KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

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

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

BEFORE THE DEPARTMENT OF COMMERCE

NATIONAL 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. 110527305-1303-02

August 8, 2011

The Center for Democracy & Technology ("CDT") respectfully submits these comments in response to the Commerce Department's Internet Policy Task Force June 2011 green paper titled "Cybersecurity, Innovation and the Internet Economy." CDT is a nonprofit public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the global Internet.

The green paper deals broadly with establishing a framework for the cybersecurity challenges faced by companies outside the critical infrastructure and key resources designation. In particular, the green paper identifies an "Internet and Information Innovation Sector" ("I3S") and lays out several policy recommendations intended to help this sector develop security best practices and voluntary codes of conduct as well as incentivize private sector cybersecurity efforts. We applaud the Department for taking up this issue. We believe the Department's overall approach to non-critical network security is essentially the right one, with a focus on incentives, transparency and best practices promoted through voluntary, collaborative endeavors with private industry.

However, while it is useful to distinguish between critical and non-critical systems, and while it is appropriate to develop government policy for improving the security of non-critical information and communications systems, we want to warn at the outset of our comments that the distinction can also be misleading. The green paper recommends an approach to cybersecurity policy for non-critical infrastructures that is based on voluntary standards, public-private cooperation, transparency, respect for privacy, and the protection of innovation. Yet those very same principles should also govern the framing of policy for critical infrastructures, and it would be a mistake to take the distinction between critical and non-critical infrastructures as suggesting otherwise.

Whether one is focused on critical or non-critical systems, the government should be hesitant to dictate technical standards for privately owned and operated systems. Whether one is focused on critical or non-critical systems, the government should not monitor private traffic flowing over private networks; monitoring private sector networks should be the responsibility of the private sector. In developing cybersecurity policies for both the critical and non-critical infrastructure, it is important to avoid stifling innovation. With respect to both critical and non-critical systems or services, it is necessary when developing cybersecurity policy responses to draw appropriate distinctions between infrastructure elements and services that primarily support free speech and those that do not. The characteristics that have made the Internet such a success – its open, decentralized and user-controlled nature and its support for innovation, commerce, and free expression – may be put at risk if heavy-handed cybersecurity policies are applied uniformly either to "critical infrastructure" or to non-critical elements. We support the light regulatory touch the Department takes in this green paper with respect to non-critical services and functions, but we also believe that government mandates are equally inappropriate for many critical systems and assets essential to the operation of the Internet. The Department should re-emphasize these points in its future contributions to the development and implementation of the Administration's cybersecurity policy.

The I3S Definition Requires Further Clarification and Refinement

The green paper focuses on cybersecurity efforts associated with an "Internet and Information Innovation Sector" ("I3S") that it defines as encompassing the following four functions and services:

- provision of information services and content;
- facilitation of the wide variety of transactional services available through the Internet as an intermediary;
- storage and hosting of publicly accessible content; and
- support of users' access to content or transaction activities, including, but not limited to application, browser, social network, and search providers.

The green paper indicates that the definition of this sector was motivated by a desire to "capture functions and services that fall outside the classification of covered critical infrastructure and have a large potential for growth, entrepreneurship, and vitalization of the economy." CDT supports the goal of identifying non-critical functions and services that will be subject to a lighter regulatory touch than those that are critical. This endeavor is particularly important because proposed definitions of the critical systems and assets that have appeared in legislative proposals are vague and lack specificity. By defining with particularity that which is non-critical, the Commerce Department may help Congress, the public and industry better understand that which is critical.

However, the distinction between "critical" and "non-critical" may not be the most important distinction that needs to be drawn in order to ensure that cybersecurity efforts are consistent with privacy, free expression, innovation and other values. In our previous comments on the NOI, we noted that the green paper "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." Unfortunately, the green paper does not address that concern. Very careful distinctions – too often lacking in cybersecurity discourse – are

needed to ensure that the elements of the Internet that serve as the basis for new economic models, human development, and civic engagement (whether those elements of the Internet are defined as critical or non-critical) are not regulated in ways that could stifle innovation, chill free speech, or violate privacy.[1]

We pose one question about the definition of the I3S sector and suggest an improvement. First the question: How does the I3S sector differ from the Information Technology sector plus the Communications sector that have been defined as critical by the Department of Homeland Security? In the sector-specific National Infrastructure Protection Plans, the Information Technology sector is defined as technologies that: provide IT products and services, provide incident management capabilities, provide domain name resolution services, provide identity management and associated trust support services, provide Internet-based content, information, and communications services, or provide Internet routing, access and connection services. The Communications sector is defined to include the nation's wireline infrastructure (including the PSTN, the Internet, and all other "next-generation" or packet-switched networks) and the nation's wireless infrastructure (including cellular phone, paging, personal communications services, high-frequency radio, unlicensed wireless, and other commercial and private radio services), as well as satellite and cable infrastructure. These technologies seem to encompass virtually all of the I3S functions and services laid out in the green paper.

If indeed the I3S encompasses all or most of the Information Technology sector and Communications sector, perhaps it would make more sense to simply continue employing the phrase "IT and communications sector" and to indicate that the green paper is proposing a framework for increasing the cybersecurity of the non-critical functions and services of that sector, instead of indicating that it is concerned with a new sector. If however, there are clear distinctions between what is intended to be covered under the I3S definition and what is covered by the IT and Communications sectors, it would be helpful to clarify the I3S definition to highlight these distinctions and explain the need for this new designation.

Beyond concerns that the I3S definition may be redundant, it would be helpful if the Commerce Department explained how the I3S definition is intended to mesh with the DHS designations of covered critical infrastructure under the pending White House legislative proposal. In particular, DHS designations of covered critical infrastructure in the Administration's proposed cybersecurity legislation http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Cybersecurity-Regulatory-Framework-for-Covered-Critical-Infrastructure-Act.pdf apply to entire entities, while the Department's I3S definition focuses on specific functions and services. The green paper does not clarify what this will mean for companies that own critical infrastructure networks and also provide I3S functions or services. Given how broad the I3S definition is, we believe this overlap is likely to apply to many — if not all — entities designated as covered critical infrastructure. The Commerce Department should clarify how the I3S definition — with its focus on functions and services — is intended to fit with the DHS designations of entire entities as covered critical infrastructure and what the two different regulatory regimes will mean for companies that would be designated as covered critical infrastructure and that also have non-critical I3S services and functions.

[1] In May 2011 testimony before a House Judiciary Subcommittee, CDT outlined the distinctions that need to be drawn in order to develop a national cybersecurity policy that properly supports privacy, free expression, innovation, and other values. See http://cdt.org/files/pdfs/20110525_lh_cybertesti.pdf at pp. 3-4.

Enforceable, Voluntary Codes of Conduct Are a Promising Means of Improving Cybersecurity

CDT supports the Department's commitment to facilitating the development of voluntary codes of conduct among I3S members. These voluntary codes of conduct can afford I3S members an appropriate amount of freedom and flexibility in their approaches to cybersecurity while ensuring that network providers, rather than government actors, are monitoring privately-owned networks for intrusions. (The same is equally true for critical infrastructures: While the security standards may need to be higher for a "critical" nuclear power plant than for a major retail chain, in both cases standards can be developed through a collaborative, voluntary process that affords flexibility and such standards can be implemented within a framework that depends on private entities to monitor their own networks and systems.) The green paper envisions a suitable supporting role for the Department in convening and facilitating members of I3S subsectors to discuss and develop these codes. NIST's involvement in this process, helping develop guidelines for subsectors that lack the resources to establish their own codes of conduct, is also appropriate, provided it, too, plays a primarily supporting and assistive role, rather than setting specific standards.

The green paper also states that these voluntary codes will be enforceable by "relevant law enforcement agencies," including the Federal Trade Commission (FTC) and State Attorneys General. CDT supports this approach. It builds on current law and practice. Entities that collect personally identifiable information are already required under federal law, as interpreted by the FTC, and by many state laws, to develop, implement and maintain reasonable safeguards to protect that data and are subject to enforcement action if they fail to do so. Voluntary codes help define what is reasonable. We particularly support the inclusion of State Attorneys General as enforcement agents, in addition to the FTC. State Attorneys General have been always essential consumer protection enforcers. In the rapidly changing online environment, sometimes state Attorney General offices are best equipped to bring quick, targeted consumer protection actions. The Federal Trade Commission is tasked with a wide range of responsibilities of which cybersecurity protection is only one, and therefore the inclusion of State Attorneys General as additional enforcers of these voluntary codes of conduct is extremely important.

Cybersecurity Information Sharing Regime Should Include a Focus on Privacy Principles and Protections

The green paper includes a policy recommendation that the Department work with other agencies, organizations, and other relevant entities of the I3S to build and/or improve upon existing public-private partnerships that can help promote information sharing. CDT supports improving cybersecurity information sharing. However, to the extent that information sharing involves personally identifiable information or private communications traffic, we would urge the Department to approach this issue cautiously and with special attention to privacy. A private-to-private information sharing model has advantages over a model with the government at the center, but any sharing of communications data or personally identifiable information must be narrowly defined and carefully implemented. To being with, the Department should explain how the information sharing regime it envisions for cybersecurity for the I3S sector would comply with Fair Information Practices principles and with the laws protecting the privacy of electronic communications.

Building on and improving existing public-private partnerships that can help promote information sharing must include, from the outset, very careful consideration for how the information being shared can best be handled, stripped of identifying information not needed for cybersecurity purposes, and disposed of to protect privacy to the greatest extent possible. Any cybersecurity information sharing regime must also include a vigorous oversight process.

CDT has previously noted that, while current law authorizes communication service providers to monitor their own systems and to disclose voluntarily communications and records necessary to protect their own systems, a very narrow exception to the Wiretap Act and Electronic Communications Privacy Act (ECPA) may be needed to permit disclosures for the defense of others. We have developed recommendations to achieve this goal and are in dialogue with policymakers and stakeholders to seek consensus on the most effective and most targeted solution. CDT has raised serious concerns with the information sharing language proposed by the Administration in its cybersecurity legislative package.[2] We urge the Department, in coordination with other departments, to seek an approach to information sharing that relies less on government centralization and more on building the capabilities of private sector entities to protect their own networks, services and functions.

The Department might also consider whether an antitrust exemption is necessary to facilitate cybersecurity information sharing. Other options the Department might study would be to provide safe harbors, insurance benefits and/or liability caps to network operators that share information about threats and attacks in cyberspace.

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.

Conclusion

We applaud the Department of Commerce for taking up the issue of cybersecurity and non-critical infrastructure features and services and formulating an appropriately light regulatory regime to govern this area. The Department should clarify the distinction between its proposed I3S definition and the existing Information Technology and Communications sectors, or else simply use the pre-existing terms. Special attention should be paid to including privacy protection measures and oversight in any cybersecurity information sharing regime proposed by the Department.

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

[2] CDT analysis of the Administration's cybersecurity legislative proposals, **Part II: Information Sharing Between the Private Sector and the Government,** http://cdt.org/blogs/greg-nojeim/wh-cybersecurity-proposal-questioning-dhs-collection-center (May 24, 2011). In our analysis, we spell out an alternative to the Administration's proposal.