RECOMMENDATIONS TO THE PRESIDENT ON INCENTIVES FOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS TO JOIN A VOLUNTARY CYBERSECURITY PROGRAM

Introduction

On February 12, 2013, the President issued Executive Order 13636, stating that the "cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront."[1] The Executive Order sets out a number of steps to address this problem, including calling on the Department of Commerce's National Institute of Standards and Technology ("NIST") to develop a Cybersecurity Framework ("Framework") and the Department of Homeland Security ("DHS") to build a voluntary program ("Program") "to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities. . ."[2] The Program could include guidance on how to implement the Framework in specific sectors, as well as incentives for companies to align their cybersecurity practices, with the practices and standards specified in the Framework. The President requires DHS, the Department of Commerce ("Commerce"), and the Department of Treasury ("Treasury") to draft separate reports on incentives to join the Program. The following recommendations are Commerce's contribution to this analysis of incentives.

Department of Commerce Recommendations

The incentives the government offers to participants in the Program must help align the Nation's interest in improving the cybersecurity posture of all critical infrastructure entities with the interests of individual companies. These incentives should specifically promote participation in the Program; involve judicious commitment of any additional federal government resources; and advance a full range of policy interests, including protecting privacy and civil liberties as well as promoting effective cybersecurity for critical infrastructure entities.

To inform its views of how to achieve this balance, Commerce issued a Notice of Inquiry ("NOI") on March 28, 2013, asking stakeholders for input on a broad array of questions about incentives that affect cybersecurity practices. Based on responses to this NOI, previous input to the Commerce Internet Policy Task Force ("IPTF"), consultations with other federal departments and agencies, and related analysis, Commerce makes the following preliminary recommendations to the President on potential actions that the U.S. Government can take to build a successful incentives structure for the Program.

- **Engage insurance companies in the creation of the Framework:** NIST should engage critical infrastructure cybersecurity stakeholders, including the insurance industry, when developing and demonstrating the utility and effectiveness of the standards, procedures,

[1] Exec. Order 13636, Improving Critical Infrastructure Cybersecurity, at § 1, 78 Fed. Reg. 11737 (Feb. 19, 2013) [hereinafter *Executive Order*] *available at* https://federalregister.gov/a/2013-03915.

[2] *Id.* at § 8(a).

and other measures that comprise the Framework and thus underlie the Program. Specifically, cybersecurity insurance carriers would bring extensive knowledge of the effectiveness of specific cybersecurity practices and could help evaluate specific proposed elements from this perspective. This collaboration between insurance companies, NIST, and other stakeholders could serve as a basis for creating underwriting practices that promote the adoption of cyber risk-reducing measures and risk-based pricing. This collaboration could also foster a competitive cyber insurance market.

- **Study tort liability:** Once the Program is developed, DHS, in consultation with the Department of Justice, should study the legal and financial risks that critical infrastructure owners and operators face from tort liabilities arising out of cyber attacks, and whether these risks promote or inhibit participation in the Program. This study should include a review of tort cases against critical infrastructure owners and operators and an assessment of mechanisms (*e.g.*, insurance or statutory liability limitations) that have the potential to reduce or transfer their tort liability if a cyber incident causes damage despite the owner or operator's adoption and implementation of some or all of the standards, procedures, and other measures that comprise the Framework.

- **Consider participation in the Program as a criterion for NSTIC Pilot and other Commerce grants:** As NIST makes future decisions about pilot grants related to the National Strategy for Trusted Identities in Cyberspace ("NSTIC"), it should work with DHS to study whether to make consistency with the framework an evaluation criterion for awarding grants. Commerce should also look into using Framework adoption and Program participation as a consideration for critical infrastructure development grants.

- **Offer guidance to federal agencies on compliance with the Framework and participation in federal grant programs:** Commerce recommends that the White House issue guidance to federal agencies to promote cybersecurity protections as appropriately weighted criteria for evaluating federal grant applicants.

- **Ensure that the Program links research and development efforts to overcoming real-world challenges:** NIST's National Cybersecurity Center of Excellence ("NCCoE") should work with DHS, Program participants, and vendors of information technology goods and services to help determine where commercially available solutions can be used and where further research and development are necessary to meet pressing cybersecurity challenges.

- **Identify candidates for regulatory streamlining:** NIST and DHS should continue to ensure that the Framework and the Program interact in an effective manner with existing regulatory structures. Once NIST has published the first version of the Framework and the Program is operational, the Administration, independent agencies, and Congress should use this information to inform discussions of specific regulatory streamlining proposals.

- **Explore a Fast-Track Patent Pilot for cybersecurity:** Research and development efforts at critical infrastructure companies are susceptible to the ongoing threat of trade

secret theft. The U.S. Patent and Trademark Office should explore building a Fast-Track Patent Pilot for members of the Program, which could provide a significant incentive for R&D-intensive critical infrastructure companies to join the Program.

- **Study the use of government procurement considerations:** The Office of the Secretary of Commerce and NIST will consider closely the report that the Department of Defense and General Services Administration will issue on using federal procurement processes to encourage the adoption of cybersecurity standards, and will work with these agencies, the United States Trade Representative, and other relevant federal offices and agencies to examine government procurement further as a possible incentive to participate in the Program.

- **No further study of the use of tax incentives:** Commenters proposed several kinds of tax incentives, but there was little consensus among respondents to the NOI on whether or which kinds of tax incentives might be effective. In Commerce's analysis, it would be difficult to ensure that tax incentives are sufficient to encourage participation in the Program and do not impose undue costs on the federal government. Accordingly, Commerce does not recommend further consideration of tax incentives.

- **Study the development of an optional public recognition program for participants in the Program:** Many companies expressed interest in mechanisms to convey that they adhere to sound cybersecurity practices. Commerce believes that many critical infrastructure entities would be interested in such a public recognition element of the program, but some also seem to be concerned that it could lead to those entities being additionally targeted. Therefore, as the Program is being developed, Commerce recommends studying how recognition for participants could be utilized as an incentive, depending on the organization, sector, and risk tolerance.

- **Explore providing specific types of technical assistance to participants in the Program:** Technical assistance should be based, first and foremost, on the immediate welfare and safety of the public. However, Commerce recognizes that certain types of technical assistance should be considered to assist participants in the adoption and implementation of the Framework.

- **Commerce does not recommend that further steps be taken to provide expedited security clearances to Program participants:** Commerce considers the expedited security clearances already allowed to owners and operators of critical infrastructure under the Executive Order to be sufficient.

For further discussion of these issues and recommendations, please see Commerce's cybersecurity incentives discussion, available at http://www.ntia.doc.gov/category/cybersecurity. Commerce welcomes the opportunity to discuss these recommendations and other ideas for incentives further. The success of the Framework and the Program depends on wide implementation. Commerce will work with relevant federal agencies to examine any issues that require further study once the Framework and the Program are finalized.