ReedSmith

Department of Commerce Calls for Voluntary Cyber Security Standards

Author: Paul Bond, Partner, Princeton
Author: Christopher Gregory Cwalina, Counsel, Washington, D.C.
Author: Amy S. Mushahwar, Associate, Washington, D.C.

Publication Date: June 13, 2011

Agency's Internet Policy Task Force Seeks Further Comments

On June 8, the Department of Commerce's Internet Policy Task Force released its cyber security Green Paper identifying some preliminary recommendations for moving forward with a comprehensive cyber security policy for private industry.

The Green Paper is a second iteration of recommendations on the Internet and Information Innovation Sector ("I3S") after an initial round of comments last year. The private companies comprising the I3S are not considered critical infrastructure and include both Internet and non-Internet companies that use the Web to conduct business. Members of I3S may provide general retail websites, information services, create Web content, facilitate transactional services, store and host publicly accessible content and/or support access to content (i.e., engine providers, application and browser developers and social networks). This broad definition seemingly applies to almost every business that utilizes the Internet, even those within critical infrastructure that have hybrid essential and non-essential facilities. Yet, while the definition applies to a very broad swath of the economy-essentially any business that uses a network, website, or manages an online business-the majority of the commenters were information technology companies.

The Green Paper focuses on four major areas:

1. Create a nationally recognized approach to minimize vulnerabilities for the I3S
2. Develop incentives for I3S to combat cyber security threats
3. Promote cyber security education and research that will protect the I3S
4. Facilitate international cooperation

The Green Paper makes no firm conclusions or policy statements, but largely summarizes comments received from the private sector on an earlier Notice of Inquiry. In doing so, the Green Paper proposes development of a voluntary cyber security code of conduct for I3S companies. Commerce's Task Force will formally seek answers to these comments in a *Federal Register* notice, and we will update you with a "comments deadline" once it is released.

Developing the Code and Minimizing Vulnerabilities

"Voluntary" Code of Conduct? The Green Paper suggests that any code of conduct developed would be a voluntary standard that would essentially memorialize reasonable security practices. But, looking "under the hood" of this statement, we can see that there is a possibility for the proposed voluntary standard to have enforcement consequences. The Green Paper suggests that once the Code has been developed and adhered to by businesses, the Federal Trade Commission ("FTC") and/or state attorneys general should be able to enforce such a code under their existing authorities to combat unfair and deceptive practices. At this stage, we do not know if companies would need to formally state that they were following the Code to subject their organizations to enforcement liability, or if any statements such as "we follow reasonable industry security standards" would be sufficient.

Use Existing Standards and Protocols (i.e., PCI DSS, NIST SP 800-53, IPSEC, DNSSEC, SSL). The Green Paper recommends using existing security standards and protocols to create a framework for the Code. Ultimately the Task Force concluded that any framework must be flexible to adapt to both developing technologies and security threats.

Automate Security, Where Feasible. The Green Paper emphasizes the need for automated security and configurations, generally. Automation can lead to more expedient identification of risks and vulnerabilities, and can serve as a means for better information-sharing within the I3S. The report notes that 80 percent of successful attacks can be attributed to known vulnerabilities, so automated threat identification scans and related communications could significantly improve existing security by speeding up communication. In this section, the Task Force specifically mentioned that cloud providers should also consider automated security improvements.

Improve Security Review Process for New Products (Security by Design?). New security products must work as advertised and be reviewed by a third party before a product hits market. The Green Paper discusses the processes of Common Criteria ISO/IEC 15408, which provides a means for third-party validation that security products work as claimed. But, Commerce discussed comments, noting that the existing processes are slow to keep pace with cyber security trends and can be rigid, delaying product releases and updates. A new, more flexible model is needed that can adapt to current security concerns when evaluating new technology products. Commenters generally supported a revamped dynamic third-party assurance process opposed to a government standard. While industry supports the third-party model, it worries that this could create rival and intrusive programs internationally.

Incentivizing I3S Compliance with the Code of Conduct

General Incentives. Private sector commenters recommended several "carrots" as ways to induce I3S to comply with any developed code. These included: tax incentives, streamlined regulations, favorable government procurement policies, grants and Small Business Administration loans.

Cyber Security Insurance Incentives. Commerce also discussed tying any developed cyber security protections to discounts on one's cyber security insurance premiums (e.g., home alarm system reductions on one's home insurance). This would create better adherence to cyber security protections, due to direct costs savings on one's premium. But, Commerce acknowledged that the cyber security risk insurance market suffers from a lack of data to evaluate whether any proposed protections could result in premium discounts. For cyber security insurance incentives to become a better impetus to abide by any Commerce guidelines, insurers need more information on the risk and impacts of cyber incidents. Currently, there is a dearth of actuarial data regarding the losses that result from cyber attacks and statistical data regarding the frequency of cyber security incidents. Commerce proposed improved information-sharing and research on the appropriate risk indicators to provide the greater statistical transparency needed. Further, Commerce also proposed an agreed-upon code of conduct would help insurers gauge risk and standard practices for pricing premiums.

Safe Harbor? The Green Paper raises considerable questions regarding the use of legal safe harbors for cyber security. The Green Paper identified negative comments stating that such a safe harbor could create a false sense of information security. Commenters raised that a poorly designed safe harbor could limit liability for some types of harm, but could provide exposure to other not-contemplated adverse events because companies may only design security to meet the safe harbor (not to anticipate additional threats around the corner). In essence, the concern is that a safe harbor could incentivize a company to do the bare minimum to be compliant with the safe harbor. The Task Force will seek comments on how a safe harbor standard could overcome these concerns.

National Data Breach Support Continues. It also bears noting that the Task Force yet again identified its support for a national data breach standard as an incentive in this Cyber Security Green Paper and as a possibility in the Department of Commerce's Privacy Green Paper, a summary of which is available here.

Incentives Needed for the Communications Conundrum. As is often heard in any discussion of cyber security, better information-sharing is needed between the private and public sector regarding security threats and issues. As background, several government vehicles exist to share threat information, such as the Information Sharing and Analysis Centers and US-CERT. And, private companies have developed a cottage industry sharing breach, security threat and system patch information. As several groups, public and private, currently exist to share such data, efforts lack uniform coordination and there is no clear delineation of authority or responsibility for managing incidents; as such, many businesses are unaware of current models for sharing such information. The Task Force seeks comments on how businesses could incentivize such communication.

Research and Development

Developing Cyber Security Tools and Professionals. Both industry and the Department agree that more needs to be done to further cyber security research and development, and to further educational opportunities for cyber security professionals. The Green Paper asks how cloud computing can be utilized to further both interests. As a next step, Commerce proposes continued work with the private sector to develop formal cyber security curricula and to continue

coordinating government research and investment efforts through the Federal Networking and Information Technology Research Development framework (NITRD).

International Collaboration

The Task Force recommended that current international collaboration efforts should continue, especially with global standards development bodies (e.g., IETF and ISO), to promote cyber security policies, standards and research. Multiple commenters asked for a seat at the table when policy positions are being developed and cautioned that the United States should ensure that it does not unilaterally adopt standards that could confuse or conflict with international standards.

Conclusion

One large question mark that remains and continues to stall cyber security government and private regulatory efforts is which federal agency will have the lead role in spearheading any standards developed. Considerable legislative efforts were derailed for several legislative sessions because of the perceived federal agency turf war. Commerce, as an agenda-setting Executive Agency, appears to be content with its role as a discussion facilitator. And its Green Paper gave no hints as to which Department or Agency should take the lead in firmly developing any set of standards.

The collaborative public-private environment of the Internet Policy Task Force seems likely to be the continued approach taken by the Administration in developing any voluntary private sector cyber security standard. Procedurally, questions remain with such an approach, such as, would the FTC need to ratify the standard or develop its own "rulemaking" on this issue before using the standard as a basis in Section 5 actions? What agency will be tasked with responding to private companies' technical concerns regarding the new standards as they are implemented? And, would the staff with such responsibilities have sufficient experience in large-scale, multi-company, private-sector networks?

The proposals identified in the report (and the gaps within those proposals) are well worth private industries' time for serious comment. Small and medium-sized businesses should take note: these proposals are likely to be above-and-beyond the discrete sector-specific privacy

protections that your company employs (i.e., many retailers might only abide by the credit card data, PCI-DSS standards). For large businesses that must already comply with several layers of regulatory security requirements and those related audits, whatever security framework develops from Commerce's discussions will be in addition to your current requirements. Thus, regardless of your business size or model, if you have an IT infrastructure, it is worth an examination of how any Commerce cyber security recommendations would impact your operations and bottom line. And, for those larger businesses it is worth conducting a bit of research to determine if another layer of regulation will even marginally impact security.

Given the high visibility data security breaches this year with RSA, Amazon, Citibank, Sony and others, this is an issue that will not go away. And, there is indeed political will to proceed with cyber security reform on a regulatory and/or legislative basis. Given that this is an issue poised for movement, we urge private industry to inject the factual reality of running a large enterprise network into the policy dialogue whenever feasible. We will update you once this item is formally noticed and a comments date has been released.