

Notices

Federal Register

Vol. 78, No. 60

Thursday, March 28, 2013

This section of the FEDERAL REGISTER contains documents other than rules or proposed rules that are applicable to the public. Notices of hearings and investigations, committee meetings, agency decisions and rulings, delegations of authority, filing of petitions and applications and agency statements of organization and functions are examples of documents appearing in this section.

DEPARTMENT OF COMMERCE

Office of the Secretary

National Institute of Standards and Technology

National Telecommunications and Information Administration

[Docket Number 130206115–3115–01]

Incentives To Adopt Improved Cybersecurity Practices

AGENCY: U.S. Department of Commerce.

ACTION: Notice of inquiry.

SUMMARY: The President has directed the Secretary of Commerce to evaluate a set of incentives designed to promote participation in a voluntary program to be established by the Secretary of Homeland Security to support the adoption by owners and operators of critical infrastructure and other interested entities of the Cybersecurity Framework being developed by the National Institute of Standards and Technology (NIST). The evaluation will include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program. The Department of Commerce (Department) will use input received in response to this Notice to inform its recommendations, which will focus on incentives for critical infrastructure owners. In addition, the Department may use this input to develop a broader set of recommendations that apply to U.S. industry as a whole.

DATES: Comments are due on or before April 29, 2013.

ADDRESSES: Written comments may be submitted by mail to the Office of Policy Analysis and Development, National Telecommunications and Information Administration, U.S. Department of

Commerce, 1401 Constitution Avenue NW., Room 4725, Washington, DC 20230. Comments may be submitted electronically to cyberincentives@ntia.doc.gov. All email messages and comments received are a part of the public record and will be made available to the public generally without change on the Internet Policy Task Force Web page at <http://www.ntia.doc.gov/category/cybersecurity>. For this reason, comments should not include confidential, proprietary, or business sensitive information.

FOR FURTHER INFORMATION CONTACT: For questions about this Notice, contact: Alfred Lee, Office of Policy Analysis and Development, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW., Room 4725, Washington, DC 20230, telephone (202) 482–1880; or send an email to cyberincentives@ntia.doc.gov. Please direct media inquiries to the Office of Public Affairs at (202) 482–4883; or send an email to publicaffairs@doc.gov.

SUPPLEMENTARY INFORMATION: The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure. The cyber threat to critical infrastructure is growing and represents one of the most serious national security challenges that the United States must confront. On February 12, 2013, the President signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."¹ As the President stated in the Executive Order, "repeated cyber intrusions into America's critical infrastructure demonstrate a need for improved cybersecurity."²

The Executive Order establishes a policy of enhancing the security and resilience of the Nation's critical infrastructure and maintaining a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy and civil liberties through a partnership with the owners and operators of critical

infrastructure³ to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards. The Executive Order sets forth three elements to establish this partnership. First, the Department of Homeland Security ("DHS") will use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. Second, the National Institute of Standards and Technology will develop a framework consisting of a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks ("the Framework"), which will provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. Third, DHS, in coordination with sector-specific agencies, will develop the Critical Infrastructure Cybersecurity Program ("the Program") to promote voluntary adoption of the Framework.

The Executive Order recognizes that further incentives may be necessary to encourage sufficient private sector participation in the Program. To develop a clearer picture of existing and potential incentives, the Executive Order directs the Department of Commerce to recommend ways to promote participation in the Program.⁴ The recommendations "shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants of the Program." Consistent

³ For the purposes of this Notice, the term "critical infrastructure" has the meaning given the term in 42 U.S.C. § 5195c(e): "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

⁴ The Executive Order also directs the Secretaries of the Treasury and Homeland Security to recommend incentives to participate in the Program. The Secretary of Defense and the Administrator of General Services are also tasked with reporting on government procurement-related issues.

¹ "Exec. Order No. 13636, 78 FR 11739 (Feb. 19, 2013), available at: <https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity>.

² *Id.*

with the Executive Order, these incentives may include technical and public policy measures that improve cybersecurity without creating barriers to innovation, economic growth, and the free flow of information. The Department of Commerce will submit its recommendations to the President through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs no later than June 12, 2013.

Improving cybersecurity practices among entities that do not own or operate critical infrastructure, or for other reasons are unlikely to join the Program, is also an important Executive Branch priority. Therefore, the Department of Commerce also seeks comment on a broader set of incentives that could help to promote the adoption of proven efforts to address cybersecurity vulnerabilities.

The Department of Commerce asked questions related to incentives for noncritical infrastructure in a July 2010 Notice of Inquiry.⁵ Responses to the July 2010 Notice aided the Department's efforts to promote standards and best practices and informed its June 2011 "Green Paper," *Cybersecurity, Innovation and the Internet Economy*.⁶ Along with the responses to this Notice, the Department plans to draw again on earlier responses in the development of recommendations to the President on incentives. In addition, the Department plans to use responsive comments to inform a follow-up to the Green Paper.

Stakeholders that responded to the July 2010 Notice may wish to focus on the following questions:

- Have your viewpoints on any questions related to incentives for noncritical infrastructure changed since you filed them in response to the July 2010 Notice?
- Do your comments related to incentives for noncritical infrastructure also apply equally to critical infrastructure?

⁵ Dept. of Commerce, *Cybersecurity, Innovation, and the Internet Economy*, 75 FR 44216 (July 28, 2010) (Notice of Inquiry), available at http://www.ntia.doc.gov/fnotices/2010/FR_CybersecurityNOI_07282010.pdf. Comments received in response to the 2010 Notice of Inquiry are available at <http://www.nist.gov/itl/cybercomments.cfm>.

⁶ Dept. of Commerce, *Cybersecurity, Innovation, and the Internet Economy* (June 2011), http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf. The questions asked in the Green Paper are available at Dept. of Commerce, *Cybersecurity, Innovation, and the Internet Economy*, 76 FR 34965 (June 15, 2011), available at <http://www.ntia.doc.gov/federal-register-notice/2011/cybersecurity-innovation-and-internet-economy>. Comments received in response to the Green Paper are available at <http://www.nist.gov/itl/greenpapercomments.cfm>.

- Does anything in the Executive Order or recent legislative proposals change your views on what incentives will be necessary or how they can be achieved? In particular, would the incentives that you previously discussed be effective in encouraging all firms that participate in the Internet economy to participate in the Program? Would these incentives encourage critical infrastructure companies to join the Program?

In answering these questions, commenters should not limit their responses to incentives that are feasible under existing law.

For all stakeholders, particularly those that did not respond to these earlier inquiries, the Department of Commerce requests comments on any of the following questions:

- Are existing incentives adequate to address the current risk environment for your sector/company?
- Do particular business sectors or company types lack sufficient incentives to make cybersecurity investments more than others? If so, why?
- How do businesses/your business assess the costs and benefits of enhancing their cybersecurity?
- What are the best ways to encourage businesses to make investments in cybersecurity that are appropriate for the risks that they face?
- How do businesses measure success and the cost-effectiveness of their current cybersecurity programs?
- Are there public policies or private sector initiatives in the United States or other countries that have successfully increased incentives to make security investments or other investments that can be applied to security?
- Are there disincentives or barriers that inhibit cybersecurity investments by firms? Are there specific investment challenges encountered by small businesses and/or multinational companies, respectively? If so, what are the disincentives, barriers or challenges and what should be done to eliminate them?

- Are incentives different for small businesses? If so, how?
- For American businesses that are already subject to cybersecurity requirements, what is the cost of compliance and is it burdensome relative to other costs of doing business?
- What are the merits of providing legal safe-harbors to individuals and commercial entities that participate in the DHS Program? By contrast, what would be the merits or implications of incentives that hold entities accountable for failure to exercise reasonable care

that results in a loss due to inadequate security measures?

- What would be the impact of requiring entities to join the DHS Program prior to receiving government financial guarantees or assistance in relevant sectors?
- How can liability structures and insurance, respectively, be used as incentives?
- What other market tools are available to encourage cybersecurity best practices?
- Should efforts be taken to better promote and/or support the adoption of the Framework or specific standards, practices, and guidelines beyond the DHS Program? If so, what efforts would be effective?
- In what way should these standards, practices, and guidelines be promoted to small businesses and multinationals, respectively, and through what mechanisms? How can they be promoted and adapted for multinational companies in various jurisdictions?
- What incentives are there to ensure that best practices and standards, once adopted, are updated in the light of changing threats and new business models?
- Voluntary industry sector governance mechanisms are sometimes used to stimulate organizations to conform to a set of principles, guidelines, and operations based on best practices, standards, and conformity assessment processes that collectively increase the level of assurance while preserving organizations' brand standing and the integrity of products and services.

- Do organizations participate in voluntary governance mechanisms?
- Which industries/groups have voluntary governance mechanisms?
- Do existing voluntary governance mechanisms have cybersecurity-related constraints?
- What are the benefits and challenges associated with voluntary governance mechanisms?

Dated: March 22, 2013.

Rebecca M. Blank,

Deputy Secretary of Commerce.

Patrick Gallagher,

Under Secretary of Commerce for Standards and Technology.

Lawrence E. Strickling,

Assistant Secretary for Communications and Information.

[FR Doc. 2013-07234 Filed 3-27-13; 8:45 am]

BILLING CODE 3510-EA-P