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

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 report is Commerce's contribution to this analysis of incentives.

I. 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

[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).

developing and demonstrating the utility and effectiveness of the standards, procedures, 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 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 ("USPTO") 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.

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.

II. Introduction

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 for the United States. On February 12, 2013, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," establishing 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."[3] The Executive Order stressed that these goals should be pursued through a "partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."[4]

The Executive Order requires NIST to work with the private sector to develop a framework, consisting of a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to addressing cyber risks ("the Framework"). The Framework 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 while promoting safety, security, business confidentiality, privacy, and civil liberties.

The Framework will map "areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations."[5] The Framework's standards will "incorporate voluntary consensus standards and industry best practices to the fullest extent possible."[6] To ensure that the Framework provides useful guidance to different critical infrastructure sectors, with their diverse mission and business needs, and is adaptable to changing threats, NIST will make the Framework technology-neutral and will focus on cybersecurity practices that are common across sectors.[7] DHS, in coordination with sector-specific agencies, is developing the Program to promote voluntary adoption of the Framework by critical infrastructure owners and operators and "any other interested entities."[8]

---

[3] *Executive Order*, *supra* note 1, at § 1.

[4] *Id.*

[5] *Id.* at § 7(b).

[6] *Id.* at § 7(a).

[7] NIST sought public input on developing the Framework through a recent Request for Information and will seek further input through a series of public workshops over the next few months. Dep't of Commerce, Developing a Framework to Improve Critical Infrastructure Cybersecurity, Notice and Request for Information, 78 Fed. Reg. 13024 (Feb. 26, 2013) [hereinafter *Framework RFI*], *available at* https://federalregister.gov/a/2013-04413.

[8] *Id.*

Developing a Voluntary Program to Encourage Adoption of the Framework

DHS will work with other agencies to develop a Program to encourage Framework adoption. The Executive Order directs "Sector-Specific Agencies, in consultation with the Secretary [of DHS] and other interested agencies, [to] coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments."[9] This guidance will identify approaches for implementing elements of the Framework, based on the needs of specific sectors. The voluntary Program may leverage existing private sector approaches, encourage the development of private sector programs and/or be based on collaborative public/private sector approaches. U.S. industry has developed effective private sector programs that address public needs and societal concerns in many sectors.

DHS will also establish incentives that encourage companies to implement the Framework. The Program's incentives should be flexible enough to accommodate the diverse regulatory and business requirements of different critical infrastructure sectors. In a comment submitted in response to a Notice of Inquiry that Commerce issued to inform its recommendations,[10] one utility noted this need for sector-sensitive flexibility in its comments:

> Due to the diversity across industries, and the diversity among companies within an industry, flexibility to address threats is crucial. By identifying a variety of ways that can suffice as Cybersecurity Framework participation, approaches to cyber security remain flexible.
>
> For example, complying with NERC CIP standards might be considered Cybersecurity Framework participation. Another example of participation might be successful results from cyber audits performed by independent third parties.[11]

NIST has stated that the Framework should be a "living document," and the voluntary Program should be leveraged to inform future development of the Framework. The standards-based approach of the Framework will facilitate the ability of critical infrastructure owners and operators to manage cyber risks, and to implement alternate solutions from the bottom up with interoperability, scalability, and reliability as key attributes.[12] It will also be designed to provide owners and operators with the ability to implement optimal security practices while facilitating communication concerning Framework implementation across their supply chain and to relevant authorities and regulators. Accordingly, NIST will make efforts to harmonize and integrate the

---

[9] *Executive Order*, *supra* note 1, at § 8(b).

[10] *See infra* note 12 and accompanying text.

[11] Southern California Edison 2013 Cybersecurity NOI Comments at 1, *available at* http://www.ntia.doc.gov/files/ntia/sce_comments.pdf. *See also* Covington & Burling / Chertoff Group 2013 Cybersecurity NOI Comments at 2, *available at* http://www.ntia.doc.gov/files/ntia/covington_burling_llp_the_chertoff_group_response.pdf ("Many larger companies are subject to multiple IT security compliance programs. NIST should consider offering companies choice in leveraging these existing compliance regimes and companies' internal controls processes to demonstrate alignment with the cybersecurity framework.").

[12] *See generally Framework RFI*.

Framework with existing relevant standards. Finally, NIST will engage with stakeholders throughout the Framework development process to better understand how industry can play a leading role in sustaining it.

The Commerce Cybersecurity Incentives Report

To develop a clearer picture of existing and potential incentives available to DHS, the Executive Order directed Commerce to recommend ways to promote participation in the Program.[13] Consistent with Executive Order guidance, this Commerce report makes 12 recommendations regarding potential incentives and discusses the merits of each, including "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."[14]

In formulating its recommendations for this report, Commerce drew on the prior work of its Internet Policy Task Force ("IPTF")[15] and the record built in response to a March 28, 2013 Notice of Inquiry, entitled "Incentives To Adopt Improved Cybersecurity Practices,"[16] supplemented by several meetings with experts. In addition, the IPTF has drawn on responses to questions posed in a July 2010 Notice of Inquiry, dealing with cybersecurity incentives and related issues for noncritical infrastructure providers and other interested parties.[17] Finally, Commerce conducted a review of relevant literature.

---

[13] *Executive Order*, *supra* note 1, at § 8(d) (stating that the 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).

[14] *Id.*

[15] Particularly relevant are prior efforts in the cybersecurity area that culminated in the June 2011 release of *Cybersecurity, Innovation and the Internet Economy* and more recent work to establish an Industry Botnet Group, a group of nine trade associations and nonprofit organizations working together on initiatives to improve efforts to combat botnets. *See* Dep't of Commerce, *Cybersecurity, Innovation, and the Internet Economy* (June 2011), http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf ("IPTF Green Paper"); *see also* Press Release, Dep't of Commerce, White House Announces Public-Private Partnership Initiatives to Combat Botnets (May 30, 2012), http://www.commerce.gov/news/press-releases/2012/05/30/white-house-announces-public-private-partnership-initiatives-combat-b. The Department of Commerce-wide IPTF was established in April 2010 to address key Internet policy challenges, including improving cybersecurity. The IPTF approach recognizes a key role for government in convening stakeholders and leading the way to policy solutions that protect the public interest as well as private profits, while avoiding government prescription.

[16] Incentives to Adopt Improved Cybersecurity Practices, Notice of Inquiry (Mar. 28, 2013), *available at* https://federalregister.gov/a/2013-07234. Over 40 commenters responded to the March 2013 Notice of Inquiry. *See* NTIA, *Comments on Incentives To Adopt Improved Cybersecurity Practices NOI* (Apr. 29, 2013), http://www.ntia.doc.gov/federal-register-notice/2013/comments-incentives-adopt-improved-cybersecurity-practices-noi.

[17] Dep't of Commerce, Cybersecurity, Innovation, and the Internet Economy, Notice of Inquiry, 75 Fed. Reg. 44216 (July 28, 2010), *available at* https://federalregister.gov/a/2010-18507. Comments received in response to the 2010 Notice of Inquiry are available at http://www.nist.gov/itl/cybercomments.cfm.

Commerce's recommendations take account of the fact that the Program is voluntary and must appeal to different sectors with different needs. Although some potential incentives could apply across multiple sectors, most organizations face a unique set of cybersecurity risks, business needs, and legal and regulatory environments associated with each particular sector. This report does not offer a full analysis of these various nuances. Instead, it discusses each potential incentive in terms of how well it aligns with the Executive Order's goal of encouraging participation in the Program, whether there are countervailing policy considerations concerning each incentive, and what steps would be necessary to provide these incentives.

III. Recommendations for Incentives to Promote Participation in the Program

1. Partner with the Insurance Industry to Promote Effective Cybersecurity Measures and Best Practices

Potential Incentive

Collaborate with the insurance industry to better understand the cyber risks facing critical infrastructure owners and operators, and develop standards, procedures, and other measures that comprise the Framework that will be effective in addressing these risks. With the advent of underwriting practices that reward the adoption of cyber risk-reducing measures, the cyber insurance market should respond with premium increases for policyholders that fail to adopt effective cybersecurity protections, and corresponding reductions for those that agree to join the Program and adopt effective Framework practices.

Commenter Positions

Commenters in the NOI proceeding noted that a growing number of companies are buying cybersecurity insurance policies. Marsh, a cybersecurity insurance carrier, described its services as covering not only losses and damages, "but also provid[ing] personalized strategies for the mitigation of a variety of cyber incidents."[18] The company noted a 33 percent increase in cybersecurity insurance clients from 2011 to 2012, with cyber insurance limits purchased by its total client base averaging $16.8 million, an increase of 20 percent, over the same time period.[19] One commenter estimated that current, total annual cybersecurity insurance purchases range from $500 million to $1 billion.[20] With the cyber insurance market growing, customers are increasing their coverage limits while continuing to pursue cyber risk mitigation strategies.[21]

---

[18] *See* Marsh 2013 Cybersecurity NOI Comments at 2, *available at* http://www.ntia.doc.gov/files/ntia/marsh_letter_may_3_2013.pdf.

[19] *Id.* Romanosky asserts that such policy limits can range as high as $300 million for some industries. Romanosky 2013 Cybersecurity NOI Comments at 6, *available at* http://www.ntia.doc.gov/files/ntia/romanosky_comments.pdf.

[20] Romanosky 2013 Cybersecurity NOI Comments at 6.

[21] For a discussion of security self-assessment forms required by most insurance carriers, *see id.* at 6-7.

Several commenters argued that the needs of insurance carriers might be served by collaboration with DHS and NIST in developing and implementing the Program and Framework.[22] One respondent explained that insurance carriers "struggle with determining what will be effective and reasonable cybersecurity measures to implement. The confusion surrounding such security measures only makes the insurance underwriting process more difficult, and lends itself to insurance carriers limiting capacity (the total amount of cyber insurance available on a global basis) and being [more] conservative with premiums and deductible limits."[23] Another commenter stated that "continued advancements in the cyber insurance market will depend on access to sufficient loss data and a knowledgeable workforce that stays current with changing technologies and threats."[24] A cybersecurity research fellow offered that insurance companies are in the best position to assess the benefits of different security controls because they possess data from their security assessment forms and claims that can be used to correlate security controls with loss outcomes.[25] This commenter advised "reaching out to insurance companies and encouraging them to participate in academic research that would enable researchers to identify firm characteristics and security controls that are most strongly associated with risk reduction. [Then Commerce could] work with carriers to use these results to help create and drive a set of best-practices that could ultimately become industry standard."[26]

Similarly, insurance carrier Marsh argued that "[i]nsurance is already an accepted mechanism that enables organizations to identify risks and vulnerabilities, and which incentivizes the adoption of best practices . . . including detailed insurance gap analyses; network security surveys to assess vulnerability; security policy reviews and developments; network vulnerability scans; and assessments of internet connectivity vulnerabilities."[27] Marsh reasoned that "once NIST finds agreement with the private sector on those metrics that should be used for the Framework, insurers can adapt the Framework to develop risk profiles of their customers, which

[22] Indeed, Marsh believes that cybersecurity insurance can drive participation in the Program. Marsh 2013 Cybersecurity NOI Comments at 2.

[23] NRECA 2013 Cybersecurity NOI Comments at 6, *available at* http://www.ntia.doc.gov/files/ntia/nreca_comments_april_29_2013.pdf.

[24] American Insurance Association ("AIA") 2013 Cybersecurity NOI Comments at 1, *available at* http://www.ntia.doc.gov/files/ntia/aia-comments-042913.pdf. AIA, with a clear reference to the Framework's nascency, seriously questions "how insurance could incentivize the adoption of a framework of standards, methodologies, procedures and policies that are underdeveloped and have not been proven or even tested as an effective solution to cyber threats." *Id.* at 2. Certainly, collaboration by the insurance industry in developing and validating the effectiveness of Framework elements could prove mutually beneficial to Framework adopters and the insurance industry as described by other commenters.

[25] Romanosky 2013 Cybersecurity NOI Comments at 9.

[26] *Id.*

[27] Marsh 2013 Cybersecurity NOI Comments at 2. *See also* Telecommunications Industry Association ("TIA") 2013 Cybersecurity NOI Comments at 13, *available at* http://www.ntia.doc.gov/files/ntia/tia_comments_042913.pdf (agreeing that cyber insurance can incentivize companies to improve cyber attack resilience).

in turn will enable those insurers to qualify companies for coverage and to price policies appropriately."[28]

The National Rural Electric Cooperative Association ("NRECA"), which stated that its electric utilities members are likely purchasers of cybersecurity insurance, also endorsed this argument. NRECA reasoned that an insurance industry partnership with the Framework developers will lead to a better understanding of "the types of threats and vulnerabilities the Cybersecurity Framework is intended to counter, how it will work, and how proper implementation will measurably increase the cybersecurity posture of a company. If insurance brokers and carriers have this information, it will allow them to better price the risks associated with cyber losses, and provide more accurate and fulsome coverage to policyholders like NRECA members. In effect, a closer dialogue with the insurance industry will allow it to better understand how cybersecurity will be improved through the Cybersecurity Framework, and allow it to more confidently extend 'good driver' discounts to Framework adoptees."[29]

Discussion

The insurance industry, its clients, and Framework developers have common incentives to develop and implement effective Framework elements. These potential partners all have a keen interest in understanding cyber risks, threats, and mitigation efforts that can drive the development of an effective Program and advance insurance carriers' underwriting capabilities. Through this collaboration, carriers would identify effective cybersecurity measures and develop more accurate premiums that reward companies adopting stronger security measures, including those developed through the Program. Critical infrastructure insurers would be able to manage their risk better through an efficient mix of cybersecurity best practices, insurance coverage at reduced premiums, and loss protection.[30]

Recommendation

- *1.1* – NIST should engage critical infrastructure cybersecurity stakeholders, including the insurance industry, when developing and demonstrating the utility and effectiveness of the standards, procedures, and other measures that comprise the Framework and underlie the Program. Cybersecurity insurance carriers would bring extensive knowledge of the

[28] Marsh 2013 Cybersecurity NOI Comments at 2; *see also* Booz Allen Hamilton 2013 Cybersecurity NOI Comments at 8, *available at* http://www.ntia.doc.gov/files/ntia/bah_response_042913_final.pdf. *See also* Romanosky 2013 Cybersecurity NOI Comments at 5 (discussing the defining characteristics of cyber insurance, including interdependent security, correlated failure, and information asymmetry).

[29] NRECA 2013 Cybersecurity NOI Comments at 6. *See also* Encryptics 2013 Cybersecurity NOI Comments at 2, *available at* http://www.ntia.doc.gov/files/ntia/encryptics_response.pdf *and* DCS Corp 2013 Cybersecurity NOI Comments, *available at* http://www.ntia.doc.gov/federal-register-notice/2013/comments-incentives-adopt-improved-cybersecurity-practices-noi#comment-29914 (for a discussion of premium discounts).

[30] Tyler Moore, *Introducing the Economics of Cybersecurity: Principles and Policy Options* 12-13 (Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy) (Nat'l Research Council 2010), *available at* http://www.nap.edu/catalog.php?record_id=12997.

effectiveness of specific cybersecurity practices, which 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 reward, through risk-based pricing, the adoption of cyber risk-reducing measures. These practices should also cultivate a competitive cyber insurance market.

2. Limiting Liability for Cybersecurity Breaches and Actions Under the Program

Potential Incentives

(1) Limit the liabilities that companies face for cybersecurity breaches under existing law.
(2) Limit the liabilities that critical infrastructure owners and operators could face for taking actions that are called for under the Program.

Commenter Positions on Limiting Existing Liabilities

Commenters pointed out that many companies face at least some liability for cybersecurity breaches under current law. These liabilities serve to prevent harm to others or to remedy cybersecurity breaches after they occur.[31] Several commenters suggested that limiting certain kinds of liability, in exchange for meeting Framework standards, would encourage participation in the Program. The relevant liabilities fall into several broad categories.

The first category of cybersecurity liability that commenters discussed is statutory or regulatory standards for cybersecurity performance.[32] For example, commenters pointed out that entities in several critical infrastructure sectors are subject to *ex ante* regulations, *e.g.*, Gramm-Leach-Bliley and the Health Insurance Portability and Accountability Act ("HIPAA"), which require them to maintain cybersecurity safeguards. Companies in those sectors would view inconsistencies between the Program and their existing legal obligations as a disincentive to participate in the

[31] Several commenters noted that critical infrastructure providers internalize some of the costs of cyber attacks, such as disruptions in service, loss of trade secrets, and damaged reputations. These commenters suggest that these internalized costs provide significant incentives for critical infrastructure companies to employ cybersecurity measures. *See, e.g.*, Internet Security Alliance ("ISA") 2013 Cybersecurity NOI Comments at 2-4, *available at* http://www.ntia.doc.gov/files/ntia/2013-04-29_isa_response.pdf; Booz Allen Hamilton 2013 Cybersecurity NOI Comments at 3; Advanced Cyber Security Center 2013 Cybersecurity NOI Comments at 2, *available at* http://www.ntia.doc.gov/files/ntia/acsc_rollout_proposal_april_2013.pdf; Covington & Burling 2013 Cybersecurity NOI Comments at 2.

[32] These legal rules include the Gramm-Leach-Bliley Act, Federal Financial Institution Examination Council control and risk management requirements, the Chemical Facilities Anti-Terrorism Standards, the Federal Energy Regulatory Commission-North American Reliability Corporation Critical Information Protection standards, the Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act, and Nuclear Regulatory Commission rules.

Program.[33] This report, in a separate section, discusses the possibility of streamlining existing regulatory obligations.

Companies also may be obligated to disclose security breaches. For example, most states require companies to notify individuals after certain kinds of personal data are exposed due to a security breach.[34] Similarly, the Securities and Exchange Commission's Division of Corporation Finance has issued guidance stating that "material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading."[35] Mandatory disclosure can encourage companies to improve their cybersecurity practices in order to prevent breaches and to avoid the negative publicity that might accompany disclosure.[36] Although some commenters argued against including a new public disclosure requirement in the Program,[37] none recommended modifying existing disclosure requirements.

In addition, companies may face liability for cybersecurity breaches under consumer protection and tort laws. The Federal Trade Commission has sued companies for failing to employ reasonable and appropriate security in their software, devices, or systems. Private plaintiffs have also brought tort claims (*e.g.*, negligence and product liability) following cybersecurity incidents,[38] though no commenter cited cases in which a private plaintiff prevailed against a critical infrastructure entity with this kind of claim.

Several commenters suggested that reducing or eliminating liability based on tort or consumer protection law for cybersecurity breaches would provide an incentive to participate in the Program. Some commenters argued specifically that limitations on cyber-related tort liabilities

---

[33] Covington & Burling 2013 Cybersecurity NOI Comments at 2; TIA 213 Cybersecurity NOI Comments at 2; IIC 2013 Cybersecurity NOI Comments at 3, *available at* http://www.ntia.doc.gov/files/ntia/iic_04-26-13_response.pdf; U.S. Chamber of Commerce 2013 Cybersecurity NOI Comments at 4, *available at* http://www.ntia.doc.gov/files/ntia/29apr13_chamber_comments.pdf.

[34] Romanosky 2013 Cybersecurity NOI Comments at 3.

[35] U.S. Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2: Cybersecurity, Oct. 3, 2011 (footnote omitted), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[36] Booz Allen Hamilton 2013 Cybersecurity NOI Comments at 3; Romanosky 2013 Cybersecurity NOI Comments at 3.

[37] *See, e.g.*, USTelecom 2013 Cybersecurity NOI Comments at 11, *available at* http://www.ntia.doc.gov/files/ntia/ustelecom-comments-2013-04-29-final.pdf (stating that "it would be harmful to the overall cybersecurity efforts to require the public disclosure of cybersecurity attacks" and "rather than act as an incentive, the public disclosure of such breaches would only serve to educate the attackers and increase the risk").

[38] Microsoft 2013 Cybersecurity NOI Comments at 4, *available at* http://www.ntia.doc.gov/files/ntia/microsoft_response.pdf. *See also* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 Md. L. Rev. 425 (2008) (reviewing cases).

would provide such an incentive.[39] According to one proponent of this view, limiting tort liability could remove some of the uncertainty surrounding financial liabilities for cybersecurity breaches and induce companies to invest more in cybersecurity protections.[40] Another commenter suggested that limitations on tort liability could work on a "sliding scale."[41] For example, compliance with the Framework could be an affirmative defense to claims for punitive damages or other kinds of increased monetary damages.[42]

Another commenter argued that compliance with the Framework should be deemed to constitute an exercise of "due care."[43] If Framework compliance constituted due care, this designation could shield companies from liability for negligence.[44] However, as another commenter noted, simply assuming that following the Framework per se amounts to due care could wrongly imply that implementing the Framework is the only way to exercise due care.[45] Finally, some commenters argued that eliminating private rights of action[46] for cybersecurity-related claims or requiring a higher burden of proof for such claims for Program participants would provide an incentive to join.[47]

Limiting liability for providers of cybersecurity technologies and services also attracted some support. Several commenters cited the SAFETY Act, which limits the liability of companies that provide and deploy qualified anti-terrorism technologies, as a model for cybersecurity liability protections.[48] Extending these protections to cybersecurity countermeasures could encourage companies to produce new technologies and incentivize critical infrastructure owners and operators to purchase and deploy them. One commenter warned, however, that restricting liability limitations to a static list of technologies could encourage companies to invest in technologies that have limited or declining effectiveness against evolving cybersecurity threats.[49]

---

[39] Financial Services Sector Coordinating Council ("FSSCC") 2013 Cybersecurity NOI Comments at 4, *available at* http://www.ntia.doc.gov/files/ntia/fsscc_response_-_doc_noi.pdf; Information Technology Sector Coordinating Council ("IT SCC") 2013 Cybersecurity NOI Comments at 10-11, *available at* http://www.ntia.doc.gov/files/ntia/2013-04-29_-_it_scc_response.pdf; Microsoft 2013 Cybersecurity NOI Comments at 8.

[40] Microsoft 2013 Cybersecurity NOI Comments at 8.

[41] BSA 2013 Cybersecurity NOI Comments at 2, *available at* http://www.ntia.doc.gov/files/ntia/bsa_comments.pdf.

[42] *Id.*; Microsoft 2013 Cybersecurity NOI Comments at 9.

[43] FSSCC 2013 Cybersecurity NOI Comments at 4.

[44] *Id.*

[45] IT SCC 2013 Cybersecurity NOI Comments at 10-11.

[46] Honeywell 2013 Cybersecurity NOI Comments at 2, *available at* http://www.ntia.doc.gov/files/ntia/honeywell_4_26_13f.pdf.

[47] ISA 2013 Cybersecurity NOI Comments at App. C, p. 9.

[48] Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act), Pub. L. 107-296, tit. VIII, subtitle G (codified at 6 U.S.C. § 441 *et seq.*). For comments on the 2013 NOI that discuss the SAFETY Act, see Covington & Burling 2013 Cybersecurity NOI Comments at 2; NRECA 2013 Cybersecurity NOI Comments at 3-54; TIA 2013 Cybersecurity NOI Comments at 23-24; U.S. Chamber of Commerce 2013 Cybersecurity NOI Comments at 4.

[49] USTelecom 2013 Cybersecurity NOI Comments at 9-10.

Commenters acknowledged that legislation would be necessary to implement most of their proposals to limit existing liabilities.

Commenter Positions on Limiting Liability for Actions Taken Under the Program

Commenters also suggested that the government should limit liability arising from actions that companies might take as participants in the Program. These kinds of liabilities could deter companies from participating in the Program. Based on information in the Executive Order, the Notice of Inquiry, and the overall context of cybersecurity policy discussions, commenters hypothesized elements of the Program and discussed how implementing them might violate a participant's legal obligations.

For example, some commenters predicted that the Program could include assessments or audits that create records of a company's security posture. The company could create this record only because it participated in the Program. According to one commenter, such records could become evidence in litigation relating to a security breach, and protecting these records from disclosure in litigation would be appropriate to prevent such use.[50]

Commenters suggested certain countermeasures that could be included as part of the Program could be deemed legally risky.[51] For example, one commenter argued that "certain defensive countermeasures may cause a temporary disruption or degradation of service, which in some cases may constitute a breach of the company's contractual quality of service obligations or create potential tort liability"[52] Others asserted that "uncertainty regarding potential legal liability arising from"[53] the use of countermeasures and "bleeding edge technology and processes" to mitigate cybersecurity risks[54] could deter companies from using these technologies.

According to one commenter, "[w]hen responding to a real-time threat or incident, companies should not be confronted with a Hobson's choice between incurring liability risks in connection with taking the most effective countermeasures and mitigation steps, versus effectuating a sub-standard response that does not raise liability concerns but may not effectively address the threat."[55] Another commenter suggested that companies should receive a safe harbor for "acting in good faith on government furnished threat information," including "any act or omission following the lawful receipt of cyber threat information."[56] Because it is difficult to know in advance which countermeasure a company might deploy to mitigate an attack, one commenter recommended "general liability protection against the wide variety of potential claims—both

[50] Fresen 2013 Cybersecurity NOI Comments at 2, *available* at http://www.ntia.doc.gov/files/ntia/fresen_response.pdf.

[51] NCTA 2013 Cybersecurity NOI Comments at 2, 4-6, *available* at http://www.ntia.doc.gov/files/ntia/042913_ncta_comments.pdf; USTelecom 2013 Cybersecurity NOI Comments at 7.

[52] NCTA 2013 Cybersecurity NOI Comments at 4-5.

[53] *Id.* at 2.

[54] FSSCC 2013 Cybersecurity NOI Comments at 4.

[55] NCTA 2013 Cybersecurity NOI Comments at 6.

[56] Honeywell 2013 Cybersecurity NOI Comments at 2.

known and unknown" as an incentive to encourage "attaining the most optimal cyber defense posture and implementation of the most effective response measures and mitigation steps."[57]

Finally, several commenters posited that information sharing could be part of the Framework and discussed potential sources of liability arising from information sharing between companies and between companies and the government. DHS is implementing the Executive Order's information sharing provisions separately from the Program. Accordingly, this report does not discuss liability that relates to information sharing.

Discussion

Liabilities Under Current Law

The most focused recommendations from commenters for limiting existing liabilities pertained to general tort liability. It is unclear from the record, however, whether cyber-related tort liability is a significant concern for critical infrastructure companies. The only specific case that a commenter cited involved a consumer electronics company, and the plaintiff lost that case.[58] Commerce is not aware of any tort claims against critical infrastructure providers for loss resulting from a cyber attack. The record also lacked examples of other areas in which limiting liability helped to align companies' incentives with investment in additional precautions to reduce the risk of harm arising from hazards akin to cyber attacks.[59] In the absence of a clear record of lawsuits that result in inefficient uses of resources to address cybersecurity risks, or conversely, of parties being unable to obtain redress for their injuries, Commerce advises further study on the concept of modifying tort liability.

Liabilities for Actions Taken as a Program Participant

The Administration is currently studying the idea of limited liability protections in other areas that could be directly related to the Program, depending on its development. For example, as part of the National Strategy for Trusted Identities in Cyberspace (NSTIC), which the President issued in order to address critical cybersecurity weaknesses caused by inadequate online identification and authentication solutions, the President stated that "the Federal government may

[57] NTCA 2013 Cybersecurity NOI Comments at 6.

[58] *See* Microsoft 2013 Cybersecurity NOI Comments at 4 (discussing a "class action lawsuit against Sony" after an "attack on some of Sony's online services," noting that the lawsuit was dismissed, and raising the question of "whether there is a more efficient and affirmative way to incentivize improved cybersecurity practices" among non-critical infrastructure companies).

[59] This point was raised clearly in a June 3, 2013 letter from Chairman John Rockefeller to Acting Secretary of Commerce Cameron Kerry: "In short, such liability protections would turn existing market incentives for implementing cybersecurity best practices on their head. Prospectively relieving companies from responsibility for the massive costs that a failure to manage cybersecurity risks might someday impose on American society discourages, rather than promotes, the Executive Order's goal of improved cybersecurity." Letter from Senator John Rockefeller, Chairman of the United States Senate Committee on Commerce, Science, and Transportation, to Acting Secretary of Commerce, Cameron Kerry at 3 (June 3, 2013), *available at* http://www.ntia.doc.gov/files/ntia/cyber_letter_to_acting_secretary_kerry.pdf.

need to establish or amend both policies and laws to address" concerns such as "the uncertainty and fear of unbounded liability that have limited the market's growth," but concerns about where liability should fall still exist.[60] The privately-led Identity Ecosystem Steering Group established in support of NSTIC is also currently contemplating whether such changes to policies and laws will in fact be needed.[61]

Countermeasures—the other main area of putative Program activities that commenters discussed in connection with liability—are also part of active legislative discussions in Congress and within the Administration.[62] Limitations on liability for deploying countermeasures are difficult to assess in the abstract. Some countermeasures, such as Internet service providers blocking botnet attack traffic, could cause unwanted side effects, such as blocking legitimate traffic. Such risks may be worth taking, but they require a careful assessment in the context of a specific legislative proposal.

Finally, limiting liability for cybersecurity products and services, such as the SAFETY Act's provisions for anti-terrorism technologies,[63] suggest the same need for caution as discussed in connection with limiting liability for countermeasures.

Recommendation

- *2.1* – Once the Program is developed, DHS, in consultation with the Department of Justice, should study whether critical infrastructure owners face significant legal and financial risk from tort liabilities and whether these risks inhibit owners' participation in the Program. This study could be limited to the sector(s) most relevant to the critical infrastructure that DHS finds to be at greatest risk.[64] This study should include a review of tort cases against critical infrastructure owners and operators and an assessment of what mechanisms, if any, critical infrastructure owners have to transfer tort liability (*e.g.*, contractual provisions, statutory immunities or limitations, common law defenses) for damage from cyber attacks.

[60] White House, National Strategy for Trusted Identities in Cyberspace (NSTIC) at 31 (Apr. 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[61] *See* Identity Ecosystem Steering Group, http://www.idecosystem.org/.

[62] NCTA 2013 Cybersecurity NOI Comments at 4; USTelecom 2013 Cybersecurity NOI Comments at 7.

[63] Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act), Pub. L. 107-296, tit. VIII, subtitle G (codified at 6 U.S.C. § 441 *et seq.*).

[64] *See Executive Order*, *supra* note 1, at § 9 (requiring DHS 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" within 150 days of the signing of the Executive Order).

3. Promoting Adoption of the Program through Federal Grants

Potential Incentive

Provide federal grants for owners and operators of critical infrastructure to defray costs associated with participating in the Program, and promote effective cybersecurity practices by introducing cybersecurity considerations into evaluations for federal grants.[65]

Commenter Positions

Respondents identified cost as a significant barrier to improving cybersecurity. USTelecom noted that "costs have previously been identified as one of the single biggest obstacles to the implementation of improved cybersecurity measures."[66] The 2009 Cyberspace Policy Review similarly concluded that "many technical and network management solutions that would greatly enhance security already exist in the market place but are not always used because of cost or complexity."[67]

Commenters supported the use of implementation grants as an incentive to directly address this perceived cost impediment. USTelecom identified grants "for the direct purchase of cybersecurity products and services" as a helpful incentive.[68] The National Cable and Telecommunications Association ("NCTA") suggested "direct Federal funding" through grants as a mechanism to "defray the high fixed costs associated with development, investment, and deployment of the most up-to-date cybersecurity assets and tools" while the American Gas Association issued a similar response.[69]

Another commenter asserted the need for grants to Information Sharing and Analysis Centers ("ISACs"), either to reward good processes or improve processes. The Financial Services Sector Coordinating Council ("FSSCC") suggested rewarding ISACs for meeting certain goals for information sharing or providing grants for adopting improved technology for analyzing information.[70] The Internet Security Alliance ("ISA") supported the latter initiative, providing grants to ISACs to raise their maturity levels.[71]

Honeywell indicated that an alternative to providing grants for investments in cybersecurity products or services could be to "tie existing grants to the adoption of the cybersecurity

---

[65] Although this section focuses on grants, similar reasoning may apply to loan programs. *See* LADWP 2013 Cybersecurity NOI Comments at 2; ISA 2013 Cybersecurity NOI Comments at App. B.

[66] USTelecom 2013 Cybersecurity NOI Comments at 8. All comments in this section came in response to the Department of Commerce's April 2013 Notice of Inquiry.

[67] White House Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure at 31 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[68] USTelecom 2013 Cybersecurity NOI Comments at 7-8.

[69] NCTA 2013 Cybersecurity NOI Comments at 2; AGA 2013 Cybersecurity NOI Comments at 2.

[70] FSSCC 2013 Cybersecurity NOI Comments at 3.

[71] ISA 2013 Cybersecurity NOI Comments at 44.

framework."[72] The Los Angeles Department of Water and Power ("LADWP") also recognized this option as a palatable alternative to providing new grants.[73]

Discussion

The record suggests two incentives for consideration. First, the Program could provide federal grants to owners and operators of critical infrastructure to defray the costs associated with participating in the Program. This kind of grant could provide a direct, positive incentive to join the Program. Second, the White House could issue guidance to federal agencies recommending that they include cybersecurity protections as appropriately weighted criteria for evaluating federal grant applications.

Both potential incentives have significant drawbacks. The first incentive could create moral hazard by providing a subsidy for companies that choose not to invest their own resources in participating in the Program. In addition, this kind of grant would require legislation.

The second incentive—integrating cybersecurity protections as evaluation criteria for federal grant applications and giving appropriate weight to Program participation— could be accomplished within existing budget authority. For example, the White House could provide evaluation guidelines for federal agencies to implement, in accordance with agency-specific grant program practices. Still, the appeal of this incentive is relatively limited. It would not guarantee broad coverage of critical infrastructure sectors because only those critical infrastructure entities interested in obtaining a federal grant would respond to this incentive. But this incentive would help to develop greater awareness among critical infrastructure providers of the importance of improving cybersecurity.

Recommendations

- *3.1* – As NIST makes future decisions about pilot grants for programs, such as those related to the National Strategy for Trusted Identities in Cyberspace ("NSTIC"), it should work with DHS to study whether NIST should credit consistency with the Framework when awarding pilot grants. This determination would be based on the use of the Identity Ecosystem, under development as part of NSTIC, as a component of the Program. Similarly, Commerce should also look into using Framework adoption and Program participation as a consideration for critical infrastructure grants.

- *3.2* – The White House should consider issuing guidance to federal agencies recommending that they include cybersecurity protections as appropriately weighted criteria in federal grant application evaluations. This recommendation, while not necessarily tied to the Program, would help to develop greater awareness among critical infrastructure providers of the importance of improving cybersecurity.

[72] Honeywell 2013 Cybersecurity NOI Comments at 2.
[73] LADWP 2013 Cybersecurity NOI Comments at 2, *available at* http://www.ntia.doc.gov/files/ntia/042913_ladwp_comments.pdf.

4. Innovation Centers & Research Cooperatives

Potential Incentive

Provide technical assistance through innovation centers and/or research cooperatives for program participants.

Commenter Positions

ISA put forward the idea of utilizing a cybersecurity public-private cooperative to improve security standards. "This organization could be charged with improving, even reinventing the cyber ecosystem in a more secure manner. Under this Cooperative's umbrella, stakeholders could share information and cybersecurity technology development to create (or fund the creation of) more alternative networking protocols, software languages, and/or hardware architectures that are more secure. . . . It could also serve as the equivalent of an [underwriter's] laboratory for cyber security by independently assessing best practices and standards along sliding scales."[74]

General Dynamics suggested the establishment and promotion of virtual innovation centers where industry vendors, government, and customer adopters can "jointly collaborate on real-life use cases and implementations where guidelines, best practices, implementation profiles, and eventually standards can be identified and developed for trusted or trustworthy solutions and prototypes."[75] Additionally, General Dynamics proposed that the results of the innovation centers also be made available to financial services organizations in order to "fastpath promising solutions."[76]

Google advocated for a "grand challenge for cybersecurity" and that a "challenge could attract the best minds in both the private and public sectors.[77] For example, an ongoing challenge with annual progress prizes, an additional grand prize, open-sourced results (*e.g.*, published papers and disclosure of successful steps forward), and public recognition of the participants and their respective success could create a virtuous cycle of innovation and competition in this space."[78] This idea of a grand challenge would be a low-cost way for the government to incentivize R&D and competition in the private sector.

---

[74] ISA 2011 Cybersecurity NOI Comments at 18-19, *available at* http://www.nist.gov/itl/upload/ISA-Comments-to-DoC-Cybersecurity-Green-Paper-Submitted-8-1-11-2.pdf.

[75] General Dynamics 2011 Cybersecurity NOI at 7, *available at* http://www.nist.gov/itl/upload/General-Dynamics-C4-Systems_NIST-RFC-110801.pdf.

[76] *Id.*

[77] Google 2011 Cybersecurity NOI Comments at 9, *available at* http://www.nist.gov/itl/upload/Google_20110801175225438.pdf.

[78] *Id.*

Discussion

Public-private research cooperatives would seek to foster closer ties between industry, government, and academia, and would establish a pipeline for cybersecurity tools and strategies that take business needs, such as cost, into consideration. The cooperatives would also give the private sector a role in establishing research priorities.

The National Cybersecurity Center of Excellence ("NCCoE"), run by NIST, is one example of a cybersecurity innovation center and research cooperative. It is a collaborative environment where engineers, from across public and private organizations, can come together to demonstrate secure platforms, built on commercially available technology, for the purpose of increasing the rate of adoption of secure technologies.

Although the focus of the NCCoE is currently broader than critical infrastructure, it provides a useful model for other research cooperatives. Particularly, the NCCoE provides a good example of balancing both industry and government desires by establishing use cases based on the security needs of businesses, and demonstrating that the solution also satisfies government cybersecurity guidance. By participating in this collaborative process, backed by the NCCoE, critical infrastructure institutions can establish a basis for trust-based cybersecurity responsibility, a potential market differentiator. NCCoE staff are already committed to working in the Framework process, in helping to identify areas where collaboration can begin.

Recommendation

- *4.1* – The NCCoE should work with DHS to link real-world challenges to research and development efforts. The NCCoE could assist in developing solutions for cybersecurity gaps identified by the Program, particularly when commercial solutions are available but encounter barriers to implementation. The NCCoE can, in turn, work with Program participants and vendors of information technology goods and services to help identify commercially available solutions with potential for greater use and areas where greater R&D will be needed to meet pressing cybersecurity challenges.

5. Streamlining Information Security Regulations and Other Government Processes

Potential Incentive

Streamline the cybersecurity requirements of existing laws and regulations, and streamline permitting, licensing, patenting, or other government requirements for members of the DHS Program.

Commenter Positions

Several respondents suggested that streamlining regulatory requirements for Program participants would be a desirable incentive. This incentive would reduce government-induced costs on industry, an alternative to direct government subsidies such as tax incentives.[79] Existing regulations, such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, Chemical Facilities Anti-terrorism Standards, and others, impose some cybersecurity obligations. For instance, HIPAA requires covered entities to report breaches affecting more than 500 individuals to the Department of Health and Human Services,[80] and Gramm-Leach-Bliley requires companies defined as "financial institutions" to ensure the security and confidentiality of personal information collected from customers.[81] Several trade associations suggested that companies working across critical infrastructure sectors already have overlapping cybersecurity requirements and regulations. Streamlining the regulations to which a Program participant must comply could be a concrete incentive to join the Program.[82]

Another area for streamlining that was identified was in regulatory audits currently required by different statutes for multi-sector companies. Commenters suggested that audits required by laws such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, etc., could be consolidated and built into the Program. ISA stated that current cybersecurity audits are burdensome, and "[i]f the government could develop a sound baseline audit to simply remove the redundancy, this could be offered as a carrot to enterprises that demonstrate investment in proven effective cybersecurity techniques."[83] Specifically, eliminating redundancy in auditing requirements would contribute to increased preparedness, because a high rating on an initial audit could lead to fewer audits in the future, creating an incentive for companies to improve security upfront. Industry could then be encouraged to invest funds that would otherwise have been used for compliance into cybersecurity R&D, further strengthening security systems.

Other commenters have discussed streamlining other government processes as an incentive – for example, allowing fast-track patent review for members of the Program.[84] USPTO has had similar programs to encourage green technology and technologies combating issues plaguing many of the world's poor.[85] Although a fast-tracked patent process for Program members is not

---

[79] ISA 2011 Cybersecurity NOI Comments at 8-9.

[80] Grant Thornton, *HIPAA/HITECH Cybersecurity solutions* (April 1, 2013), http://www.gt.com/staticfiles/GTCom/Advisory/IT/HIPAA%20HITECH%20Cybersecurity%20solutions/Grant%20Thornton%20HIPPA-HITECH%20Solutions.pdf.

[81] 15 U.S.C. § 6801 *et seq.* (1999).

[82] UTC 2013 Cybersecurity NOI Comments at 4, *available at* http://www.ntia.doc.gov/files/ntia/utc_noi_response.pdf; API 2013 Cybersecurity NOI Comments at 6, *available at* http://www.ntia.doc.gov/files/ntia/api_noi_response_f26apr13.pdf; Internet Infrastructure Coalition 2013 Cybersecurity NOI Comments at 3; US Chamber of Commerce 2013 Cybersecurity NOI Comments at 4.

[83] ISA 2011 Cybersecurity NOI Comments at 23-24.

[84] ISA 2013 Cybersecurity NOI Comments, app. A at 5.

[85] *See* U.S. Patent and Trademark Office, *Green Technology Pilots Program - CLOSED*, http://www.uspto.gov/patents/init_events/green_tech.jsp; U.S. Patent and Trademark Office, *Patents for Humanity* http://www.uspto.gov/patents/init_events/patents_for_humanity.jsp.

directly related to improving technology for cybersecurity, R&D intensive companies have experienced intellectual property losses as the result of cyber-intrusions.[86] Some critical infrastructure companies hold large patent portfolios, and thus the financial incentive stemming from fast-tracked patents may serve as a reasonable incentive to join the Program.

Discussion

Many of the suggestions to streamline regulatory cybersecurity requirements in this section are broad and may relate to the creation of liability considerations and other legal benefits discussed elsewhere in this paper. Still, the commenters raise an important point: can the creation of a voluntary effort take the place of existing, overlapping requirements?

In the creation of the Framework and the Program, both NIST and DHS demonstrated that they are taking existing regulatory structures into account in an effort to avoid duplication.[87] For instance, Section 10(c) of the Executive Order requires that "within 2 years after publication of the final Framework, . . . agencies identified in subsection (a)[88] of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements."[89] As this work progresses, the Section 10(c) work of DHS and NIST could be used by Congress to streamline existing requirements for Program participants.

The Fast-Track Patent Pilot is another option that stands out for its clarity of purpose and execution. Although a patent pilot would not advantage the specific categories of patents that critical infrastructure providers would likely submit, R&D intensive industries – such as oil and gas, telecommunications, and transportation – may indeed be more willing to join the Program if it could help offset general patent costs.[90] The resulting increased Program participation would extend wider benefits to the nation and the economy.

Incentives that would truly streamline existing regulations may require legislative action. While NIST and DHS can work with sector-specific agencies to make sure that the Framework and Program limit duplication to the best of their abilities under current law, the actual task of offering regulatory streamlining as an incentive would likely need to be established by law.

---

[86] *See e.g.* Executive Office of the President, *Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets* (Feb. 2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf (detailing economic loss due to cyber attacks).

[87] Developing a Framework To Improve Critical Infrastructure Cybersecurity, 78 Fed. Reg. 13024-01 (Feb. 26, 2013).

[88] These are agencies with responsibility for regulating the security of critical infrastructure.

[89] *Executive Order*, *supra* note 1 at § 10(c) (requiring reporting of redundant regulatory requirements).

[90] ISA 2013 Cybersecurity NOI Comments at 31.

USPTO can set up fast-track pilots under existing law. The scope of pilots should not impose such a burden that it affects the ability of USPTO to otherwise perform its mission and meet its existing performance goals.

Recommendations

- *5.1* – NIST and DHS should continue to ensure that the appropriate agencies document how the Framework and the Program work in relation to the existing regulatory structures. Once the first version of the Framework has been published and the Program is operational, this information could be used by Congress as a means of creating incentives by streamlining existing regulations. This effort is consistent with Section 10(c) of the Executive Order.

- *5.2* – USPTO should further explore the idea of building a Fast-Track Patent Pilot for Program participants, including examining whether the potential scope of such a pilot could be broad enough to serve as a real incentive to R&D intensive critical infrastructure companies.

6. Federal Procurement Considerations

Potential Incentive

Provide preferential federal procurement considerations for participants in the Program, or require Program participation before a critical infrastructure owner or operator can engage in business with the U.S. Government.

Commenter Positions

Respondents shared mixed reactions to the use of federal procurement considerations to incentivize participation in the Program. Broadly, the use of government procurement considerations could be particularly effective because, as the Center for Democracy and Technology submitted, "manufacturers prefer to design software that can be used both by the Government and by the private sector."[91] Thus, "increased security standards for government systems can promote increased security for private systems."[92] As Microsoft stated, this incentive might have greater relevance because of tighter competition in the market for public sector spending. Microsoft believes the U.S. Government should leverage its procurement power to encourage improved cybersecurity practices, and recommended that such efforts be "technology neutral so that they do not favor a particular solution or vendor to the exclusion of others that might satisfy the Government's needs."[93] Covington & Burling LLP and the Chertoff Group submitted that incorporating cybersecurity into government procurement would be a

[91] CDT 2010 Cybersecurity NOI Comments at 3, *available at* http://www.nist.gov/itl/upload/Center-for-Democracy-and-Technology_Cybersecurity-NOI-Comments_9-20-10.pdf.

[92] *Id.*

[93] Microsoft 2013 Cybersecurity NOI Comments at 13.

"low-cost, high-impact measure," which would allow companies to differentiate themselves, as long as the criteria are technology neutral.[94]

The Chamber of Commerce supported government procurement as an incentive as long as the Administration "[does] not determine how companies design, develop, and manufacture their technology and products."[95] This statement parallels concerns raised by other respondents regarding government involvement in how products are designed and developed. ITI expressed a strong preference that "federal procurement policy in no way include any mandates regarding how the IT industry designs and develops its products," including how companies run their supply chain.[96] ITI was concerned that such an approach could "lead to de facto technology mandates on the U.S. IT industry and disrupt the innovation process of U.S. IT companies, as well as the global business model of build-once, sell globally and adherence to global standards."[97] Oracle, Intel, Cisco, and IBM also expressed concerns that this incentive might give the U.S. Government authority to dictate the design, development, or supply chain of commercial IT products. In their view, not only would these regulations have the potential to slow the U.S. Government's uptake of new technologies, it could "balkanize the global market with the effect of putting U.S. companies at a competitive disadvantage around the globe, and undermine the existing Common Criteria regime already led by the NIAP [National Information Assurance Partnership]."[98] Such procedures could adversely affect both innovation and security.

Additional respondents raised concerns about the use of cybersecurity standards in government procurement, particularly regarding the agility with which the U.S. Government is able to adopt and deploy up-to-date technologies. A submission by Oracle, Intel, Cisco and IBM raised concerns with "[t]he government's cumbersome and lethargic federal acquisition process has often left federal employees using outdated and at times unpatched technologies."[99] An additional regulation to the acquisition process could further slow the U.S. Government's uptake of new technologies, rather than speed it up.

Discussion

The use of a procurement incentive has been proposed in several previous reports, including the President's Cyberspace Policy Review from May/June 2009 and output from DHS's Cross Sector Cyber Security Working Group, Incentives Subgroup from September 2009. There would be two general approaches to implementing federal procurement considerations based on cybersecurity: 1) Provide preferential considerations to participants in the Program; or 2) Require participation by critical infrastructure owners and operators in the Program to do business with the government; and numerous ways to structure the actual incentive. Both approaches raise

[94] Covington & Burling 2013 Cybersecurity NOI Comments at 3.
[95] U.S. Chamber of Commerce 2013 Cybersecurity NOI Comments at 5.
[96] ITI 2011 Cybersecurity NOI Comments at 14, *available at* http://www.nist.gov/itl/upload/ITI-Comments-on-Commerce-Dept-Cyber-Green-Paper-FINAL.pdf.
[97] *Id.*
[98] Cisco/IBM/Intel/Oracle 2011 Cybersecurity NOI Comments at 12, *available at* http://www.nist.gov/itl/upload/Cisco-IBM-Intel-Oracle-Green-Paper-comments-8-1-11.pdf.
[99] *Id.*

challenging questions. For example, how would making participation in the Program a condition of contracting with the federal government affect small businesses? Is this approach consistent with the voluntary nature of the Program? Could the requirement, or alternatively a preference for Program participants, feasibly be restricted to critical infrastructure owners and operators? How many critical infrastructure owners and operators are also small businesses? What are the international trade implications of this approach?

To further investigate the potential government procurement incentive, a separate report from the Secretary of Defense and the Administrator of General Services, also required by Executive Order 13636, will make specific recommendations to the President on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration.

Recommendation:

- *6.1* – Based on the comments received and our preliminary analysis, the use of government procurement considerations could provide an incentive for companies to participate in the Program. NIST and the Office of the Secretary of Commerce will closely consider the upcoming report that will be issued by the U.S. Department of Defense and General Services Administration to ensure a full understanding of potential consequences, and will work with these agencies, the United States Trade Representative, and other relevant federal offices and agencies to further examine government procurement as a possible incentive to participate in the Program.

7. Tax Incentives

Potential Incentive

Provide tax incentives, including tax deductions for R&D or lower capital gains rates on the sale of assets of corporations that participate in the Program.

Commenter Positions

Numerous respondents support the idea of tax incentives as a way to spark innovation and investment in cybersecurity R&D and the adoption of improved standards. There are many ways this incentive could be implemented. For example, TechAmerica advised that "ways to devise a refundable tax credit for cybersecurity investments should be explored,"[100] while Triad Biometrics suggested that "[i]ncentives could take the form of tax credits for R&D relating to improved cyber-risk abatement."[101] FSSCC recommended instituting a program where "all costs associated with complying (*e.g.*, time, hardware and software) with the NIST Framework could

[100] TechAmerica 2010 Cybersecurity NOI Comments at 27, *available at* http://www.nist.gov/itl/upload/TechAmerica_Cybersecurity-NOI-Comments_9-20-10.pdf.

[101] Triad Biometrics 2010 Cybersecurity NOI Comments at 2, *available at* http://www.nist.gov/itl/upload/Triad-Biometrics_Cybersecurity-NOI-Comments_9-16-10.pdf.

be considered tax deductible or amortized over a period of time thus providing a financial incentive for private sector entities to invest in Framework implementation."[102] A second option put forward by FSSCC would provide tax credits or deductions to critical infrastructure owners, operators, and the firms that "interface with their systems or networks who have also adopted the Framework. This would encourage the owners of these utilities to promote the Framework to firms participating on their networks (*e.g.*, ACH), thereby increasing the overall security of the network and providing a tax benefit for all involved."[103]

One concern commenters raised is that the provision of tax or R&D credits might not create substantial savings for large companies and thus would not be an incentive to participate in the Program. One incentive that would target these large, publicly-traded companies would be to reward shareholders with a lower capital gains tax rate on the sale of assets (stocks and bonds) of corporations that participate in the Program. This incentive would integrate cybersecurity into a company's overall strategy with shareholder support, leading companies to "sustain investment in cyber assurance while maximizing overall return on investment to shareholders."[104] Shareholders of companies that do not meet the security standards specified in the Program or elect not to participate would pay the normal capital gains tax rates. As proposed by VOXEM, "to qualify their shareholders for the lower capital gains tax rate, corporations would certify to the Securities and Exchange Commission" that they are in compliance with the Program with penalties for misrepresentation.[105] This incentive has the potential to motivate the private sector to adopt improved cybersecurity standards and act in the interest of national security in order to deliver value to their shareholders.

Discussion

The federal government frequently uses tax incentives to encourage specific behaviors. For example, the Hiring Incentives to Restore Employment ("HIRE") Act, enacted in 2010, provides lower taxes for businesses that hire individuals who are among the longer term unemployed.[106] This law motivates businesses to hire long-term unemployed individuals by effectively exempting them from their share of Social Security taxes on wages and providing a $1,000 business tax credit for 2011 if the workers were retained at least a year. A second example of tax incentives to promote positive behavior is the Energy Star program, run by the Environmental Protection Agency and the Department of Energy. The government provides tax incentives to consumers and businesses to purchase energy-efficient products. This same mechanism could be applied to cyberspace for businesses that support critical infrastructure to purchase secure technologies and improve cybersecurity standards. The use of tax incentives as a means to

[102] FSSCC 2013 Cybersecurity NOI Comments at 4.
[103] *Id.*
[104] Voxem 2013 Cybersecurity NOI Comments at Appendix 1, *available at* http://www.ntia.doc.gov/files/ntia/voxem_noi_response.pdf.
[105] *Id.* at Appendix 2.
[106] Hiring Incentives to Restore Employment Act (HIRE Act), PL 111-147, 124 Stat 71 (March 18, 2010).

increase the adoption of cybersecurity standards was also included in the Cyberspace Policy Review released by the Administration in 2009.[107]

While it is very clear that tax credits are popular among companies, it is less clear that some of the specific tax incentives suggested would actually motivate companies to join the Program. For example, R&D tax credits work over the long-term, but it is not clear they can serve as the kind of short-term motivation that can get a company to join the Program. The record does not contain much evidence that such a tax credit would work in this case. Also, it is not clear that the capital gains tax cuts for shareholders would provide enough of a direct benefit to companies unless the company itself holds shares and sells them to take advantage of the lower capital gains rate.

Creating any type of tax incentive to encourage participation in the Program would require legislative action. Moreover, it is difficult to calculate the anticipated costs of such tax proposals without specific information about how many companies would participate or file for cybersecurity tax relief, and to what extent.

Recommendation

- *7.1* – Based on the comments received, Commerce's analysis, and discussions with other relevant federal agencies, Commerce does not recommend further consideration of tax incentives to encourage participation in the Program.

8. Additional Suggested Incentives

In addition to the previously discussed incentives, respondents suggested many other ways that the U.S. Government could be involved with improving cybersecurity for critical infrastructure, including:

- Study the creation of a certification system to identify and provide public recognition to companies that participate in the program.
- Provide prioritized technical assistance to program participants.
- Provide expedited security clearances to program participants.

Commenter Positions on Public Recognition

Respondents took a variety of positions on the use of public recognition as an incentive to induce participation in the Program. For supporters of public recognition, this incentive could be used to boost consumer confidence and promote trust in the owners and operators of critical infrastructure. As StopBadware stated, awarding seals to companies that pledge to uphold certain standards "have proven effective at driving baseline privacy and security practices in

[107] White House Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure at 19, 28.

other contexts" and thus have the potential to be successful in improving cybersecurity.[108] On the other hand, NCTA opposed the use of public recognition as an incentive, calling it the "wrong" approach.[109] NCTA argued that a "name-and-shame" program would "call attention to vulnerabilities in critical infrastructure that will draw the attention of those entities intent on launching cyber attacks."[110]

Commenter Positions on Prioritized Technical Assistance

Few respondents commented on instituting a system of prioritized technical assistance for participants in the Program. Honeywell supported the idea of such an incentive but did not provide details on the implementation of such a program. NCTA responded by calling the use of preferential treatment, such as prioritized technical assistance, "the wrong approach" to establishing compliance with a minimum set of security standards.[111] NCTA identified the use of preferential treatment as a reverse incentive that would negatively affect the adoption of improved standards.[112]

Commenter Positions on Expedited Security Clearance Process

Respondents who addressed the use of security clearances as an incentive to join the Program, including NRECA, the American Gas Association, and the American Public Power Association, expressed support for this incentive. NRECA noted that in order to effectively undertake the information sharing between the public and private sectors that is necessary for improved cybersecurity, the private sector must be able to access Secret or Top Secret classified materials. As NRECA stated, "[t]he granting of such clearances will help ensure that valuable information is passed along not only in a timely manner, but also in a way that is meaningful to end users such as NRECA members."[113] An alternative approach to the security clearance process submitted by Monsanto called for increased sponsorship of "security clearances for companies, [which] would help facilitate timely conversations on emerging threats, and expedite and further enhance cybersecurity throughout the nation" or, in this case, participate in the Program.[114]

Discussion

Although respondents who submitted comments related to prioritized technical assistance or expedited security clearance as an incentive were generally supportive of such programs, these types of proposals are of concern to Commerce. The agency believes strongly that the need for assistance and clearance should be by the government based on an organization's need and

---

[108] StopBadware 2011 Cybersecurity NOI Comments at 1, *available at* http://www.nist.gov/itl/upload/StopBadware_response-to-DOC-Cybersecurity-Green-Paper.pdf.

[109] NCTA 2013 Cybersecurity NOI Comments at 12.

[110] *Id.*

[111] *Id*.

[112] *Id.*

[113] NRECA 2013 Cybersecurity NOI Comments at 5.

[114] Monsanto 2013 Cybersecurity NOI Comments at 3, *available at* http://www.ntia.doc.gov/files/ntia/monsanto_comments-04-26-13.pdf.

should not be contingent on an organization's adoption of a program for critical infrastructure. For this reason, these two categories should not be used as an incentive to join the Program in those instances, but should continue to be pursued for critical infrastructure companies. Commerce would support technical assistance as an incentive for non-emergency situations, but the value of this type of incentive would need to be demonstrated to be effective over time.

A public recognition program has the potential to provide direct value to participants of the Program. This increased recognition along with increased consumer confidence could provide direct financial returns to participation in the Program. The voluntary Program may leverage existing private sector approaches, encourage the development of private sector programs and/or utilize collaborative public/private sector approaches. By joining the Program, or leveraging private sector approaches, participants would show their commitment to cybersecurity and would be rewarded through a seal of recognition, potentially increasing the market value of the company. Although concerns have been raised that a public recognition program could cause harm instead of benefits by making recognized businesses a target for malicious actors, participants in the Program could have the option of displaying the seal, but should not be required to do so. Legislation would not be necessary to implement this type of public recognition effort.

Recommendations

- *8.1* – Commerce should work with DHS to study the creation of an optional public recognition program for participants in the Program that could leverage private sector approaches. Many companies expressed interest in a form of public recognition, such as an emblem or seal, which they could display to convey that they follow certain practices. Commerce believes that most companies that join the Program will want to display such an emblem but also understands that some companies are concerned that their displaying a seal could lead attackers to target them. Therefore, Commerce recommends studying how public recognition efforts, including the use of emblems or a seal, could support the Program.

- *8.2* – Commerce recommends exploring the provision of 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.

- 8.3 – Commerce does not recommend that further steps be taken to provide prioritized technical assistance or expedited security clearances to participants in emergency situations. Commerce considers the expedited security clearances already allowed to owners and operators of critical infrastructure under the Executive Order to be sufficient.

IV. Summary Table of Recommendations

Type of Incentive	Number in Report	Commerce Recommendation	Is Legislation Necessary to Implement?
Partner with the Insurance Industry in Promoting Effective Cybersecurity Measures and Best Practices	1.1	NIST should engage critical infrastructure cybersecurity stakeholders, including the insurance industry, when developing and demonstrating the utility and effectiveness of the standards, procedures, and other measures that comprise the Framework. This collaboration should 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 that results in premium reductions for critical infrastructure clients who agree to join the Program and adopt effective Framework practices.	No.
Limiting Liability for Cybersecurity Breaches	2.1	Once the Program is developed, DHS, in consultation with the Department of Justice, should study further whether critical infrastructure owners face significant legal and financial risk from tort liabilities and whether these risks inhibit owners' participation in the program. This study should include a review of tort cases against critical infrastructure owners and operators and an assessment of mechanisms	The study will not need legislation, but depending on the results, a legislative solution may be necessary.

Type of Incentive	Number in Report	Commerce Recommendation	Is Legislation Necessary to Implement?
		what mechanisms, if any, critical infrastructure owners have to transfer tort liability (*e.g.*, contractual provisions, statutory immunities or limitations, common law defenses) for damage from cyber attacks..	
Promoting Adoption of the Program through Federal Grants	3.1	As NIST makes future decisions about pilot grants for programs such as those related to the National Strategy for Trusted Identities in Cyberspace ("NSTIC"), it should work with DHS to study whether NIST should credit consistency with the Framework when awarding pilot grants. Similarly, Commerce should also look into using Framework adoption and Program participation as a consideration for critical infrastructure grants.	No.
	3.2	Commerce recommends that the White House issue guidance to federal agencies to promote cybersecurity protections as appropriately weighted criteria for evaluating federal grant applicants.	No.
Innovation Centers & Research Cooperatives	4.1	NIST's National Cybersecurity Center of Excellence ("NCCoE") should work with DHS should work with DHS to link real-world challenges to research and development efforts. The NCCoE could assist in developing solutions for cybersecurity gaps identified by the Program, particularly when commercial solutions are available but encounter barriers to	No.

Type of Incentive	Number in Report	Commerce Recommendation	Is Legislation Necessary to Implement?
		implementation. The NCCoE can, in turn, work with Program participants and vendors of information technology goods and services to help identify commercially available solutions with potential for greater use and areas where greater R&D will be needed to meet pressing cybersecurity challenges.	
Streamlining Information Security Regulations and Other Government Processes	5.1	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.	Yes, it is likely that NIST and DHS would develop a list for Congress that would require legislation.
	5.2	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 the idea of 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.	No.
Federal Procurement Considerations	6.1	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	It seems unlikely that a legislative solution would be necessary, but we look to the U.S. Department of Defense and General Services Administration to make that

Type of Incentive	Number in Report	Commerce Recommendation	Is Legislation Necessary to Implement?
		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.	determination.
Tax Incentives	7.1	Commerce does not recommend further consideration of tax incentives to encourage participation in the Program.	Yes.
Additional Suggested Incentives	8.1	Commerce recommends studying how recognition for those that participate in the program could be utilized as an incentive, depending, on the organization, sector, and risk tolerance.	No.
	8.2	Commerce recommends exploring the provision of 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.	No.
	8.3	Commerce does not recommend that further steps be taken to provide prioritized technical assistance or expedited security clearances to participants in emergency situations. Commerce considers the expedited security clearances already allowed to owners and operators of critical infrastructure under the Executive Order to be sufficient.	No.