Treasury Department
Report to the President on

Cybersecurity Incentives
Pursuant to Executive Order 13636

SUPPORTING ANALYSIS

PART I: INTRODUCTION

Our national and economic security depends on the reliable functioning of this nation's critical infrastructure, especially in an interconnected, data-driven world. We rely on the Internet and other computer networks to run systems that help light our homes, provide fuel for our cars, and ensure that our water is safe to drink. Each day, trillions of dollars of electronic transactions flow across the payment networks and settlement systems that touch nearly every corner of our financial system and help keep track of funds in business and consumer accounts.

However, the cyber threat to critical infrastructure is growing. It represents one of the most serious challenges that the United States must confront. Because the majority of our critical infrastructure[1] is owned and operated by private companies, facing this threat requires government and industry to work together to strengthen our digital defenses.

On February 12, 2013, President Obama signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."[2] The Executive Order establishes a policy of enhancing the security and resilience of the nation's critical infrastructure and maintaining a cyber-environment that encourages efficiency and innovation while, importantly, protecting privacy and civil rights. It provides for all Federal agencies and departments to take appropriate steps to secure our critical infrastructure, in advance of any legislative action. In addition, the Executive Order outlines the terms of a partnership with owners and operators of critical infrastructure to improve information sharing and collaboratively develop and implement risk-based standards.

As part of the Executive Order, President Obama instructed: (1) the Director of the National Institute of Standards and Technology (NIST) of the Department of Commerce to develop a "Cybersecurity Framework" (or "Framework")[3] and (2) the Secretary of Homeland Security to establish a voluntary program to support the adoption of the Framework by owners and operators of critical infrastructure and other interested entities. Work on the Framework and voluntary program is currently ongoing. The Executive Order also directed the Secretary of the Treasury, along with the Secretary of Commerce and the Secretary of Homeland Security, to

[1] Critical infrastructure is defined in the Executive Order as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

[2] Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11737 (February 19, 2013) (herein after "Executive Order"), available at https://federalregister.gov/a2013-03915.

[3] As envisioned in the Executive Order, the Framework should "include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks." It should, in addition, "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."

each make recommendations on a set of incentives that would promote private sector participation in the voluntary program.[4]

This report outlines an approach for policymakers to evaluate the benefits and relative effectiveness of government incentives in promoting the adoption of the eventual Framework. It seeks to identify types of situations in which private incentives may be insufficient to provide an appropriate level of cybersecurity. Then, the report reviews a set of seven potential policy options, in areas where the Treasury Department has significant experience or expertise, that could be used as incentives to encourage the voluntary adoption of the Framework.[5] These policy solutions, while targeted at critical infrastructure organizations, might also be applicable to a broader group of private sector participants.

In preparing this report, Treasury directly engaged with stakeholders and coordinated with the Department of Commerce (Commerce) and the Department of Homeland Security (DHS). Treasury also reviewed the 45 formal responses to Commerce's Notice of Inquiry[6] as well as public comments from stakeholders at panels hosted by DHS and other private sector groups.[7] In addition, Treasury independently solicited and received input from critical infrastructure organizations in the financial services sector and other critical infrastructure groups.

However, this report is part of ongoing work by the government. In October 2013, NIST is expected to publish a preliminary version of the Framework in anticipation of a final version early next year. As the Executive Order states, that Framework will be reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, feedback

---

[4] Executive Order, supra note 2, at Sec. 8(d): "The Secretary of [Homeland Security] shall coordinate establishment of a set of incentives designed to promote participation in the [voluntary cybersecurity] Program. Within 120 days of the date of this order, the Secretary and Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law or authorities to participants in the Program."

[5] This report is not intended to provide an analysis of all available policy options. To complement the efforts of its counterparts at the Department of Commerce and the Department of Homeland Security, the Treasury Department narrowed the scope of its review from DHS's broader list of 14 incentive categories to seven incentive categories, in which it has significant experience in policy development or administering a cybersecurity program.

[6] *See NTIA*, Comments on Incentives To Adopt Improved Cybersecurity Practices NOI (April 29, 2013), http://www.ntia.doc.gov/federal-register-notice/2013/comments-incentives-adopt-improved-cybersecurity-practices-noi

[7] This includes engagement with the Incentives Working Group, the Cross-Sector Cybersecurity Working Group, the Financial and Banking Information Infrastructure Committee, the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, L.L.C., the Financial Services Information Sharing and Analysis Center, and the Internet Security Alliance.

from owners and operators of critical infrastructure, implementation concerns, and other relevant factors.[8]

PART II: GENERAL PRINCIPLES FOR GOVERNMENT INCENTIVES

Safeguarding critical infrastructure is fundamental to preserving the stability of our financial system. The dependence of the global financial system on a rapid and accurately functioning technological infrastructure cannot be overstated. At the same time, cybersecurity threats pose significant financial, compliance, and reputational risks that can reverberate throughout the financial system. Indeed, the 2013 Financial Stability Oversight Council (FSOC) annual report states that cyber incidents that "disrupt, degrade, or impact the integrity of critical financial infrastructure could have consequences on operations and efficiency" of financial institutions and markets.[9]

In recognition of the crucial role that technological infrastructure plays in the operation of financial markets and the economy as a whole, financial institutions and market utilities are subject to regulation and examination standards relating to network and systems integrity. Moreover, many financial firms have a long history of voluntary collaboration with government through public-private partnerships, such as the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, LLC (FSSCC) and the Financial Services Information Sharing and Analysis Center (FS-ISAC), which has been active in advising firms on ways to strengthen cybersecurity measures. Notwithstanding existing regulations and the fact that many critical infrastructure organizations already maintain high cybersecurity standards, establishing incentives that encourage adoption of the Framework may lead them to further increase their overall cybersecurity level and help to reduce the risk of successful attacks.[10] The financial services sector's adoption of the Framework should complement, rather than substitute for, the existing regulatory and supervisory regime.

More broadly, the same logic applies to critical infrastructure organizations in other industries. And the next part of this section provides a framework for evaluating how those incentives might be most effectively deployed. Generally, government policy tools to provide incentives to private sector participants should be considered when private incentives are insufficient to provide a desirable level of additional investment in an area, such as increasing cybersecurity. Economists refer to this condition as a market failure.

---

[8] Executive Order, supra note 2, at Sec. 7(f).

[9] Financial Stability Oversight Council Annual Report (2013), pp. 136.

[10] Beyond providing incentives, economic research has suggested that there may be other effective ways to encourage adoption of Framework. This might include establishing default settings on products or policies so that individuals that used them were automatically in compliance with the Framework.

Of course, not every potential market failure requires direct government intervention. Although externalities, which arise when one party's actions directly impose costs or benefits on others, are widespread in the private sector, certain incentives (such as reputation preservation) and private arrangements (such as bilateral contracting solutions to internalize costs or cooperative and self-policing arrangements to address coordination problems) already exist to make public intervention unnecessary in many cases.

When a market failure exists and private market solutions are inadequate, government support in the form of incentives may be appropriate. If a government role is warranted, the potential incentive should ideally: (i) be appropriately tailored and scaled to the magnitude of the under-investment in cybersecurity; (ii) protect taxpayers by being cost-effective while still achieving the policy objectives; (iii) adjust to changing circumstances and the availability of new information; (iv) be coordinated, so as not to duplicate, other incentives; and (v) motivate private sector entities to expend their own resources to further protect their critical infrastructure assets. These principles should be crucial factors in any decision about whether the government should provide incentives; however, they should not be viewed as requirements.

The next part of this section identifies several market failures pertaining to cybersecurity. It also broadly outlines potential incentives or other policy solutions that could be used to address them.

Underinvestment in Knowledge. A private company may limit its investment in cybersecurity research to a level it believes is sufficient to further its objectives, even if increased investment in research may provide the company both additional benefits and spillover benefits to other companies. Although those additional and spillover benefits would raise the overall level of cybersecurity, companies still underinvest for reasons of cost or perception that existing threats do not warrant additional investment. Such underinvestment is a market failure that could justify government support for certain types of cybersecurity research and development.

Barriers to Information Sharing. Government, pursuant to its national security, regulatory, or other roles, may have access to specific information on threats or mitigation measures. Private firms that are preparing to defend against an impending cyber threat, or recently experienced a cyber incident, might also have specific information that could help identify potential vulnerabilities, induce other firms to make new investments in security technologies, or aid them in taking additional steps to reduce the risk of cyber events. Yet the existence, or even perception, of certain legal and regulatory measures can prevent the public and private sectors from sharing information that could yield security benefits. These circumstances may justify some form of government intervention through incentives. With respect to sharing classified information, the potential costs of disclosure would have to be carefully assessed, and the circumstances and means of disclosure appropriately circumscribed. Government could also facilitate information sharing among private firms. In doing so, however, it is important to

safeguard firms' concerns about reputation and competition, and third parties' concerns regarding privacy and contractual obligations.

Coordination Failures. The financial services sector relies on multiple networks, such as exchanges, clearinghouses, and payment systems, all of which connect many users. The interconnectedness of market participants through these institutions and other relationships could mean that the failure of one member (such as a network utility) to implement adequate cybersecurity measures could increase the vulnerability of other network members to a cyber incident. In systems for which access can be controlled, the owners or managers of the system have some incentive and ability to require certain security measures from users and participants. These measures may include required minimum security standards to participate in the network, a monitoring system, and contractual assignment of liability. Even so, the possibility of market failures arising from coordination failures persists. Even in controlled access systems, for example, without coordination, some members may choose to underinvest and enjoy a free ride on the investment of others. Accordingly, government could respond through a combination of regulatory requirements and incentives to further encourage private sector cybersecurity collaboration and coordination.

Network Externalities. The full benefit of a new security protocol might not be achieved until it is adopted by a sufficient number of users in a network; as a result, there may initially be a reduced incentive for individual software developers to create new protocols. Network effects can also lead to technology "lock-in." Here, users become bound to a certain operating platform or protocol because of the costs of switching from an established, widely-used hardware or software system to a new, less widely-used one, even if the new platform or protocol may be more secure. Private firms have begun paying for the identification of software vulnerabilities, and selling the information to the creators and users of the software. This can prod software developers into making upgrades that they might otherwise not have created. Nevertheless, government may also be able to address network externalities with incentives, including regulation, either to improve the security of existing networks or, in appropriate cases, change protocols or platforms.

Moral Hazard. If companies do not bear the full consequences of their actions, they may not put in place the appropriate measures needed to achieve an optimal level of cybersecurity. A failure or an inability to assign liability to a party that has not taken sufficient security measures could lead to underinvestment in cybersecurity. In an insurance context, private underwriters of cyber insurance should continue to recognize that policyholders may, because of insurance, fail to take necessary or sufficient actions that would decrease the probability of the occurrence of a cyber incident or mitigate the financial consequences of such an event.

Adverse Selection. In today's cyber insurance market, prospective policyholders likely have greater knowledge about their security practices than the insurers – a type of market failure arising from asymmetric information. As a result, insurers may not be able to differentiate

between more or less risky policyholders, and may accordingly fail to charge the appropriate premium rates. Such circumstances would enable higher-risk, prospective policyholders to buy insurance at a subsidized cost or not adequately reward prospective policyholders that adopt prudent cybersecurity measures. To mitigate this problem, as part of the underwriting process insurers typically establish minimum standards that all policyholders must meet, as well as rating factors that distinguish between risk levels. Disclosure of relevant information by the insured, whether mandated by government or the private sector, can play a similar role in making sure all parties have a standardized level of information.

PART III: EVALUATION OF POTENTIAL GOVERNMENT INCENTIVES

1. Enhancing Information Usage Capabilities to Support Information Sharing

Improving Cybersecurity. Critical infrastructure stakeholders suggested that real-time information sharing would significantly improve cybersecurity by providing firms with quicker access to knowledge they need to pro-actively bolster their defenses.[11] This means improving and increasing the flow of information among critical infrastructure organizations about security threats observed by the organizations themselves, and the government's dissemination of such information to the private sector for preventive purposes. The significant attribute of this type of information sharing program is that it must occur as a routine matter, rather than solely in the context of an incident, and that it must involve mutual sharing obligations by private entities. Government can play a significant role in overcoming the perceived legal, regulatory, and other barriers to sharing information. More broadly, government policy may indirectly help solve the coordination failures noted earlier in this report.

Advantages and Disadvantages. Although private firms recognize the value of receiving such information, they indicate that they may be hesitant to contribute to an information sharing program, principally out of liability concerns.[12] For example, firms are apprehensive that their information, if confidential and not subject to any duty of disclosure, could become a matter of public knowledge and adversely impact their reputation, financial position, or result in litigation over the appropriateness of their public disclosures. In this vein, financial and other critical infrastructure stakeholders have also expressed concern that confidential information they provide the government in good faith could be made public under a Freedom of Information Act (FOIA) or other open records request.[13] Other grounds for concern over litigation relate to legal prohibitions (contractual, regulatory, or statutory) that may govern the sharing of firm information with third parties. Stakeholders state that any information sharing scheme would not be successful unless there were some litigation protections.

[11] Comment letter from Booz Allen Hamilton (April 29, 2013) (hereinafter "BAH letter"), pp. 8; Comment letter from the FSSCC (April 29, 2013) (hereinafter "FSSCC letter"), pp. 2; Comment letter from the Telecommunications Industry Association (April 29, 2013) (hereinafter "TIA letter"), pp. 12; Comment letter from the United States Telecom Association (April 29, 2013) (hereinafter "U.S. Telecom letter"), pp. 6-7.

[12] Comment letter from Microsoft Corporation (April 29, 2013) (hereinafter "Microsoft letter"), pp. 14-16.

[13] Comment letter from the American Gas Association (April 29, 2013) (hereinafter "AGA letter"), pp. 2; FSSCC letter, supra note 11, at 4; Comment letter from Honeywell International Inc. (April 29, 2013) (hereinafter "Honeywell letter"), pp. 2; Comment letter from the Internet Infrastructure Coalition (April 26, 2013), pp. 2; Comment letter from Monsanto (April 26, 2013) (hereinafter "Monsanto letter"), pp. 2; Comment letter from the National Cable & Telecommunications Association (April 29, 2013) (hereinafter "NCTA letter"), pp.7.

Stakeholders also expressed concern that information shared in good faith could, if disclosed to competitor firms, give those competitors an advantage.[14]

To allay the foregoing concerns, information sharing can be highly targeted to deliver actionable information only to those with a need to receive and in a form that is anonymized. Moreover, both the private and public sector may be able to leverage existing infrastructure by broadening and deepening engagement with ISACs, to ease the cost and implementation burden. There are some limitations. First, even with a well-executed information-sharing program, there is no guarantee that firms will act upon the information they receive. Second, as organizations like ISACs expand, there may be a point at which there are diminishing returns from participation. The more extensive an information-sharing program becomes, the more likely that firms will "free-ride" on the benefits of hearing lessons learned of others without making contributions of their own. In addition, one unintended consequence could be that the more that data is shared, the greater the risk that some critical information may leak, exposing the organization to new or additional threats.

Current Status. The federal government shares information with private sector organizations when there is a cyber incident or an imminent, specific threat. Treasury has already been working to improve and increase the regular flow of information — between firms, between regulators and firms, and through FS-ISAC, which was established to share threat and vulnerability information with firms across the sector. Treasury's Office of Critical Infrastructure Protection and Compliance Policy (OCIP) routinely plays a facilitating role with the financial services sector, encouraging financial institutions that have experienced an attack to reach out to their counterparts and other appropriate agencies, regulators and law enforcement.[15]

Encouraging Adoption of the Framework. The federal government must make information that could be useful to improving cybersecurity available to affected firms, especially in the context of imminent or ongoing incidents. However, the Executive Order specifically calls for the establishment of a voluntary information sharing program for critical infrastructure organizations.[16]

In order to fully participate in this program, critical infrastructure organizations must have the capability to send, receive, and act upon information about cyber threats and vulnerabilities. Adoption of the Framework could lead to the creation of more standardized information-sharing practices and policies, which would help these firms and others that adopt its

[14] NCTA letter, supra note 13, at 8-9.

[15] Treasury's OCIP has authority to increase its dissemination of timely cyber threat information to the financial services sector, provided that such dissemination is consistent with other applicable authorities including laws protecting privacy, civil rights, civil liberties, and national security information.

[16] Executive Order, supra note 2, at Sec. 4.

measures to better utilize threat information for the timely and effective mitigation of cyberthreats within their environments.

In keeping with the Executive Order, the Framework must ensure that there are appropriate protocols governing both the form in which it is shared and controls over further dissemination. The protocols should be designed to avoid compromising privacy, civil rights, civil liberties, and U.S. national security, as well as to protect reputational and competition concerns of the firms sharing the information. In terms of protecting confidentiality of information, supervisory rules governing confidential bank examinations might be informative. Other relevant paradigms may be found in recent legislative proposals, which contain provisions that limit dissemination and use of the information that is shared by an entity.[17] For example, stripping information of personal identification elements that do not implicate cybersecurity or preserving the anonymity of the institution providing the information that is disseminated to other institutions may be important safeguards.

2. Leveraging Framework Adoption to Clarify Liability Risk

Improving Cybersecurity. Establishing a standard of conduct that would recommend minimum levels of performance could minimize liability risk for entities that have faced a cyber incident and caused damages to another party. Therefore, it should be considered as a mechanism for strengthening cybersecurity practices through incentives. It could also assist in mitigating moral hazard, namely the concern that private firms will take undue risks if they do not bear the full consequences of their actions.

Assigning liability, on the basis of established, widely recognized practices is one way of creating an incentive for critical infrastructure organizations to take affirmative steps to improve cybersecurity and possibly minimize their risk of loss in the event of litigation following an incident. Joining the voluntary program that supports the Framework, or implementing the Framework – or at the very least, some of its practices – could serve this purpose and provide the basis for greater legal certainty sought by many critical infrastructure stakeholders. A firm that does not meet these practices might be found negligent in failing to prevent a cyber incident or failing to take actions to limit the consequences arising from a cyber incident. A firm that meets or surpasses these recommendations, meanwhile, might not be held liable for damages arising from the incident.

[17] For example, Title VII of S. 3414 - the Cybersecurity Act of 2012 - a Senate bill that failed to be enacted last year, also included a provision that prohibited a private entity from using shared information to gain an unfair competitive advantage, as well as restricted the use, retention, or further disclosure of that information to protecting information or information systems from cybersecurity threats, or mitigating those threats.

Advantages and Disadvantages. Further discussion of consensus practices could induce more critical infrastructure organizations to improve their cybersecurity measures alone, especially if deploying best practices or, more specifically, best-in-class software or equipment were made part of the Framework. It should also encourage deployment of additional security measures, whereby a firm could demonstrate that it has taken more than sufficient measures to meet the Framework could defend itself in the event of a civil action for damages resulting from a cyber incident.

The result of Framework development might also encourage the sharing of cyber incident information by firms. As noted earlier, many critical infrastructure organizations recognize the value of information sharing programs but are reluctant to participate because information and other statements that they contribute might be held against them during litigation. If a firm using the Framework or is a participant in the voluntary program at the time of the cyber incident, it might be less reluctant to share information about the cyber incident and the firm's cybersecurity defenses. Moreover, sharing information could enhance the firm's ability to follow the Framework and improve cybersecurity, thus furthering its ability to defend itself against liability.

Of course, determining implementation of the Framework will be challenging. And, as discussed further below, establishing the Framework as a relevant standard may introduce some element of moral hazard, undermining the policy goal of encouraging critical infrastructure organizations to adopt advanced practices in the Framework.

Current Status. Although there are many cybersecurity standards, practices, and guidelines, they do not appear to be consistently or uniformly applied.[18] This kind of uncertainty may lead to heightened levels of financial, legal, and reputational risk for critical infrastructure organizations. Establishing participation in the voluntary program that supports Framework, or the implementation of some or all of its measures, could provide critical infrastructure organizations with greater legal certainty. However, policymakers will first need to address whether and how to do so.[19] Once the Framework is adopted, courts, through a series of judicial decisions, could establish the implementation of the Framework or practices therein as relevant standards of conduct for purposes of determining liability, particularly where they are not fixed by legislation or administrative regulations.

As with recent legislative proposals, satisfaction of the practices found in the Framework could be used as a complete or partial defense against liability. At least two approaches could be

[18] Such cybersecurity standards include those set forth by ISO/IEC 27001, ISO 15408, the International Security Forum, North American Energy Reliability Corporation (NERC), NIST, Internet Engineering Task Force, International Society of Automation and American National Standards Institute, and ISA Security Compliance Institute.

[19] For example, the standard could be fixed by legislation or, in the absence of legislation, defined by a series of judicial decisions.

taken. First, demonstrated compliance with the practices within the Framework could serve as an affirmative defense, thus creating a liability safe harbor for critical infrastructure organizations.[20] A safe harbor approach would create incentives for firms to meet the Framework's practices, and thus would generally enhance cybersecurity levels.

Alternatively, legislation could provide that demonstrated compliance with the Framework's practices establishes a rebuttable presumption of reasonable conduct by the defendant critical infrastructure organization, subject to further proof by the plaintiff that the critical infrastructure organization could have taken additional reasonable steps under the circumstances to prevent the loss, but did not. Under the latter approach, critical infrastructure organizations would not have a complete defense against liability by adopting the Framework. While the latter approach could mitigate the moral hazard risk by potentially requiring critical infrastructure organizations to do more, it might not provide the legal certainty that critical infrastructure stakeholders seek.

Encouraging Adoption of the Framework. As the voluntary program is developed, the resulting level of certainty that might accompany participation the program or using the practices in the Framework could serve as an attractive incentive for critical infrastructure organizations to join the program. This is because critical infrastructure organizations will know that if they adopt the Framework, their risk of loss in a civil action for damages directly caused by a cyber incident might be reduced if they are, at the time of the cyber incident, following practices consistent with it.

Many critical infrastructure stakeholders have indicated that establishing the Framework as a standard of conduct would be a strong incentive to induce adoption of the Framework, in substantial part if firms are granted liability protections in return for adopting the Framework or joining the voluntary program.[21] Although it may be beneficial to provide some appropriately-defined additional liability protection for critical infrastructure organizations that adopt the Framework, broadly shielding firms from legal liability may introduce an element of moral hazard and cause firms to take insufficient precautionary measures. For these reasons, liability protection as an incentive should be continued to be studied by the Administration.

3. Government Funding to Encourage Basic Cybersecurity Research

[20] For example, section 104(c) of S.3414 – the "Cybersecurity Act of 2012" – generally provides that a critical infrastructure organization shall not be liable for punitive damages in any civil action for damages directly caused by a cyber incident if such organization is, at the time of the cyber incident, in substantial compliance with the appropriate cybersecurity practices established by a new, federal inter-agency council.

[21] Microsoft letter, supra note 12, at 9-13; Comment letter from U.S. Chamber of Commerce (April 29, 2013) (hereinafter "U.S. Chamber letter"), pp. 3-4.

Improving Cybersecurity. Federal funding for research and development (R&D) of cybersecurity measures has been identified as a policy tool that could improve security. Stakeholders in many sectors identified federally-funded R&D as playing a key role in advancing cybersecurity products and practices.[22]

Private sector companies, like software developers, have strong financial incentives to invest in R&D tied to their products because they will be able to appropriate the bulk of the gains. Even so, a software developer may still underinvest in such research relative to a desirable level of cybersecurity, because the developer determines that greater investment will not be to its net benefit, or it determines that its customers are "locked-in" to using its existing operating platforms and software, or for other reasons.[23] Therefore, government may need to bridge the gap by providing direct financial support to the software developer in order to encourage additional research. In other words, it can help address market failures arising from the underinvestment in knowledge, coordination failure, and network externality problems discussed in Part II.

Advantages and Disadvantages. Government support for applied research may be more attractive to critical infrastructure organizations because they will accrue a larger share of the benefits. But federal grants for basic research may provide greater rewards to society overall. For example, basic research can support the development of more secure code, more effective security training tactics, and more robust operating platforms. In turn, that can strengthen cybersecurity for critical infrastructure end-users and a broader group of private sector participants that reap these spillover benefits. Consider a software company that creates a more secure product as a result of federally-funded research. The company's product is now safer, its end users are better protected, and confidence in their business practices improves, which in turn, may free up resources for more productive purposes. Academic studies have documented other broad spillover effects from basic research, such as the introduction of new methods and information, the development of skilled graduates, and the establishment of new firms.[24]

Of course, there will always be a question of whether the outcome of funded basic research actually supports the purpose for which the grant was originally intended. Most basic research tends to have a longer time horizon and a broader mission. In addition, drawing a

---

[22] FSSCC letter, supra note 11, at 3; NCTA letter, supra note 13, at 9; TIA letter, supra note 11, at 2, 12-13; Comment letter from the Utilities Telecom Council (April 8, 2013), pp.4; Comment letter from the National Electrical Manufacturers Association (April 29, 2013), pp. 3.

[23] Anderson, Ross. "Why Information Security is Hard – An Economic Perspective. In 17th Annual Computer Security Applications Conference (2001), pp. 358-365.

[24] As examples, see "Academic Research and Industrial Innovation: an Update of Empirical Findings." by Edwin Mansfield, Research Policy 1998; "The Relationship Between Publicly Funded Basic Research and Economic Performance: A SPRU Review." HM Treasury, London 1996, available at http://www.hm-treasury.gov.uk/d/156.pdf.

boundary between basic research, and applied R&D that has a specific intended application in mind, may be difficult. Any federal grants should be awarded judiciously.

Current Status. The federal government currently provides direct support for basic R&D pertaining to cybersecurity, with research grant and other support administered by several agencies, such as the National Science Foundation, DHS's Science and Technology Directorate and its Homeland Security Advanced Research Projects Agency, and the Intelligence Advanced Research Projects Activity.[25] Although Treasury does not directly provide R&D funding, Treasury's OCIP has been a strong advocate within the government for R&D that is critical for promoting cybersecurity innovation in the financial sector.[26]

Encouraging Adoption of the Framework. Research grants, defined broadly, were cited by several critical infrastructure stakeholders as a potential incentive to encourage adoption of the Framework.[27] For example, stakeholders in the financial services sector identified cybersecurity "innovation grants" as a potential inducement and called for the creation of a "National Program Office."[28]

Other stakeholders were more measured, with one commenter noting that federally-funded R&D tends to focus on fundamental research, which does not incentivize increased cybersecurity.[29]

Some stakeholders raised the idea that critical infrastructure organizations could receive preferential treatment for federal research funds in return for Framework adoption. [30] In that vein, Treasury believes the Framework could serve as an incentive if research proposals aligned with the Framework received preferential treatment for federal research funds. To increase the effectiveness of these research grants, agencies should use alignment with the Framework as a selection criteria. Research that is informed by, and intended to support, the Framework is more likely to lead to beneficial products and services.

In light of the existing federal grant-making infrastructure, the addition of another grant making agency appears unnecessary. However, Treasury, in its capacity as the Sector-Specific

[25] In addition stakeholders identified the collaborative approach of applied research exhibited in NIST's National Cyberspace Center of Excellence and the proposed Federally Funded Research and Development Center. Both were noted in comments from the Telecommunications Industry Association and National Telecommunications and Information Administration in response to the Department of Commerce Notice of Inquiry.

[26] For example, Treasury's OCIP has brought together the FSSCC, DHS, and NIST to create a Cooperative Research and Development Agreement on identity proofing, which has identified new methods for satisfying the "know your customer" requirements of financial institutions.

[27] Honeywell letter, supra note 13, at 2; U.S. Telecom letter, supra note 11, at 7-8.

[28] FSSCC letter, supra note 11, at 3.

[29] Comment letter from Sempra Energy Utilities (April 29, 2013) (hereinafter "Sempra letter"), pp. 1.

[30] NCTA letter, supra note 13, at 9-10.

Agency (SSA) for the financial services sector, could assume more expanded duties, such as communicating the financial industry's R&D interests to government grant administrators, and conversely, identifying and publicizing federal grant-making resources to the financial sector. No additional legislation would be required since Treasury's OCIP already serves as an "R&D liaison" on a limited basis.[31]

4. Providing Technical Assistance

Improving Cybersecurity. A significant number of critical infrastructure stakeholders identified technical assistance as a policy tool to strengthen cybersecurity.[32] In this context, technical assistance means assisting critical infrastructure organizations to properly configure their computer networks, patch system vulnerabilities, or address other potential threats as requested and necessary.

Critical infrastructure organizations' access to prioritized and enhanced levels of assistance, both regularly and during incidents, could improve computer network security and reduce the likelihood of a successful cyber incident. Providing technical assistance to critical infrastructure organizations could overcome some of the information coordination issues discussed in Part II.

Advantages and Disadvantages. Technical assistance could be well-targeted, providing tailored advice to the specific circumstances of each critical infrastructure organization. It also could provide a very immediate and flexible response, enabling firms to adapt quickly to changing cyber threats. Technical assistance should be thought of as a complement to — not a substitute for — other information sharing initiatives, such as accelerating the dissemination of security clearance application materials to critical infrastructure organization personnel or strengthening real-time information sharing.

However, there are significant implementation challenges. Scaling a technical assistance program could quickly become expensive, even if the assistance was restricted to critical infrastructure organizations. That is because the federal government bears all of the costs and may not have sufficient personnel or other resources in place to provide one-on-one consultation on a widespread basis.

Federal technical assistance may also raise concerns of moral hazard, whereby critical infrastructure organizations may not take the proper precautions to secure their systems because they believe the government will ultimately respond in the event of a cyber threat. Such organizations may also forego consultation with private sector service providers and put in place

[31] Appropriations for Treasury's OCIP are available to develop and implement programs, which could include establishing an "R&D liaison" program.

[32] Honeywell letter, supra note 13, at 3; Comment letter from the Los Angeles Department of Water and Power (April 29, 2013) (hereinafter "LADWP letter"), pp. 2.

fewer precautionary measures than might otherwise be desirable. Along these lines, stakeholders have noted that technical assistance primarily benefits businesses with more limited resources.[33] On the other hand, there is also a possibility that technical assistance from government could be stigmatizing if the fact becomes publicly known. As a result, critical infrastructure organizations may sometimes choose not to request government help. Nonetheless, the potential benefits of providing enhanced and particularized technical assistance could outweigh the potential drawbacks, especially if critical infrastructure organizations have put in place measures consistent with the Framework.

Current Status. To date, Treasury's OCIP facilitates cybersecurity technical assistance to financial institutions largely on a case-by-case basis, where such technical assistance is provided in response to a cyber incident. Typically, a financial institution will reach out to its primary regulator to request assistance in connection with an incident. After evaluating and approving the request, the regulator passes the request along to OCIP, which will assess the request to identify the type of problem needing assistance, and then work with other federal government entities to provide appropriate assistance, if it is available.

Encouraging Adoption of the Framework. The federal government will continue to provide technical assistance to any firm that requests emergency help. However, in non-emergency situations, the offer of additional programmatic technical assistance supporting implementation of the Framework could be used to spur adoption of the Framework.[34] Given the myriad of ways that a formal technical assistance program could be structured, however, it is difficult to assess its potential effectiveness as an incentive at this time

For example, during the implementation stage, any critical infrastructure organization seeking to adopt the Framework could be eligible for basic technical assistance regarding the implementation of measures that are consistent with Framework.[35] This could lower adoption costs.

Technical assistance could also be employed as an incentive after critical infrastructure organizations have adopted the Framework. Under this scenario, critical infrastructure organizations that demonstrated they had adopted the Framework would have access to continued technical assistance and relevant information to facilitate compliance with the Framework. The provision of such forms of assistance and information could enable enhanced protection for cyber-systems.

Additionally, when technical assistance is provided to a critical infrastructure organization, it might receive a series of source documents to increase its knowledge on how to

[33] U.S. Telecom letter, supra note 11, at 9.

[34] LADWP letter, supra note 32, at 2-3.

[35] Comment letter from Emmanuel Adeniran (April 29, 2013), pp. 3.

defend its system. These source documents could include the Framework and information on how adoption of the Framework could increase the security of the organization's systems. In this way, provision of technical assistance to critical infrastructure organizations that had not adopted the Framework could act as an incentive to encourage it to implement the Framework. No additional legislation would be required to expand Treasury's role as a facilitator of technical assistance. [36]

5. Further Accelerating the Security Clearance Process

Improving Cybersecurity. A significant number of critical infrastructure stakeholders identified accelerating the clearance process as a policy tool that could strengthen cybersecurity.[37] Security clearances would increase and improve information sharing between the government and private sector, enabling critical infrastructure organizations to overcome the information barrier and coordination failures identified in Part II.

Today, government security clearances for personnel at critical infrastructure organizations are typically granted on a limited basis, and from the perspective of many private sector firms, the clearance process can take several months to a year to complete. As a result, some stakeholders expressed concern that, during a cyber incident, targeted firms may be limited in their ability to obtain information that might be helpful to protect their systems.[38]

In July 2013, the federal government took a significant step toward accelerating the security clearance process for critical infrastructure organizations. In response to the Executive Order, DHS submitted a plan to the Assistant to the President for Homeland Security and Counterterrorism to overhaul its security clearance processes and timetables.[39] The revamped process calls for nominations of qualified personnel from critical infrastructure organizations to receive approval from the DHS Assistant Secretary for Infrastructure Protection within 48 hours of receipt, and be granted an interim Secret clearance within five to seven days of when the applicant submits all required paperwork. Then, in keeping with the Intelligence Reform and Terrorism Prevention Act, the Office of Personnel Management generally has 40 days to conduct

[36] Treasury's OCIP may use its appropriations to develop and implement a cybersecurity-related technical assistance program to help financial institutions identify vulnerabilities and mitigate incidents. This would be consistent with its responsibilities as the SSA for the financial services sector under Presidential Policy Directive/PPD-21 ("Critical Infrastructure Security and Resilience") (February 12, 2013), which provides in pertinent part that SSAs shall provide, support, or facilitate technical assistance for their respective sectors.

[37] See notes 38, 41, and 44.

[38] Comment letter from National Rural Electric Cooperative Association (April 29, 2013) (hereinafter "NRECA letter"), pp. 5.

[39] On July 12, 2013, DHS submitted its plan to the Assistant Secretary for Homeland Security and Counterterrorism for expediting the processing of security clearances for critical infrastructure organizations. This plan sets forth new clearance processes and timetables under a three-tiered prioritization system, including expedited prioritization for critical infrastructure organizations identified under section 9 of Executive Order 13636. It also lays out additional communication and reporting procedures.

the background investigation and the requesting agency generally has 20 days to adjudicate the paperwork and make a decision regarding granting access to classified information and issuance of the security clearance.[40]

Treasury welcomed the new streamlined process for critical infrastructure organizations, known as "expedited prioritization." However, even with recent changes, Treasury believes that improved controls – including tracking the processing times at every step of the clearance process, rather than just investigation and adjudication times – would lead to significant improvements. For example, the time between when DHS receives a clearance nomination and when the appropriate DHS official signs off on that nomination and submits it for investigation is not currently tracked by the federal government. Notably, Treasury's recent experience suggests it is a major bottleneck in the system. Treasury believes this step of the process should be carefully tracked on a regular basis by DHS and other federal agencies, consistent with the newly revised clearance process.

Treasury, as the SSA for the financial services sector, is also scheduled to receive from DHS a monthly report on the status of all applications for security clearances for the sector and the specific status of each application. In addition to this information, Treasury believes that it would be beneficial to have a single point of contact at DHS – a designated individual who would be responsible for promptly responding to outside inquiries about the status of pending security clearance applications and address actual or perceived bottlenecks.

Furthermore, Treasury recommends that the federal government be more active in educating all private sector organizations of the eligibility criteria and the approval process for obtaining a security clearance. Treasury believes the communication portion of the plan that DHS submitted in response to the Executive Order is an important new development and fully supports that effort.

Advantages and Disadvantages. Currently, the federal government investigates and adjudicates security clearances in a timely fashion. However, Treasury believes that other parts of the security clearance process could be accelerated. Together, the measures noted above – the new "expedited prioritization" process, tighter controls, and greater educational outreach – should yield significant improvement. That, in turn, should help support the enhanced exchange of information on a regular basis, aiding those critical infrastructure organizations in their ability to protect their systems and national security.

[40] Section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. § 435b) generally established security clearance processing timeliness goals of 60 days – 40 days to conduct the background investigation, and 20 days to adjudicate —and the federal government has met this goal every quarter since 2009. However, this timetable does not include the time it has taken DHS to review and have the appropriate official sign off on the clearance nomination – a process which tacked on additional months.

These measures will also help reinforce the objectives of existing programs, such as technical assistance efforts, or the work of Information Sharing and Analysis Centers (ISACs).[41] If critical infrastructure organizations have put in place stronger cybersecurity measures, their employees should be poised to go through the security clearance process more quickly. As a result, in cases when government has classified information regarding a threat or an incident, government would be in a better position to advise the right senior information security officials in the private sector and critical infrastructure organizations would be in a better position to respond through action or reciprocal provision of information.

In most cases, expediting the clearance process could require an investment in additional personnel, particularly if clearance request volumes also increase. Currently, it costs the Office of Personnel Management an estimated $228 to conduct an investigation for a secret clearance and an estimated $4,005 to conduct an investigation for a top secret clearance.[42] However, because these recommendations are largely administrative actions, implementation should be relatively low-cost. Furthermore, because they do not affect the investigation or adjudication phases, these process improvements should allow the overall security clearance process to be accelerated without compromising national security interests.

Current Status. Treasury's OCIP can and does steer qualified security professionals in the financial industry into a clearance program run by DHS. After identifying a potential candidate, Treasury's OCIP confirms with the primary regulator of that institution that the individual should have a clearance. Treasury OCIP then sends the application request to DHS in what is known as the "pre-submission and coordination" phase of the DHS security clearance process. However, as indicated above, this period – from the time when DHS receives a clearance nomination to when the appropriate DHS official signs off on that nomination and submits it for investigation – often appears to be a major bottleneck. As a result, it can take several months to more than a year for an individual to receive security clearance application materials following this phase, rather than the expedited basis envisioned by the Executive Order and the new DHS plan. Treasury believes there is a need to accelerate this step of the process.

Encouraging Adoption of the Framework. The federal government has an interest in seeing that qualified and appropriate information security personnel at critical infrastructure organizations have an opportunity to apply for a security clearance – a policy priority made clear by the Executive Order and the recent process improvements that were made in response to it.[43]

---

[41] Comment letter from CACI International Inc. (April 29, 2013) (hereinafter "CACI letter"), pp. 1-2, noted the importance of having cleared personnel to information sharing efforts.

[42] These FY 2013 estimates are referenced on page 32 of the Federal Investigative Services Fiscal Year 2012 Annual Stakeholder Report. It can be found at http://www.opm.gov/investigations/background-investigations/reference/annual-report-for-fiscal-year-2012.pdf.

[43] Executive Order 13636, at Sec. 4(d).

Likewise, critical infrastructure stakeholders have expressed strong interest in granting additional personnel access to classified information, so long as receiving a security clearance would not be made contingent upon adoption of the Framework. Personnel at critical infrastructure organizations in certain sectors, such as those in the financial services sector, have previously benefited from expedited security clearances. In addition, critical infrastructure stakeholders in other sectors have noted strong interest in being granted security clearances.[44]

Adoption of the Framework should enhance the value of holding a security clearance because firms that satisfy its requirements will be in a better position to leverage threat information and protect their own systems in a more timely and effective manner. As a result, there will be increasing pressure on the federal government to eliminate bottlenecks and process security clearance applications as quickly as possible. Treasury believes the above measures should further accelerate the process, and because they are administrative actions, would not require additional legislation.[45]

6. Tax Incentives

Improving Cybersecurity. A significant number of stakeholders in a broad range of sectors identified tax incentives as a potential way to improve cybersecurity. If too few economic resources were being devoted to cybersecurity, tax incentives could be used to lower the after-tax costs of investing in this activity. This could help address the market failures that arise from an underinvestment in knowledge and coordination failure concerns that were noted in Part II. Tax incentives can take several forms. For example, one such incentive could be provided by an enhanced tax credit for research into cybersecurity technologies. Investment tax credits and accelerated cost recovery deductions could also be provided for the purchase or development of hardware and software systems that strengthen cybersecurity. [46]

---

[44] "We also see substantial benefits from an increased number of security clearances." Comment letter from the American Public Power Association (April 29, 2013), pp. 2; AGA letter, supra note 13, at 2; CACI letter, supra note 41, at 1-2; Honeywell letter, supra note 13, at 2; Comment letter from the Internet Security Alliance (April 29, 2013) (hereinafter "ISA letter"), Appendix B, pp. 3; LADWP letter, supra note 32, at 2; Monsanto letter, supra note 13, at 3; NRECA letter, supra note 38, at 5; Sempra letter, supra note 29, at 7-8.

[45] The Treasury Department already has the authority under several Executive Orders to sponsor security clearances for private sector firms to access classified information to protect the critical infrastructure. In particular, Executive Order 12968 (Access to Classified Information) (August 2, 1995) sets out the standards for determining eligibility for access to classified information, and Executive Order 13549 ("Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities") (August 18, 2010) specifically addresses access for the "private sector." However, Executive Order 13636 ("Improving Critical Infrastructure Cybersecurity") (February 12, 2013) tasks the Secretary of the Department of Homeland Security (as the Executive Agent for the program under E.O. 13549) to "expedite the processing of security clearances to the appropriate personnel employed by critical infrastructure owners and operators… ." This "expedited" security clearance program is currently the responsibility of DHS and it has recently began implementing the program and has reached out to Treasury as the sector-specific agency for the financial services sector as part of this program.

[46] One stakeholder (see Comment letter from VOXEM, Inc. (April 29, 2013) (hereinafter "Voxem letter"), pp. 1-6) proposed that taxes on capital gains earned from sales of stock of corporations that had achieved compliance with

Advantages and Disadvantages. The effectiveness of tax incentives in promoting cybersecurity would depend upon the ability of the government to define qualifying assets and activities in a way that would truly incentivize appropriate cybersecurity investments. Defining "qualifying expenditures" to avoid being either over-inclusive or under-inclusive could prove difficult. Overly broad definitions of the targeted activity could encourage investments of the wrong type, so that little actual additional cybersecurity would be achieved.[47] On the other hand, overly restrictive definitions could cause truly desirable investments to be ignored or even reduced. Tax incentives may also create economic distortion by favoring a specific type of investment along a dimension that is unrelated to the targeting criteria.[48] Avoiding such distortions may not be feasible in practice because the neutrality of an incentive may depend on the characteristics of individual taxpayers or of specific assets.

Calibrating the level of subsidy is similarly challenging. Credit rates and other tax incentive parameters should be tailored to the size of the externality being addressed, but the size of the externality is rarely ascertainable with precision. Taxpayer responses to incentives are also uncertain. In the network environment of cybersecurity, the failure to gauge the appropriate level of incentives could lead to market distortions, as early adoption of a "wrong" technology could discourage or even eliminate adoption of a better technology. There are also operational considerations. The availability of cybersecurity tax credits might require the involvement of multiple agencies in the promulgation of regulations and possible certification of investment projects. In any case, administering and enforcing cybersecurity tax incentives would require additional Internal Revenue Service (IRS) resources that would have to be provided either through increased funding or a reallocation of existing resources.

Current Status. The IRS may not grant incentives to taxpayers in the absence of authority granted under the Internal Revenue Code. However, various tax incentives are currently available under existing law, although they are not targeted specifically at cybersecurity activities.

For example, businesses may qualify for a tax credit for increasing research on cybersecurity products and methods. However, a major justification for the existence of the research credit is that the ensuing benefits obtained from developing new technologies cannot be captured fully by private parties. As applied to an increased rate of investment tax credit for cybersecurity research, this justification would need to be extended to an argument that cybersecurity knowledge spillovers are especially important. Moreover, the supporting evidence would need to be developed and presented. Investment tax credits are allowed for eligible

---

the Framework be reduced. We do not discuss this incentive here, since the targeting of this incentive to specific cybersecurity activities would be quite difficult and the incentive would entail difficult implementation issues.

[47] For example, identifying eligible property simply as assets "placed in service as part of implementing the Framework" would be too vague.

[48] For example, investment tax credits generally favor assets with shorter economic lives.

outlays on energy assets and other types of eligible property. These credits are intended to incentivize businesses to undertake "marginal" investments in eligible assets that would otherwise be deemed unprofitable.[49] Similarly, enhanced targeted investment tax credits could be devised to incentivize specified types of investments in cybersecurity hardware and software.

The acceleration of cost recovery deductions – by shortening the cost recovery period, by front-loading the deductions within that period, or both – increases the present value of the deductions, and provides an incentive for businesses to invest in depreciable property. In the extreme, investment costs of such property could be deducted fully (i.e., "expensed"). Expensing of outlays for certain tangible assets and for purchased computer software is currently available to small businesses, and is available to all businesses for costs associated with the development of most intangible property (patents, internal-use computer software, customer lists, brand recognition, etc.). Similarly, taxpayers may expense research and experimental expenditures. Firms that are engaged in increasing their level of cybersecurity may be able to take advantage of these incentives. In addition, it would be possible to accelerate further cost recovery deductions for "qualified" depreciable cybersecurity assets through new legislation.

Encouraging Adoption of the Framework. Several stakeholders in a broad range of sectors identified tax incentives as a potential inducement for adoption of the Framework.[50] Tax incentives could have a significant effect if there were many projects or investment opportunities that were on the cusp of profitability – and a tax credit would assure a positive return. Alternatively, they would have a negligible effect if there were only a few projects that would become profitable as a result of the incentives. Ultimately, adoption of a tax incentive would come at the expense of foregone revenue for the government or reallocation of existing fiscal obligations. Accordingly, the impact of a tax incentive should be carefully considered before adopted. Under the current circumstances, further consideration of tax incentives appears not to be warranted.

7. Cyber Insurance

Improving Cybersecurity. Insurance is a risk transfer product, where an institution obtains an insurance policy to cover a pre-identified risk and the risk of loss is shifted to the insurer in

[49] Such incentives also subsidize "infra-marginal" investments, or those that would have been undertaken regardless of the evidence of the investment credit. Attempts to minimize this effect have not been highly successful. For example, the research credit is calculated on qualified expenditures that are in excess of a base amount, which is determined by the amount of research spending (relative to gross receipts) that a taxpayer undertook within a five-year historical period. This base amount is an overly crude estimate of the taxpayer's research expenditure in the absence of the credit.

[50] U.S. Chamber letter, supra note 21, at 5; Comment letter from Encryptics (April 29, 2013) (hereinafter "Encryptics letter"), pp. 2; FSSCC letter, supra note 11, at 4; ISA letter, supra note 44,at 16, 28; NCTA letter, supra note 13, at 4, 12-13; Sempra letter, supra note 29, at 4-6, 8; U.S. Telecom letter, supra note 11, at 7; TIA letter, supra note 11, at 13; Voxem letter, supra note 46, at 1-6.

exchange for a premium. Cyber insurance is an emerging line of insurance that has garnered attention from critical infrastructure stakeholders as a potential tool to strengthen cybersecurity.[51] Some suggest that the federal government support the cyber insurance market by creating a cyber insurance or reinsurance program.[52]

However, views among critical infrastructure stakeholders are mixed as to whether the government should play a role in the cyber insurance market.[53] Several stakeholders suggested that cyber insurance should remain a private market incentive to improve cybersecurity.

Cyber insurance can promote adoption of stronger security measures. Insurers typically worry about moral hazard, namely the concern that policyholders might be encouraged to take undue risks, knowing that the risk of loss has been transferred to the insurer. Consequently, insurers could require policyholders to comply with minimum security standards as a condition of insurance coverage, including adoption of the Framework. Insurers also may encourage policyholders to implement even stronger cyber protections by offering premium discounts to those who make additional security investments that reduce risks of loss to events covered by cyber insurance.

Insurers also have significant concerns about adverse selection and have strong financial incentives to make sure policyholders take effective precautions to mitigate losses. In instances in which the government can disclose emerging cyber threats to insurers, those insurers should educate policyholders and incentivize specific cybersecurity measures that mitigate such risks. An insurer might also implement loss mitigation procedures on behalf of an insured in the immediate aftermath of a cyber-attack.

The growth of the private cyber insurance market could lead to a better understanding of cyber threat patterns and improved information sharing between the government and insured firms. Because insurers need credible data to appropriately underwrite and price policies, insurance creates incentives for standardized data collection and reporting.

Advantages and Disadvantages. Cyber insurance can provide an indirect, private market incentive. It is important to recognize that an insurer's primary obligation is to mitigate risk of financial losses, not to defend against cyber threats. However, insurers could be well positioned to encourage higher levels of cybersecurity; for example, insurers can help establish minimum cybersecurity standards, monitor market threats, and play an important compliance role.

---

[51] BAH letter, supra note 11, at 8.

[52] LADWP letter, supra note 32, at 2; NRECA letter, supra note 38, at 6; also, several stakeholders (see, comment letter from Marsh Inc. (April 29, 2013) (hereinafter "Marsh letter"), pp. 2; NRECA letter, supra note 38, at 6) have asked the federal government to clarify whether cyber incidents are covered by the Terrorism Risk Insurance Act of 2002. This question is beyond the scope of the focus on cyber insurance as an incentive for enhanced cybersecurity.

[53] Encryptics letter, supra note 50, at 2; Honeywell letter, supra note 13, at 3; TIA letter, supra note 11, at 25.

As an incentive, cyber insurance could also be responsive to a rapidly changing environment. Because carriers compete on how effectively insurance products are priced and underwritten, they are likely motivated to ensure the minimum security standards that they establish do not become obsolete.

Current status. Some cyber insurance experts note that the market "has remained small for many years, and has repeatedly fallen short of optimistic growth projections."[54] Indeed, the premium volume for the U.S. cyber insurance market is difficult to gauge, but some private estimates put annual gross written premiums in the $1 billion range[55] – a tiny fraction of the $247 billion of direct premiums written for the total U.S. commercial lines insurance market in 2012.[56]

When risks are considered "uninsurable" in the private market, policymakers may consider whether the federal government should intervene to replace or stabilize the private market. One example of action by the federal government in this area is the National Flood Insurance Program, which was established in part in response to a perceived failure of the private market to insure adequately against flood risk.

So far, however, it appears that cyber insurance is a growing market, albeit still a nascent one. Insurers report that many private firms are unaware of their cyber risk exposures, suggesting there may be substantial room for increased take-up and coverage growth. More insurers are entering the cyber insurance market and are competing to gain market share.[57] Indeed, one stakeholder representing the interests of major property and casualty insurers noted in its comment letter that "there is a market for cyber liability coverage and we need to allow the market to work."[58]

Encouraging Adoption of the Framework. Insurers could create an incentive for adoption of the Framework by tying eligibility or premiums to adoption of the cybersecurity Framework. This would be a private sector incentive, rather than a government-sponsored incentive.

---

[54] Moore, Tyler Introducing the Economics of Cybersecurity: Principles and Policy Options, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy (2010), available at http://cs.brown.edu/courses/csci1800/sources/lec27/Moore.pdf

[55] The Betterley Report, "Cyber/Privacy Insurance Market Survey." (June 2012).

[56] The market for third-party cyber insurance is developing quickly because losses that a firm causes to its customers, such as from a data breach, are relatively predictable. Conversely, the market for first-party cyber insurance is less developed, as direct cyber losses to firms arising from business interruption and destruction of data and intellectual property are more volatile and not as well understood.

[57] The Betterley Report, "Cyber/Privacy Insurance Market Survey" (June 2012).

[58] Comment letter from the American Insurance Association (April 29, 2013), pp. 1.

Insurers might also choose to require adoption of the Framework as a condition of eligibility for coverage.[59] Alternatively, insurers might choose to reward policyholders who adopt the Framework, such as offering lower premiums or offering more heavily discounted premiums for policyholders with robust security practices. In this respect, the growth of the cyber insurance market may drive the adoption of the Framework as policyholders seek to comply with its requirements. A cybersecurity Framework that establishes consistent standards and best practices could improve the ability of insurers to price and underwrite cybersecurity insurance. That, in turn, should enable those insurers to take on greater volumes of cybersecurity risk and grow the market for cyber insurance. In either case, significant input and collaboration with the insurance sector could play a critical role in the development of a more robust Framework.

[59] Marsh letter, supra note 52, at 2.