UNITED STATES DEPARTMENT OF COMMERCE

OFFICE OF THE SECRETARY,
NAITONAL INSTITUTE OF STANDARDS AND TECHNOLOGY,
INTERNATIONAL TRADE ADMINISTRATION, AND
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

In the Matter of

Cybersecurity, Innovation and the Internet Economy

Docket No. 100721305-0305-01

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

September 20, 2010

The Center for Democracy & Technology ("CDT") respectfully submits these comments in response to the Commerce Department's Notice of Inquiry regarding cybersecurity, innovation, and the Internet economy ("NOI"). CDT is a nonprofit public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the global Internet. We have been deeply involved in discussions with government agencies such as the Department of Homeland Security, with technology and communications companies, and with Congress, in working to develop cybersecurity solutions that protect civil liberties and preserve the open Internet. While it is clear that the United States faces significant cybersecurity threats from state actors, from private actors motivated by financial greed, and from terrorists, these threats can be mitigated in a way that protects privacy and promotes innovation.

The NOI asks broadly what measures should be taken to improve cybersecurity while sustaining innovation and asks stakeholders to help the Department develop an up-to-date understanding of the current public policy and operational challenges affecting cybersecurity. It seeks this information in connection with a report it is to prepare on cybersecurity, innovation, and the Internet economy. We applaud the Department for taking up this issue in a comprehensive way.

We focus our comments on approaches the Department might take to incentivize rather than to dictate private sector cybersecurity efforts. The Commerce Department should support information sharing that is necessary to cybersecurity while recognizing the extent to which the law already permits necessary information sharing. It should support careful use of government procurement power to enhance cybersecurity. Finally, to help ensure that consumer protection and privacy are built into identification and authentication programs, it should position itself to play a key role in implementing the National Strategy for Trusted Identities in Cyberspace.

A Careful and Nuanced Approach Is Required for Securing the Internet

In developing a national policy response to cybersecurity challenges, a nuanced approach is critical. It is absolutely essential to draw appropriate distinctions between government systems and systems owned and operated by the private sector. Policy towards government systems can, of course, be much more "top down" and much more prescriptive than policy towards private systems.

It is also necessary to distinguish between various private systems, especially between various elements of the Internet. While certain computers or certain networks of computers that connect to the Internet may merit one approach, other elements of the Internet may merit a very different approach. Policy toward private systems should seek to preserve the characteristics of the Internet that have made it such a success – its open, decentralized and user controlled nature and its support for innovation, commerce, and free expression. These attributes would be put at risk if heavy-handed cybersecurity policies were applied uniformly to information systems across the board.

While the Internet is a "network of networks" encompassing at its edges everything from personal computers in the home to servers controlling the operation of nuclear power plants, cybersecurity policy should not sweep all entities that connect to the network into the same basket. For example, while it is appropriate to require authentication of a user of an information system that controls the electric power grid, it would not be appropriate to require authentication of ordinary Americans surfing the Internet on their home computers. The NOI appropriately recognizes this distinction. The report the Department prepares in connection with this NOI would make a significant contribution to cybersecurity policy if it distinguishes in a principled way the elements of the Internet that can be regulated without threatening openness and innovation.

In sum, very careful distinctions – too often lacking in cybersecurity discourse – are needed to ensure that the elements of the Internet and communications structures critical to new economic models, human development, free speech and privacy are not regulated in ways that could stifle innovation, chill free speech or violate privacy.

Raising Security Standards for Information Systems

The National Institute of Standards and Technology ("NIST") can play a crucial role in developing metrics for measuring the security performance of software for information systems and determining whether such software meets risk-based performance standards set by industry, working cooperatively with NIST.

It is important that NIST not attempt to specify with particularity the configuration of software widely used in the Federal government, by government contractors and grantees and by others in the private sector. This would be an enormous undertaking of questionable benefit. It would slow innovation and threaten the development of technology, including the technologies needed for cybersecurity defense. The standardization that would result from such a heavy-handed approach could actually worsen security because a vulnerability in a standardized system could affect many entities.

Any role that NIST undertakes to test or measure security performance must be tailored to permit NIST to act with speed and agility. The Department must be careful to avoid imposing – or encouraging – a demanding, time-consuming performance evaluation process that would slow market adoption of necessary cybersecurity measures.

CDT does not object to the government judiciously using its procurement power to encourage companies to manufacture more secure software and hardware. NIST can, and does, establish software standards for software used by the Federal government. Since manufacturers prefer to design software that can be used both by the government and by the private sector, increased security standards for government systems can promote increased security for private systems. We believe that this power must be used carefully and with due consideration of the need of industry to be flexible and efficient in meeting the needs of its non-governmental customers, who may be located in the U.S or abroad. When industry has adopted a security standard that is sufficient for governmental use, it may be appropriate for NIST simply to recognize that standard for government systems.

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

When the White House released the Cyberspace Policy Review on May 29, 2009, President Obama said:

> "Our pursuit of cybersecurity will not – I repeat, will not – include monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans."

CDT strongly agrees. No governmental entity should be involved in monitoring private communications networks as part of a cybersecurity initiative. This is the job of the private sector communications service providers themselves, not of the government. Private sector operators already monitor their systems on a routine basis to detect and respond to attacks and as necessary to protect their networks, and it is in their business interest to continue to ramp up these defenses. Indeed, providing reliable networks is essential to maintaining their business.

Current law gives communications service providers substantial authority to monitor their own systems and to disclose to the government and to their peers information about cyberattack incidents for the purpose of protecting their own networks. Appropriately, the law does not authorize ongoing, routine disclosure of traffic. In particular, the federal Wiretap Act provides that it is lawful for any provider of electronic communications service to intercept, disclose or use communications passing over its network while engaged in any activity that is a necessary incident to the protection of the rights and property of the provider. 18 U.S.C. 2511(2)(a)(i). This includes the authority to disclose communications to the government or to another private entity when doing so is necessary to protect the service provider's network. Likewise, under the Electronic Communications Privacy Act (ECPA), a service provider, when necessary to protect its system, can disclose stored communications (18 U.S.C. 2702(b)(3)) and

customer records (18 U.S.C. 2702(c)(5)) to any governmental or private entity.[1] 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" [2] if the owner or operator of the computer authorizes the interception and there are reasonable grounds to believe that the communication will be relevant to investigation of the trespass. 18 U.S.C. §2511(2)(i). These provisions do not, in our view, authorize ongoing or routine disclosure of traffic by the private sector to the government. To interpret them so broadly would destroy the promise of privacy in the Wiretap Act and ECPA.

Information Sharing Can Be Improved, But First Needs Must be Concretely Identified

There is a widespread perception that cybersecurity information sharing as practiced is inadequate and there is some concern that the provisions of the Wiretap Act and ECPA are impediments to information sharing. This issue must be approached very cautiously, for exceptions intended to promote information sharing could end up severely harming privacy.

First, it should be noted that there has not been sufficient analysis to determine what information should be shared that is not shared currently. Improving information sharing should proceed incrementally. It should start with an understanding of why existing structures for critical systems, such as the U.S. Computer Emergency Readiness Team ("U.S. CERT")[3] and the public-private partnerships represented by the Information Sharing and Analysis Centers (ISACs),[4] are inadequate. The Government Accountability Office (GAO) recently made a series of suggestions for improving the

---

[1] 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).

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

[3] 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.

[4] Each critical infrastructure industry sector defined in Presidential Decision Directive 63 has established Information Sharing and Analysis Centers (ISACs) to facilitate communication among critical infrastructure industry representatives, a corresponding government agency, and other ISACs about threats, vulnerabilities, and protective strategies. See Memorandum from President Bill Clinton on Critical Infrastructure Protection (Presidential Decision Directive/NSC-63) (May 22, 1998), available at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. The ISACs are linked through an ISAC Council, and they can play an important role in critical infrastructure protection. See THE ROLE OF INFORMATION SHARING AND ANALYSIS CENTERS (ISACS) IN PRIVATE/PUBLIC SECTOR CRITICAL INFRASTRUCTURE PROTECTION 1 (Jan. 2009), available at http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf.

performance of U.S. CERT.[5] The suggestions included giving U.S. CERT analytical and technical resources to analyze multiple, simultaneous cyber incidents and to issue more timely and actionable warnings; developing more trusted relationships to encourage information sharing; and providing U.S. CERT sustained leadership within DHS that could make cyber analysis and warning a priority. All of these suggestions merit attention.

Secondly, it seems that industry self-interest, rather than government mandate, should be relied on to facilitate information sharing, and that industry-led information sharing models are more likely to be successful than government-led models. The Commerce Department should explore whether additional market-based incentives could be adopted to encourage the private sector to share threat and incident information and solutions. Since such information could be shared with competitors and may be costly to produce, altruism should not be expected, and compensation may be appropriate. One option, therefore, would be to compensate companies that share with a clearinghouse the cybersecurity solutions in which they have invested substantial resources. The Department might also consider whether an antitrust exemption to facilitate cybersecurity collaboration is necessary. Other options would be to provide safe harbors, insurance benefits and/or liability caps to network operators that share information about threats and attacks in cyberspace by terrorists and others.

CDT strongly disagrees with proposals to solve the information sharing dilemma by simply expanding government power to seize privately held data. We urge the Department to resist proposals to give the Department or any other governmental entity unfettered authority to access private sector data that is relevant to cybersecurity threats and vulnerabilities, regardless of whether the information to be accessed is proprietary, privileged or personal and without regard for any law, regulation or policy that governs governmental access, including privacy laws like the Electronic Communications Privacy Act.[6] Such an approach would be dangerous to civil liberties and would undermine the public-private partnership that needs to develop around cybersecurity. Collecting large quantities of sensitive information into a common database can also undermine security because such a database could, itself, become a target for hackers.

While, as noted above, current law authorizes providers to monitor their own systems and to disclose voluntarily communications and records necessary to protect their own systems, we have heard concern that the provisions do not authorize service providers to make disclosures to other service providers or to the government to help protect the systems of those other service providers. Perhaps it should. Many types of attacks could affect multiple providers, and disclosure by one entity about such an attack could be helpful to others. Therefore, there might be a need for a very narrow exception to the Wiretap Act and ECPA that would permit such disclosures about specific attacks

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

[6] See, e.g., Section 14 of the Cybersecurity Act of 2009 as introduced, S. 773.

and malicious code on a voluntary basis. The exception would have to be narrow so that routine disclosure of Internet traffic to the government or other service providers would remain clearly prohibited.

We believe that any such exception should be considered in the broader context of ECPA reform. Because the statute has not undergone a comprehensive update since enacted nearly a quarter century ago, ECPA has failed to keep pace with advances in technology. This has threatened consumer trust and confidence in promising new technologies that could enhance cybersecurity, including cloud computing. We discussed the role ECPA reform would have on information privacy and innovation in the Internet economy in comments we filed with the Department on June 14, 2010.[7]

Overall, given the risks to privacy, we urge the Department to take only incremental approaches to promoting information sharing, avoiding more radical approaches, such as encouraging or mandating broad sharing of Internet traffic information that may be personally identifiable.

The government also has a legitimate role, to the extent it has any special expertise, in helping the private sector develop effective monitoring systems to be operated by the private sector. The government should be sharing information with private sector network operators that will help them identify attacks at an early stage, defend in real time against attacks, and secure their networks against future attack. Most of the federal government's cybersecurity effort regarding private sector networks should focus on improving information sharing and otherwise strengthening the ability of the private sector to protect private sector networks.

Building Privacy Into Identity and Authentication Requirements Designed To Thwart or Discourage Malicious Activity

One of the most talked-about approaches to preventing and tracing cyber attacks is to improve identity and authentication of those who would seek access to the system that must be protected. If an attack cannot be attributed to a particular person because the person cannot be identified, it is difficult to prosecute the perpetrator. While identification and authentication will likely play a significant role in securing critical infrastructure, identity and authentication requirements should be applied judiciously to specific high value targets and high-risk activities.

Some have argued for broad authentication mandates across the Internet – including calls for "Internet passports." However, mandating strong identity and authentication measures for routine Internet interactions could seriously compromise user privacy, slow on-line interactions and transactions so much that their utility would be impaired, and fundamentally limit the ways in which people use the Internet. Identity technologies are very promising, but care must be taken to ensure that all stakeholders are represented in developing the systems for private sector and government.

---

[7] Comments of the Center for Democracy & Technology in Docket No. 100402174-0175-01, Information Privacy and Innovation in the Internet Economy, June 14, 2010, *available at* http://www.cdt.org/files/pdfs/20100613_doc_privacy_noi.pdf.

The National Strategy for Trusted Identities in Cyberspace ("the Strategy"), released by the White House for comment on June 25, 2010, warrants an in-depth discussion. The Department of Commerce is uniquely suited to develop a set of best practices and standards to implement the Strategy. A national strategy should define the desired attributes for an identity ecosystem, recommend government incentives for the creation or adoption of online identity, delineate the differing roles of government and the private sector, and explicitly address how privacy, free expression and other values will be preserved.

a. New Identity Technologies Carry Great Promise, but Associated Risks Must Be Carefully Considered

The new identity systems envisioned in the Strategy and the National Broadband Plan have significant promise. User-centric identity has the potential to be a boon to privacy and security. However, the technology and policy frameworks supporting new identity systems must be appropriately designed and deployed. Accordingly, it is crucial that the risks associated with new identity systems be carefully considered and discussed. For example, centralizing data into identity systems increases the risk of a data breach, and creates more targets for criminal enterprises. In addition, federated identity must be properly paired with strong policies and requirements for ecosystem members in order to ensure a high level of trust.

There is skepticism from privacy and security advocates that user-centric federated identity will be implemented in ways that maximize the potential of these technologies for consumers, industry, and government. Including at the outset policies to protect consumers and ensure privacy is key to consumer trust and large-scale adoption across public and private sectors.

b. The Strategy Should Focus on Guiding and Nurturing the Nascent Identity Ecosystem, Not Establishing a Government-Centric Identity Scheme

The Strategy has the potential to contribute significantly to the development of better online identities for governmental and commercial purposes. However, the Strategy's current focus on the use of government credentials for private transactions is cause for concern. A pervasive, government-run online authentication scheme is incompatible with fundamental American values and antithetical to the user-empowering and user-controlled nature of the Internet.

Instead, the Strategy – and any Department actions – should focus on guiding and nurturing the nascent identity ecosystem. The Strategy, while laying out several possible use cases for an identity ecosystem, fails to discuss important aspects of a trust framework that will establish a successful adoption process. Creating an identity ecosystem requires standards, interoperability, and well-articulated responsibilities and roles. Work by the Department, NIST, and NTIA in this sphere would greatly contribute to the identity management ecosystem both inside and outside government. Furthermore, the government could endorse market-driven schemes and implement a certification/audit regime. There is ample opportunity for productive engagement with other identity ecosystem stakeholders to further develop standards and technologies.

c. The Strategy Should be Implemented by the Department of Commerce

The Department of Commerce should position itself to lead or to play a key role in the implementation of the National Strategy for Trusted Identity in Cyberspace. Identity and authentication will be critical to many on-line interactions and much on-line commerce. It will support transactions that have little to do with national security. The Commerce Department has both the knowledge and expertise necessary to define practices and policies for the identity ecosystem, and has a public-facing mission that is consistent with ensuring participation by the nation's identity infrastructure and encouraging the commercial sector to participate as well.

Conclusion

We applaud the Department of Commerce for taking up the issue of cybersecurity and placing it within the context of innovation and the economy. We encourage the Department to favor incentives to private industry over security mandates, which could stifle innovation and slow adoption of necessary cybersecurity technologies. The Department should consider economic incentives to encourage the sharing of cybersecurity threat, vulnerability and incident information and should favor information sharing models that are industry led and operated. Finally, the Department should play a key role in implementing the National Strategy for Trusted Identity in Cyberspace, by nurturing and incentivizing the already developing identity ecosystem and working to ensure that privacy, free expression, and other values are preserved in identification and authentication programs.

For further information, please contact Gregory T. Nojeim, Senior Counsel, Center for Democracy & Technology, 202/407-8833, gnojeim@cdt.org.