Justice have disclosed much more information about Einstein than was previously known. However, key information is still shrouded in secrecy. For example:

- What is the nature of the personally identifiable information that Einstein 2 has collected so far?
- What have law enforcement and intelligence agencies done with Einstein information shared with them, and, more to the point, is the system being used to identify people who should be prosecuted or people who are of intelligence interest?
- To what extent are private sector operators keeping information about communications that appear to match attack signatures?

19. DEP'T OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE INITIATIVE THREE EXERCISE 3 (2010), *available at* http://www.dhs.gov/xlibrary/assets/ privacy/ privacy_pia_nppd_initiative3.pdf.

20. *Id.*

- How should users be notified that their visits to government websites and their email communications with government employees are being scanned for security reasons?[21]

Congress is seeking answers to questions like these. The Senate version of the Intelligence Authorization Act for Fiscal Year 2010 calls for reports to Congress about the privacy impact of Einstein and other cybersecurity programs. It also calls for information about the legal authorities for cybersecurity programs and about audits conducted or planned for cybersecurity programs such as Einstein.[22]

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

### *2. Sharing Intrusion and Threat Information on Private Systems*

The challenges associated with the government's access to intrusion, threat, and vulnerability information held by private operators of critical infrastructure systems differ from those raised by the government's access to information on its own systems. Clearly, the government cannot simply search and seize communications content for cybersecurity reasons without running afoul of the Fourth Amendment, the Federal Wiretap Act, and the Electronic Communications Privacy Act (ECPA).[23] Such a search in real time would amount to a wiretap and would require judicial authorization

---

21. *See* CTR. FOR DEM. & TECH., EINSTEIN INTRUSION DETECTION SYSTEM: QUESTIONS THAT SHOULD BE ADDRESSED 1 (2009), *available at* http://www.cdt.org/security/20090728_einstein_rpt.pdf (for a fuller listing of open questions about the Einstein Intrusion Detection System).

22. *See* Intelligence Authorization Act for Fiscal Year 2010, S. 1494 §340, 111th Cong. (2009), *available at* http://intelligence.senate.gov/090722/2010bill.pdf; *see also* S. Rep. No. 111-55, at 22 (2009) (for the Senate Select Committee on Intelligence's Report on the bill), *available at* http://intelligence.senate.gov/090722/2010report.pdf. The House version of the bill does not include a similar provision.

23. The Federal Wiretap Act was enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, *codified at* 18 U.S.C. §§2510-2520. It established standards and procedures for law enforcement wiretaps and bugs (hidden microphones). The Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848, *codified at* 18 U.S.C. §§2510-2520, amended the Federal Wiretap Act to establish procedures and standards for law enforcement interception of electronic communications such as email. It also added the Stored Communications Act (18 U.S.C. §§2701-2712) to the criminal code to establish standards and procedures for law enforcement access to electronic communications in storage, as opposed to those in transit.

based on a showing of probable cause. It would also violate the President's promise that the government will not monitor private networks.

While security on private networks is primarily the responsibility of private sector operators – and they already monitor their systems on a routine basis to detect and respond to attacks quickly – the government can play a helpful role. For the government to do so, there will need to be a two-way exchange of information between the private sector and the government. To the extent that it has special expertise, the government should share that knowledge to help the private sector develop effective monitoring systems to be operated by the private sector. The government should also share with private sector network operators the information they need to determine when they are under attack, to defend themselves in real time against attacks, and to secure their networks against future attacks.

In contrast, the sharing of information the other way, by the private sector with the government, is problematic, as it implicates privacy rights and competitive commercial interests. When an attack occurs, or when events suggesting a possible attack are observed, private sector providers may need to share with the government limited information that is necessary to understand the attack, respond, and resist further attack. The Federal Wiretap Act and the ECPA contain "self-defense" provisions that are broad enough to permit the sharing of communications information held by the private sector with the government to the extent necessary to respond to an attack.[24] The self-defense provisions do not authorize private sector providers to make ongoing or routine disclosures of traffic to the government. If construed broadly, the self-defense provisions would swallow ECPA's promise of privacy. Thus these provisions should apply only when companies believe that they are or might be under attack, or that an attack has occurred.

Although laws authorize such sharing of information, actual practice has been inadequate. Still, there has not been sufficient analysis to determine what information that is not currently shared should be. Efforts to improve information sharing should begin by probing why existing structures, such as U.S. CERT and the public-private partnerships represented by the Information Sharing and Analysis Centers (ISACs),[25] are inadequate.

---

24. For example, the Federal Wiretap Act provides that it is lawful for a person acting under of law to intercept electronic communications of a computer trespasser if the owner or operator of the computer authorizes the interception and there are reasonable grounds to believe that the contents of the communication will be relevant to investigation of the trespass. 18 U.S.C.A. §2511(i) (West 2000 & Supp. 2010). *See also id.* §§2511(2)(a)(i), 2702(b)(5), 2702(c)(3). It may be necessary to supplement these self defense provisions with carefully circumscribed additional authority to share information for the purpose of protecting the networks of others, as opposed to protecting one's own network.

25. Each critical infrastructure industry sector defined in Presidential Decision Directive 63 has established Information Sharing and Analysis Centers (ISACs) to facilitate communication among critical infrastructure industry representatives, a corresponding

The Government Accountability Office (GAO) recently offered suggestions aimed at improving the performance of U.S. CERT.[26] For example, the GAO suggested that U.S. CERT: be given analytical and technical resources to analyze multiple simultaneous cyber incidents and issue more timely and actionable warnings; develop more trusted relationships to encourage information sharing; and establish sustained leadership within the DHS and make cyber analysis and warning a priority.

From the standpoint of preserving civil liberties, proposals aimed at strengthening U.S. CERT seem preferable to some others under discussion. For example, Section 14 of the Cybersecurity Act of 2009, as introduced, would have had the effect of transferring U.S. CERT's information sharing function to the Department of Commerce. It would have given Commerce the authority to override laws, regulations, and policies, including privacy laws and laws protecting trade secrets, in order to gain access to information held by private parties that might be useful to an information sharing mission.[27]

The Federal Wiretap Act and the Stored Communications Act (SCA)[28] already establish rules for government access to communications and associated traffic data flowing through information systems that are part of the critical infrastructure. Generally, under the Federal Wiretap Act, the government must obtain a court order if it wants to intercept private communications. The SCA provides similar protection for email and other communications content stored by communications service providers. "Non-content information" (for example, telephone numbers dialed) is also protected, but under less exacting standards. Section 14 of the Cybersecurity Act would have eliminated these privacy protections in the interest of enhancing cybersecurity.[29]

---

government agency, and other ISACs about threats, vulnerabilities, and protective strategies. *See* Memorandum from President William Clinton on Critical Infrastructure Protection (Presidential Decision Directive/NSC-63) (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. The ISACs are linked through an ISAC Council, and can play an important role in critical infrastructure protection. *See*, THE ROLE OF INFORMATION SHARING AND ANALYSIS CENTERS (ISACS) IN PRIVATE/PUBLIC SECTOR CRITICAL INFRASTRUCTURE PROTECTION 1 (Jan. 2009), *available at* http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf.

26. *See* GOV. ACCT. OFF., *supra* note 8.

27. *See* Cybersecurity Act of 2009, S. 773, 111th Cong., §14(b)(1), *available at* http://www.opencongress.org/bill/111-s773/text. The provision, which the authors stripped from the bill at a mark-up on March 24, 2010, at the Senate Committee on Commerce, Science and Transportation, could have been interpreted to authorize seizure of constitutionally-protected communications content without a court order based on probable cause. This would have created serious constitutional concerns.

28. *See* Federal Wiretap Act and SCA, *supra* note 23.

29. As amended on March 24, 2010 by the Senate Committee on Commerce, Science and Transportation, Section 403 of the Cybersecurity Act also empowers the President or his designee to issue rules and procedures that detail the criteria by which private sector owner of critical infrastructure will share cybersecurity threat and vulnerability information with

To facilitate a threat clearinghouse function, it is not necessary to override existing laws. Instead, new information-sharing initiatives should be developed within the context of existing statutes and regulations that protect information, with limited exceptions when both necessary and appropriate to facilitate the sharing of critical information. In such exceptional cases, there should be descriptions of the information to be shared and statutory protections imposed on any information shared with the government, including use limits and restrictions on the circumstances in which information could be shared with other private sector organizations or with law enforcement and intelligence officials.

It seems that information sharing is best served by enhancing industry self-interest, rather than imposing a broad government mandate. Congress should explore whether additional incentives need to be adopted to encourage private sector providers to share threat and incident information and solutions. Since such information could be shared with competitors and might be costly to produce, altruism should not be expected. One option would be to compensate companies that share with the government (and with their competitors) cybersecurity solutions in which they had to invest substantial resources. At the least, Congress could require a study of how such a program would work and whether it would be effective.

Currently, companies have little incentive to report network vulnerability information to the government. Who, after all, would voluntarily tell anyone that the lock on their back door is broken? Thus, additional measures should be considered to encourage the sharing of vulnerability information. The experience addressing the Year 2000 millennium software problem might be relevant. Companies could receive immunity from liability if they disclose vulnerabilities.

Other approaches, including a mandatory reporting requirement, should not be ruled out. With safeguards, Congress could require periodic reporting of significant cybersecurity vulnerability information by private sector operators of critical infrastructure information systems. Congress could also support a market for cybersecurity risk management that would include civil liability, insurance, and government reinsurance.[30] This market-based approach to cybersecurity could create incentives for industry to increase the level of security that providers implement for critical

---

the government. The marked up version of the bill is available at http://commerce.senate.gov/public/?a=Files.Serve&File_id=06b53a92-d0ec-4f77-87b1-79b038ab4840. The scope of this mandate is left unclear. *See* Cybersecurity Act of 2009, *supra* note 27.

30. Section 15 of the Cybersecurity Act as introduced recommended a study of such measures (stating that within one year after the date of enactment, the President or the President's designee, must report to Senate and House committees on the feasibility of "creating a market for cybersecurity risk management, including the creation of a system of civil liability and insurance (including government reinsurance"). *See* Cybersecurity Act of 2009, *supra* note 27, at §15(1). The provision was watered down at mark-up to require only a report on the feasibility of creating a market for cybersecurity risk management.

infrastructure information systems – without imposing mandates that could have unintended consequences for security and liberty.

Reporting of significant threat and attack information might become necessary. In such cases, the information reported would not include personally identifiable information. Proprietary information would have to be protected against disclosure by the government. Congress would need to take particular care in defining the vulnerability, threat, and attack information that would have to be reported if reporting would establish a safe harbor from liability, or if failure to report adequately would expose a company to fines.

### *B. Hardening Targets*

While a variety of measures can be adopted to make critical infrastructure systems more difficult to attack, two issues have received extensive attention: raising software and network security standards, and requiring authentication for access to sensitive systems. However, mandating standards for all critical infrastructure systems and their software building blocks would threaten both privacy and innovation. Similarly, requiring authentication for routine Internet interactions could unnecessarily hinder e-commerce and reduce user privacy.

#### *1. Software Security Standards*

Perhaps in no other cybersecurity area is the need to distinguish between public and private networks more apparent than for software security. Certainly, the government can and should set standards for its own systems. Congress provided a comprehensive framework for such standards in the Federal Information Systems Management Act (FISMA) of 2002.[31] While the FISMA empowered the National Institute of Standards and Technology (NIST) within the Commerce Department to issue standards for information systems used by the federal government,[32] there are no mechanisms for ensuring the effectiveness of measures once implemented.[33] Congress is currently considering legislation to rectify the

31. Federal Information Security Management Act of 2002, 44 U.S.C. §§3541-3549 (2006).

32. The GAO recently summarized the NIST's extensive activities in this area. *Cybersecurity: Continued Federal Efforts Are Needed To Protect Critical Systems and Information, Hearing Before Subcom. on Tech. and Innovation of the H. Comm. on Sci. and Tech.* (Gov't Accountability Office GAO-09-835T), June 25, 2009, at 15-20 (2009) (statement of Gregory C. Wilshusen, Dir. Info. Sec., GAO), *available at* http://www.gao.gov/new.items/d09835t.pdf.

33. *See id* at 23.

situation by strengthening the FISMA to require adequate security performance.[34]

Section 204 of the Cybersecurity Act, as reported by the Senate Committee on Commerce, Science, and Transportation, would empower the NIST to recognize and promote industry risk management measures and techniques, as well as best practices, for critical infrastructure information systems in the government and private sector. These measures, techniques, and best practices would have to be auditable, and each owner and operator of a critical infrastructure information system would be required to report semiannually the results of an independent audit of its compliance with this NIST-recognized industry standard. If the NIST can move quickly enough, this collaborative approach is likely to yield substantial benefits in terms of security, without the downsides of the original version of this provision.

As introduced, Section 6 of the Cybersecurity Act would have required the NIST to specify configuration of software widely used by the federal government, government contractors and grantees, and private sector operators of critical information systems and networks. It would have required 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 have empowered the director of the NIST to enforce compliance with these standards by software manufacturers, distributors, and vendors, and would also have required operators of critical infrastructure information systems to demonstrate their compliance.[35]

While the NIST can and does establish software standards for use by the federal government, it would stifle innovation if it imposed mandates on software for systems used in the private sector. Standardization could actually worsen security because a vulnerability in a standardized system could affect many entities. In addition, a requirement that all software products used in the private sector be tested against government standards could slow deployment of software designed to enhance security. The approach taken by the Senate Committee avoids these risks to innovation by requiring the NIST to recognize the standards set by industry, rather than coming up with standards independently.

The Senate Committee's approach can account for the enormous amount of work that industry has already done to establish best practices. The Information Technology ISAC has collected many of the best practices standards already adopted.[36] It would be impractical for the NIST to issue such comprehensive best practices. Industry is most likely to adopt – and adopt rapidly – the best practices it has developed itself.

---

34. *See* U.S. Information and Communications Enhancement (ICE) Act of 2009, S. 921, 111th Cong. (2009).

35. *See* Cybersecurity Act of 2009, S. 773, 111th Cong., §§6(a)(5), 6(a)(7)(B), 6(d).

36. *See* ISAC, Industry Best Practices, *available at* http://www.fsisac.com/news/industry_best_practices/.

### *2. Building Privacy into Identity and Authentication Measures*

One of the most frequently discussed approaches to preventing cyber attacks is to improve the authentication[37] of the identities of those seeking access to systems that must be protected. While identity authentication measures are important elements of cybersecurity, their effect can be either to promote privacy or put it at risk, depending on how they are designed and implemented.

To illustrate, the fact that a transaction or interaction cannot be traced to an identifiable individual may enhance privacy. The right to speak anonymously enjoys constitutional protection.[38] On the other hand, authentication can enhance privacy. For example, authenticating a party to a transaction may strengthen privacy by preventing identity fraud. Disclosing personally identifiable information might put privacy at risk, but it might also protect privacy if the data are used to establish trusted credentials that can be used for many online transactions, thereby eliminating the need to provide such information for each transaction and for many different vendors.[39] Instead of submitting personal information to ten websites in order to make ten purchases, the information could be submitted once to a credentialing organization, which would perform the authentication necessary to the other transactions.

Identity authentication requirements should adhere to the principles of proportionality and diversity.[40] Under the proportionality principle, if a transaction is rated highly significant and sensitive and potential

---

37. "Authentication" is the process of establishing confidence in users' identities electronically presented to an information system. *See* NAT'L RES. COUN., WHO GOES THERE? AUTHENTICATION THROUGH THE LENS OF PRIVACY (Stephen T. Kent & Lunette I. Millett eds., 2003), *available at* http://www.nap.edu/openbook.php?isbn=0309088968. "Individual authentication" is the process of establishing an understood level of confidence that an identifier refers to a specific individual. *Id.*

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

39. *See* CENTER FOR STRATEGIC AND INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 1, 63 (2008) [hereinafter CSIS Report], *available at* http://csis. org/files/media/csis/pubs/081208_securingcyberspace_44.pdf. The CSIS report advocates strong authentication of identity for these sectors: information and communications technology, energy, finance, and government services. *See id.* It also recognizes that authentication requirements should be proportional to the risk they address and that consumers should have choices about the authentication they use. *See id.*

40. The Center for Democracy & Technology, the author's employer, has outlined these and other Privacy Principles for Identity in the Digital Age. *See* CTR. FOR DEM. & TECH., PRIVACY PRINCIPLES FOR IDENTITY IN THE DIGITAL AGE 1 (2007), *available at* http://www.cdt.org/security/identity/20080108idprinciples.pdf (version 1.4 of the principles). The privacy principles for identity that extend beyond proportionality and diversity are based on Principles of Fair Information Practices and include specifying the purpose for the system being used, limiting the use and the retention period of personal information collected, giving individuals control and choice over identifiers needed to enroll in a system to the extent this is possible, and providing notice about collection and use of personally identifiable information, security against misuse of the information provided, accountability, access, and data quality.

authentication failure as high risk, it may be appropriate to require the collection of additional sensitive information in order to authenticate identity. This principle applies to both private and public sector operators. Private sector operators know their systems best and thus are best qualified to decide the level of identity authentication appropriate for systems and transactions. Determination of appropriate levels of authentication requires knowledge of the degree of risk posed and degree of trust that is called for.

The Office of Management and Budget explained in 2003 how federal agencies should implement the proportionality principle in connection with operations involving users accessing government services online.[41] The E-Authentication Guidance for Federal Agencies directs federal agencies to organize their online transactions and interactions with the public into four risk levels that reflect the degree of harm that could result in case of an authentication failure and the likelihood of an occurrence. According to the Guidance, level one interactions require no authentication and include such activities as participation in online discussions on whitehouse.gov. Level three interactions include submissions of confidential information, such as to the Patent and Trademark Office. If improperly disclosed, such information would cause harm by giving competitors an unfair advantage. The Guidance applies only to interactions on government systems. Operators of private critical systems make similar risk assessments for their own systems and interactions, and impose authentication requirements accordingly.

The diversity principle for privacy in identity management schemes holds that it is better to have multiple identification solutions, because use of a single identifier or credential creates a single target for privacy and security abuses. A single identifier also enables multiple transactions and interactions to be tied to that identifier, thus potentially making invasive data surveillance possible. Under the diversity principle, identification and enrollment options would function like keys on a key ring, with different identities for different purposes.[42]

The Cyberspace Policy Review recognizes the diversity and proportionality principles. The Review calls for the federal government to build a security-based identity management vision and strategy for the nation in collaboration with industry and civil liberties groups. This would be a significant undertaking. It should build on existing systems and privacy measures. The Review embraces the diversity and proportionality principles by calling for an array of interoperable identity management systems that would be used only for "high value" activities, like certain "smart grid" functions (aimed at energy efficiency), and then only after explicit user acceptance. While some have called for broader

41. *See* Memorandum from Joshua R. Bolten, Dir., Off. of Mgmt. and Budget, E-Authentication Guidance for Federal Agencies (Dec. 16, 2003), *available at* http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf.

42. *See* CTR. FOR DEM. & TECH, *supra* note 40.

authentication mandates across the Internet, the Review expresses no support for such proposals. Authentication mandates would compromise user privacy and could slow routine online interactions and transactions to the point of impacting utility.

### *C. Presidential Authority To Shut Down Networks in Response to Attacks*

Once an attack is detected, what forms of defense are appropriate?[43] One of the most troubling proposals in the Cybersecurity Act as introduced would have given the President the power to shut down or limit Internet traffic to federal government and private critical infrastructure information systems and networks. Section 18(2) of the Act would have permitted the President to limit or shut down Internet traffic to and from any compromised critical infrastructure information system or network in an emergency.[44] It would have permitted the President, acting unilaterally, to determine the circumstances that constitute an emergency and to decide which information systems are "critical" and therefore subject to this power.[45] Section 18(6) of the same bill would have gone even further by giving 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 would be required; the term "national security" probably encompasses an ill-defined array of U.S. economic and political interests, as it has in other contexts. The President would determine what systems or network "disconnections" would serve national security.

Providing the President with such powers involves risk. While the President should have clear authority to limit or shut down Internet traffic to and from *government* systems in an emergency, exercising 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

---

43. The Pentagon recently announced that it will establish a new U.S. Cyber Command that will develop offensive as well as defensive capabilities. It is beyond the scope of this article to examine the civil liberties implications of a full scale cyber war and of affirmatively mounting a cyber attack. *See, e.g.*, Lolita C. Baldor, *Pentagon Cyber Command To Create Force for Future*, ASSOCIATED PRESS FINANCIAL WIRE, May 5, 2009.

44. 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." Cybersecurity Act of 2009, S. 773, 111th Cong., §18(2).

45. The President would 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 shutdown approaches different from those he might apply to the servers supporting the Google search engine.

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 the President to coerce costly, questionable – even illegal – conduct by threatening to shut down a system.

There is no demonstrable need to provide the President with such powers. Critical infrastructure information system providers in the private sector already have control over their systems and have financial incentives to protect them from cyber attacks. They already limit or cut off Internet traffic to particular systems when they need to do so. No example has been cited when operators have refused to shut down systems that clearly needed to be shut down. As a result, it is difficult to justify giving the President power to order such a shutdown.

Moreover, there is no special expertise in the government. Proposals to give the President shutdown authority assume that government officials will be in a better position than operators of private sector systems to determine when a system or component needs to be taken offline. The government's abject failure to date to protect its own systems gives reason to question this assumption.

Finally, such authority might create perverse incentives. Granting the President authority to shut down networks could discourage information sharing. Private sector operators will be reluctant to share information about vulnerabilities and possible attacks if the government could use that information to shut them down. Private operators might become hesitant and prefer to wait to see if the government will act. Fearing liability, private sector operators might be reluctant to act independently, and they could lose precious time while waiting for a government directive.

The Senate Committee substantially modified the provisions at mark-up. As amended, Section 201 of the Cybersecurity Act requires the President to work with industry to develop and rehearse emergency response and restoration plans that clarify the roles, responsibilities, and authorities of the government and private sector actors during a cybersecurity emergency. The President would still have discretion to decide whether there is an emergency that triggers implementation of these plans. Whether or not the President would have the power in such an emergency to shut down or limit Internet traffic to a critical infrastructure information system is left unclear. The bill indicates that the emergency planning provision does not expand the President's existing authorities. But it does not indicate whether those existing authorities include the power to shut down or limit Internet traffic to a critical infrastructure information system in a cybersecurity emergency.

## III. TRANSPARENCY AND THE ROLE OF INTELLIGENCE AGENCIES IN CIVILIAN CYBERSECURITY EFFORTS

The government should disclose more than it has to date about the measures being taken to protect networks and their potential effects on business interests and the privacy of individual users. Transparency is important to two essential elements of cybersecurity: private sector cooperation and public trust.

Over eighty-five percent of critical infrastructure information systems that must be secured 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 to enhance security and whether it will be shared with competitors. Private sector cooperation with the government cybersecurity effort depends on trust, and a lack of transparency undermines trust, something that has plagued cybersecurity efforts to date.

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

Not every aspect of the program needs to be made public. In fact, there are many details that should remain classified to ensure that those attempting to breach sensitive networks are not provided with information that could aid them. For example, information collected by intelligence agencies that describe the attack signatures of foreign adversaries or their capabilities must be handled very carefully.

However, by imposing high levels of secrecy about cybersecurity, the Bush administration put the success of the program at risk. It withheld information that the public needed in order to understand the respective roles of the government and private sector, and privacy concerns. Indeed, the former Assistant Secretary for Policy at DHS under the Bush administration, Stewart A. Baker, has said that secrecy surrounding the Bush administration's cybersecurity initiative inhibited public understanding and reinforced mistrust of the intelligence community.[46]

---

46. Ellen Nakashima, *Cybersecurity Plan To Involve NSA, Telecoms; DHS Officials Debating the Privacy Implications*, WASH. POST, July 3, 2009, at A1.

Transparency is implicated in the question of which government agency should lead cybersecurity efforts. When an intelligence agency such as the NSA takes a lead role in securing civilian systems, it almost certainly means less transparency, less trust, and less corporate and public participation. It also increases the likelihood of failure or ineffectiveness. The NSA is committed – for legitimate reasons – to a culture of secrecy that is incompatible with the kind of information sharing necessary for the success of a cybersecurity program.

Distrust of the NSA relates in part to its recent involvement in secret eavesdropping activities that failed to comply with statutory safeguards. In the Terrorist Surveillance Program (TSP), the NSA eavesdropped on communications between parties in the United States and abroad when one party was thought to be an agent of al Qaeda or an affiliated terrorist organization. The Foreign Intelligence Surveillance Act (FISA) generally requires a court order for such surveillance when it targets persons in the United States.[47] Because no court orders were obtained, many believe that some surveillance under the program violated the FISA.[48] The TSP placed private sector companies that were asked to assist with the surveillance in an extremely difficult position, and those that provided assistance were exposed to massive potential liability. Given the NSA's very recent history of acting outside statutory limits, the private sector and the public at large may not trust the NSA with an expanded role in monitoring domestic cybersecurity.

The concerns with the NSA go beyond the recent activity. The NSA has long had a dual role. It spies on adversaries, cracks their computer networks, and breaks their codes. It also protects U.S. government communications from interception. These two roles tug in opposite directions because the United States and its adversaries frequently use the same technology. As a result, if the NSA finds security vulnerabilities in a widely used product, it may be inclined to keep the loophole a secret so it can exploit those vulnerabilities against its targets. The effect would be to deprive other government agencies and private operators of information they could use in defending against attacks.

This does not mean that the NSA should not play a cybersecurity role. Certainly, it can and does play a direct role in securing military and classified systems. To the extent that the NSA has developed special expertise, the government should establish a process to ensure that such

47. *See* Foreign Intelligence Surveillance Act, 50 U.S.C. §§1801-1871 (2006), *as amended by* Pub. L. No. 110-261, 122 Stat. 2436 (2008).

48. For example, fourteen former government officials and constitutional law scholars, including a former FBI Director and former attorneys in the Department of Justice Office of Legal Counsel, wrote a letter to Congress arguing that the program violated FISA. *See* Letter from Curtis Bradley et al., to Congress on NSA Spying, N.Y. REV. BOOKS, Feb. 9, 2006, at 2, *available at* http://www.nybooks.com/articles/18650.

expertise is available to any civilian agency leading cybersecurity efforts for civilian systems.

## CONCLUSION

While cybersecurity is a significant problem, solutions should not threaten user privacy and liberty or the innovation that is essential to technology development. A cybersecurity program will succeed to the extent it accomplishes the following three objectives:

- Accounts for differences among critical infrastructure systems.
- Promotes industry participation and cooperation rather than using government mandates.
- Provides transparency.