wiley

ALERT

Commerce Department Seeking Industry Comment on Cybersecurity Incentives—Opportunity to Shape Policy

March 28, 2013

On Thursday, March 28, the Department of Commerce issued a request for public comment on how to promote private sector participation in a voluntary cyber program. President Obama introduced this program in a recent Executive Order on Improving Critical Infrastructure Cybersecurity, and the Department of Homeland Security will establish and administer the program, using a framework of standards and procedures which are under development by Commerce's National Institute of Standards and Technology (NIST). The notice, published in the Federal Register, requests comments from companies by April 29. As with other cyber initiatives percolating throughout government, the timelines are fast and the potential for additional compliance obligations is real.

Comments from the private sector on implementing the cybersecurity program are important as they could shape or influence industry standards, and "incentives" could include or catalyze regulatory action. Commerce previously asked for comment in a July 2010 public notice, and used public input to inform its June 2011 "Green Paper" on Cybersecurity, Innovation and the Internet Economy.

With this March 2013 request for comment, Commerce envisions developing recommendations not only for the implementation of the voluntary cyber program but also additional recommendations "that apply to U.S. industry as a whole." It asked commenters to describe whether recommended incentives would require legislation or may be implemented through existing authorities, so recommendations may generate additional regulation.

Authors

Nova J. Daly
Senior Public Policy Advisor
202.719.3282
ndaly@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

International Trade
Privacy, Cyber & Data Governance
Telecom, Media & Technology

Other key issues that Commerce has asked companies to address include the best ways to encourage businesses to make risk-appropriate investments in cybersecurity, the barriers to cybersecurity investments and especially those encountered by small business and/or multinational companies, and the costs of compliance to existing cybersecurity requirements. Additionally, Commerce seeks input on implications of two potential policies: one that would create liability for companies whose failure to exercise reasonable care results in a loss due to inadequate security measures, and another that would require entities to join the cybersecurity program prior to receiving government financial guarantees or assistance.

Companies should also be aware of a number of related cyber issues, including NIST's request for information (RFI) on a cybersecurity framework directed by the Executive Order, and draft cybersecurity legislation. On February 26, NIST issued an RFI seeking input on the development of a set of standards, methodologies, procedures and processes that align policy, business and technological approaches to address cyber risks. Comments on the NIST RFI are due on April 8.

Congress has also been very active on cybersecurity. As mentioned in our previous Client Alert, a provision in H.R. 933, the continuing resolution signed into law on March 26 that funds the federal government for the next six months, bans certain federal government purchases of information technology products from firms that the Chinese government owns, directs or subsidizes. The President has expressed interest in cybersecurity legislation in the near future as well. The House of Representatives is expected to take up the Cyber Intelligence Sharing and Protection Act that was passed in the House last year and has been re-introduced last month. The House is slated to have a "cyber week" the week of April 15. An intelligence bill by Rep. Mike Rogers (R-MI), chairman of the House Permanent Select Committee on Intelligence, will be the most important bill moving that week. Further, the Senate is working on various drafts related to infomation sharing and comprehensive reform. Companies should pay close attention to these and other cyber developments in order to take opportunities to provide comment on potential policies and to ensure their compliance with any new obligations or standards.

Wiley Rein closely tracks cybersecurity law and policy and engages Congress and the Administration in advising, interpreting and applying applicable cyber law and policy. Our cybersecurity team, which consists of former senior level Executive branch appointees and congressional staffers, is exceptionally placed to provide guidance on the latest critical information and intelligence related to cybersecurity law and policy and stands ready to work with companies to understand applicable provisions and to comply with relevant law.