Information Technology Sector Coordinating Council (IT SCC) Response

March 28, 2013 Notice of Inquiry

of the

U.S. Department of Commerce,
National Telecommunications & Information Administration

About the Information Technology Sector Coordinating Council (IT SCC):
The Information Technology Sector Coordinating Council (IT SCC) was established on January 27, 2006 and currently has 95 member companies. The purposes of the IT SCC is to bring together companies, associations, and other key IT sector participants on a regular basis to coordinate strategic activities and communicate broad sector member views associated with infrastructure protection, response and recovery that are broadly relevant to the IT Sector. The IT sector envisions a secure, resilient, and protected global information infrastructure that can rapidly restore services if affected by an emergency or crisis, ensuring the continued and efficient function of information technologies, infrastructures and services for people, governments, and businesses worldwide.

Prefatory Note:
For the purpose of responding to the Department of Commerce Notice of Inquiry on the use of incentives pursuant to the President's Executive Order on cyber security the IT SCC takes the perspective that incentives can be applied across sectors to entities regardless of the regulatory environment the reside in or their possible classification as critical or most critical infrastructures.

* * * * *

1. Are existing incentives adequate to address the current risk environment for your sector/company?

A. Which Risks in the Current Risk Environment Do the Executive Order and This Question Seek to Address?

Within the current risk environment, there are many types of cyber risks. It is unclear, however, which cyber risks the Presidential Executive Order or this question seeks to

address. While the Executive Order focuses on the risk of regional or national catastrophic events, those tasked with implementing the Order have talked about the creation of a Framework designed to prevent what is perhaps the primary issue that CIOs deal with every day: the theft of intellectual property, personal data, and business process. Because these risks differ in terms of their probability of occurrence, the techniques required to mitigate against such risks, and the associated costs or incentives to deploy them, clarification is needed.

For example, with respect to the attacks referenced in the Executive Order that would result in a national or regional catastrophe, such attacks would essentially be acts of war that could only be deployed once (or a few times in quick succession). Because of the sophistication required to successfully carry out these attacks and to overcome system resiliencies, the perpetrators would most likely be nation-states or those working on behalf of nation-states. A recent Intelligence Community Threat Assessment described the probability of these types of attacks, however, as "remote," not because they were technologically infeasible, but because there was little incentive to conduct them.[1] Feasibility and incentives aside, another reason that such an event is remote is due to the success of currently available defenses, including system resiliencies. Despite daily attacks, there has never been a single instance where an attack has resulted in such a catastrophe.

The far more common threat, and the threat that some Administration officials have mentioned in relation to Framework development, is the threat of intellectual property, personal data, and business process theft. Success for this type of attack does not occur with penetration (or "breach") and disruption/destruction as in the case of catastrophic attacks, but rather with breach, data location, and then data exfiltration from the network or system to another website or URL.

B. The Adequacy of Incentives and Incentivization is Dependent on the Risk to be Mitigated

As an initial matter, the Information Technology sector is a sector with a wide-ranging diversity of companies and businesses. There are companies within it that are both large and small, with different business plans and business strategies. However, there is one constant: each information technology company is a legal construct that has been established with the purpose of returning a profit for its investors. Indeed, that is each company's legal mandate, codified in statute and case law.[2] Within this construct,

---

[1] Clapper, James R. Statement to the House Permanent Select Committee on Intelligence. "Worldwide Threat Assessment of the U.S. Intelligence Community." Hearing. April 11, 2013. Web. <http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20WWTA%20US%20IC%20SFR%20%20HPSCI%2011%20Apr%202013.pdf>.

[2] Dodge v. Ford Motor Co., 170 N.W. 668 (Mich.1919); Carlton Investments v. TLC Beatrice International Holding, Inc., 1997 Del. Ch. LEXIS 86, 45 (ct. of Chancery, New Castle May 30, 1997).

companies will invest in cyber security to a level that is justifiable according to their own business plans. In making this determination, companies not only assess their own economic circumstances vis-à-vis the costs of security, but also their own risk profile, including the risks they face, the value of their assets (e.g., their intellectual property), as well as the probability of a risk's realization.

That said, companies already have strong incentives for continuous improvements in the security including incentives for continuity of operation, incentives to continue to improve their productive capacity, incentives to gain a competitive advantage in the market, incentives to maintain the trust of their customers, and incentives to preserve their company's reputation and brand – all of which are powerful economic incentives for continued improvement in adopting voluntary cybersecurity best practices. In one survey, seventy-six percent of companies say making cybersecurity a priority increases their efficiency and gives them a competitive advantage in the market.[3] Their systems are down less often, they're not losing customers due to lack of trust, and their brand is not threatened.

To address the risks that companies perceive as probable and consequential, private sector spending on cyber security has doubled in the past five years from $40 billion to $80 billion a year.[4] By contrast, the Department of Homeland Security, which is tasked with defending the United States homeland on the ground and in cyber space, only received a mere $59 billion in 2012 for the entirety of its programs.[5]

In order to defend against the national or regional catastrophic attacks described in the Executive Order, however, private sector critical infrastructure spending would have to increase by 9-fold or 900%.[6] Such a spending increase is not sustainable. To guard against a threat like that, which has been labeled "remote," the government would have to provide incentives so that companies can move beyond what is business justifiable to that of a national security level. Indeed, it is the Federal Government's duty, as expressed in the Constitution, to provide for the common defense.[7] Energy generation plants are not expected to arm themselves with anti-ballistic missile systems to guard against a kinetic attack of that level, and, thus they should not be expected to arm themselves at their own cost for a cyber equivalent.

---

[3] Savage, Marcia. "Cybersecurity boosts bottom line." SC Magazine. 13 Feb. 2005. Web. <http://www.scmagazineus.com/cybersecurity-boosts-bottom-line/article/31735/>.

[4] Ponemon, Larry. Ponemon Institute IT Security Tracking Study Estimates. Feb. 2012.

[5] U.S. Department of Homeland Security. "Department of Homeland Security Budget in Brief: FY 2012. Oct. 2011." 6 Feb. 2012. Web. <http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf>.

[6] Domenici, Helen, and Afzal Bari. "The Price of Cybersecurity: Improvements Drive Steep Cost Curve." Ponemon Institute-Bloomberg Government Study, 31 Jan. 2012.

[7] "The Constitution of the United States," Preamble.

C. Enhancing Cyber Security: Incentives Required

We agree with the premise of the NOI that the best way to promote voluntary adoption of the Framework is through incentives. This is because the cyber security equation favors the attackers. Cyber attacks have become easy as well as cheap (which also can be out-sourced inexpensively through the Internet). In addition, attacks can be extremely profitable, with the estimates of annual theft ranging in the multi-billions to $1 trillion.[8],[9] Moreover, the chances of getting caught are slim, with estimates indicating that less than two percent of cyber criminals are successfully prosecuted.[10]

By contrast, cyber defense has numerous economic disincentives, with the defenders usually lagging a generation behind the attackers. Further, the perimeter to be defended is virtually limitless. Return on investment, a critical calculus in the private sector where firms are obligated to be profitable, is difficult to demonstrate. Even with a return on investment success requires preventing something from happening, which is almost impossible to measure. In addition, a recent study shows that nearly half of private sector entities have been forced to either defer or reduce their investment in cyber security, mostly for economic reasons.[11]

As long as the economic equation for cyber security remains unbalanced, incentives are key to generating ongoing improvements in cyber security behavior.

D. Appropriate "Adequacy" Metrics within the Current Risk Environment.

Although not a question in the scope of this NOI, we would like to point out that currently we lack understanding about what constitutes "adequate security." In some cases there is an assumption that a penetration, or breach of a cyber system demonstrates inadequate security and negligence. However, many factors contribute to adequate security, and we suggest the Administration consider, a subsequent NOI that explores this complex issue more fully.

---

[8] Ruppersberger, C.A. "Dutch." Statement. House Permanent Select Committee on Intelligence. "Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE," Hearing. 13 Sept 2012. Web. <http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/09122012DutchOpening.pdf >.

[9] Executive Office of the President. "Cyberspace Policy Review." 2009. Web. <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

[10] Regoli, Robert M., and John D. Hewitt, *Exploring Criminal Justice: The Essentials* (Sudbury, MA: Jones and Bartlett Publishers, 2010), 378.

[11] PricewaterhouseCoopers. "The Global State of Information Security." Rep. 2013.

2. Do particular business sectors or company types lack sufficient incentives to make cybersecurity investments more than others? If so, why?

A. Addressing the Problem: Incentives Are Needed to Address Economic Imbalances.

Placed in a historical context, our modern cyber systems are a marvel. These systems are not yielding to attackers because they are bad systems; they are, in fact, quite resilient. Rather, as discussed, the cyber security problem exists because the incentives calculus favors attackers over organizational defenders. Attackers do not have to make significant investments to successfully execute attacks, and often reap significant financial or other value for the relatively low investment, which is further complicated by a low risk of being caught. On the other hand, defenders make considerable investments in security, but the positive security benefit gained is difficult to measure or to directly correlate to the investments. Accordingly, in order to successfully advance cyber security, the Government must address this economic imbalance. Indeed, in this rapidly changing environment, incentives to undertake the most effectively tailored measures, is what is required in order to secure our cyber systems.

B. The Defense Industrial Base Example: Powerful Incentives for Security Equal Greater Security.

In terms of cyber security, the Defense Industrial Base is among the elite. For DIB companies, cyber security is not an "add-on"; for them, it is at the core of their business and it is a component for which they are economically compensated. Because the level of security is tied to the incentives to be secure, other sectors should likewise receive incentives for enhanced and greater security.

3. How do businesses/your business assess the costs and benefits of enhancing their cybersecurity?

A. The Private Sector Assesses Security Primarily in Economic Terms, As Is Mandated by Law

Most critical industry companies are publically traded organizations. In the United States, these companies operate under the legal obligation to maximize shareholder value.[12] As a result, companies assess the costs and benefits of all security investments on a risk-management basis, balancing the costs of security against the economic costs of security enhancements. In sum, they make an economic ("monetary") calculation to determine if security expenditure is business justifiable. A good example of this

[12] Dodge v. Ford Motor Co., 170 N.W. 668 (Mich.1919); Carlton Investments v. TLC Beatrice International Holding, Inc., 1997 Del. Ch. LEXIS 86, 45 (ct. of Chancery, New Castle May 30, 1997).

approach is found in the retail industry: it is well known, that if, every month, a retailer experiences the theft of inventory equal to approximately 10% of that month's revenues, the retailer will not hire guards and install cameras to prevent the theft if such expenditures exceed 10% of monthly revenues.

Nonetheless, a straight up economic calculation can often lead to critical investments in security. For example, companies have strong incentives to invest in security for continuity of operation, incentives to continue to improve their productive capacity, incentives to gain a competitive advantage in the market, incentives to maintain the trust of their customers, incentives to protect their intellectual property, and incentives to preserve their company's reputation and brand – all of which are powerful economic incentives for continued improvement in investing in and adopting voluntary cybersecurity best practices.

B. The U.S. Government Assesses Security on an "Economic +" Basis Based on Its Constitutional Mandate to Provide for the "Common Defense" of the United States.

By contrast, the U.S. Government assesses the costs and benefits of security on a slightly different basis, which often leads to very different results. Under the U.S. Constitution, the U.S. Government is tasked with providing for the "common defense."[13] So, while the U.S. Government can and will consider the economic costs and benefits of security, it will also consider other criteria when making a decision, namely, national security, civil liberties, etc.

C. Because the U.S. Government and Industry Assess Risk in Aligned, But Not Identical, Approaches, Their Analysis of Catastrophic Cyber Risk Differs.

The cyber systems we are considering in this NOI are a shared network of networks. While this sharing of networks means that government and industry face the same or similar cyber risks, it is important to appreciate that the basis upon which they each analyze these shared risks is aligned, but not identical. As discussed above, industry assesses risk on an economic basis, while the U.S. Government assesses risk on an "economic +" basis. Appreciating this difference becomes especially important in the context of the catastrophic cyber events described in the President's Executive Order and by Administration officials. Private companies generally do not assess costs and benefits against the prospect of nation-state attacks.

[13] "The Constitution of the United States," Preamble.

4. What are the best ways to encourage businesses to make investments in cybersecurity that are appropriate for the risks that they face?

A. Since Private Sector Cyber Investments Are Made At the Corporate Level, And Not a National or Sector Level, A Single National Standard or Sector Standard May Be Inadequate.

As discussed, the best way to encourage a business to make investments in cyber security is to make these investments economically beneficial to that particular business. Even within industry sectors, different businesses have different systems, cultures, partnerships and business plans. As a result, cyber investment decisions are made on a company-by-company basis (sometimes such decisions are even made on a division-by-division basis or less); not on a national or sector basis.

B. We Should Provide Incentives Tied to a Range of Globally Determined Standards and Practices That Have Been Proven Effective And That Have Been Selected By Companies to Meet Their Business/Security Needs.

The U.S. Government should provide incentives to companies that voluntary adopt any of a variety of the globally developed standards and practices, so long as those adopted standards and practices have been empirically proven to be effective.

As stated in the civil liberties and multi-trade association white paper, "Improving Our Nation's Cybersecurity through the Public-Private Partnership":

> "Many cybersecurity standards have been and are continually being established and updated through the transparent consensus processes of standards development organizations (SDO). Many of these processes are international in design and scope, and they routinely include active engagement by multinational corporations and various government entities that participate as developers or users of the technology. The multitude of continually evolving standards is essential because of the widely disparate configurations that are in use, and these configurations are constantly evolving and being updated to support rapid innovation in a dynamic industry. Both industry and government organizations voluntarily adopt the resulting best practices and standards that best fit their unique requirements, based on their roles, business plans, and cultural or regulatory environments. This historic process of standards development is widely embraced is, highly participatory, and maintains high credibility in the global community…."[14]

[14] Internet Security Alliance, Business Software Alliance, TechAmerica, U.S. Chamber of Commerce, and Center for Democracy and Technology. "Improving Our Nation's Cybersecurity through the Public-Private Partnership." White Paper. March 2011. Web. <http://isalliance.org/publications/2C.%20Industry-Civil%20Liberties%20Community%20Cybersecurity%20White%20Paper%20-

6. Are there public policies or private sector initiatives in the United States or other countries that have successfully increased incentives to make security investments or other investments that can be applied to security?

We have not had an opportunity to fully assess how other nations are using cyber security incentives, nor have we had a chance to directly engage with the various critical infrastructure sectors to gauge the successfulness of various policy initiatives in each of their sectors. It is for these reasons that we believe the industry leaders themselves are best suited to advise on the policies and practices that work best within their sectors. But we believe there are likely to be various examples and opportunities throughout each critical infrastructure sector for enabling investment in the kinds of innovation and innovative technologies that can further improve security. They involve specific liability protection, tax incentives, direct financial incentives, low interest loans, and regulatory relief.

7. Are there disincentives or barriers that inhibit cybersecurity investments by firms? Are there specific investment challenges encountered by small businesses and/or multinational companies, respectively? If so, what are the disincentives, barriers or challenges and what should be done to eliminate them?

Cybersecurity investments have been significant over the last 5 years. According to a recent Ponemon study, private sector spending by U.S. companies on cyber security has in fact doubled in the last 5 years to approximately $80 billion dollars for 2011.[15]

For small businesses, general education and awareness are primary barriers. That is one of the reasons the Federal Communications Commission launched its Small Biz Cyber planner together with leading industry leaders.[16]

Another barrier to cybersecurity investment is the lack of timely, actionable intelligence provided to industry on existing and emerging threats. We are pleased that the EO seeks to improve the Government's provision of timely and actionable cyber threat information to the private sector.

%20Improving%20our%20Nation's%20Cybersecurity%20through%20the%20Public-Private%20Partnership%20-%203-2011.pdf>.

[15] Ponemon, Larry. Ponemon Institute IT Security Tracking Study Estimates. Feb. 2012.

[16] In October 2012, the FCC re-launched the Small Biz Cyber Planner 2.0, an online resource to help small businesses create customized cybersecurity plans. The effort was initially launched with HP, McAfee, Symantec, Thomson Reuters, US Chamber of Commerce, National Urban League & SCORE. http://www.fcc.gov/cyberforsmallbiz

8. Are incentives different for small businesses? If so, how?

Small businesses working within the critical infrastructure and key resources sectors are also disadvantaged by incentive misalignments (see responses to Questions 1, 3, and 4 for a more detailed discussion on incentive misalignments). With more pronounced concentrations of intellectual property than that of larger businesses, small businesses have become an even more attractive target for attacks and exploitation. In addition, many leading technical advances are generated within small businesses. Collectively, these considerations suggest that the "ripeness" of small business as a cyber attack target is especially pronounced. Combined with potentially immature cyber practices and insufficient cyber security investments, cyber attacks against small businesses within the critical infrastructure and key resources segments can yield significant rewards.

Indeed, in its recently released "Internet Security Threat Report: 2013," Symantec described how targeted attacks against small businesses (that is businesses with between 1 to 250 employees) accounted for 31% of all targeted attacks in 2012, compared with 18% in 2011. This was a threefold increase. As Symantec noted:

> "While small businesses may assume that they have nothing a targeted attacker would want to steal, they forget that they retain customer information, create intellectual property, and keep money in the bank. White it can be argued that the rewards of attacking a small business are less than what can be gained from a large enterprise, this is more than compensated by the fact that many small companies are typically less careful in their cyber defenses."[17]

In order to effectively incentivize small businesses to voluntarily adopt the Framework, special consideration should be given to tiered levels of incentives that would be sufficient to provide meaningful assistance to small businesses to motivate them to voluntarily adopt and adhere to the Framework.

9. For American businesses that are already subject to cybersecurity requirements, what is the cost of compliance and is it burdensome relative to other costs of doing business?

Over the past few years, the Ponemon Institute has conducted a number of surveys to track private sector spending related to cyber security, including spending on computer

[17] Symantec. "Internet Security Threat Report: 2013." 16 April 2013. Web. <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf>.

security technologies, such as firewalls, intrusion detection systems, etc.; governance and control activities, such as traffic monitoring, compliance, and training; security management outsourcing; and securing industrial control systems.[18] The results are noteworthy. Over a five year period, private sector annual spending on cybersecurity has increased by 100% from $40 billion to approximately $80 billion in 2011.[19] By contrast, the official spending request for the entire Department of Homeland Security during that same time frame, for calendar year 2012, was only $57 billion.[20] This was the complete requested budget, inclusive of FEMA, TSA, ICE, etc.

In terms of compliance cost, one example of where the cybersecurity-related regulatory cost has been overly burdensome is related to the DHS implementation of the Chemical Facility Anti-Terrorism Standard (CFATS). Specifically, the cybersecurity components of the CFATS audit regime and process are overly repetitive and redundant across an impacted business, and the oversight process is manpower intensive. Rather than conduct one site visit at an impacted business's headquarters where much of the information resides, auditors have tended to go to each facility wherein they request the same or similar information. More effectively partnering with industry in the development of any regulatory regime would enable a more efficient and effective audit process for both industry and government stakeholders.

10. What are the merits of providing legal safe-harbors to individuals and commercial entities that participate in the DHS Program? By contrast, what would be the merits or implications of incentives that hold entities accountable for failure to exercise reasonable care that results in a loss due to inadequate security measures?

In some instances, liability protections can be beneficial. For example, providing safe harbor to those companies that share attack information in good faith as part of an information-sharing program could help remove the litigation concerns that might prevent companies from otherwise sharing information. However, liability protections should be accompanied by incentives, such as, such as regulatory forbearance, streamlined permitting, preferential treatments, and tax and grant benefits.

With respect to the "reasonable care" portion of the above question, it seems to indicate that (1) those that adopt the Framework and enroll in the incentives programs would be exercising due care while those that do not adopt the Framework would not be exercising due care and (2) those that experience loss from an attack are *per se*

[18] Domenici, Helen, and Afzal Bari. "The Price of Cybersecurity: Improvements Drive Steep Cost Curve." Ponemon Institute-Bloomberg Government Study, 31 Jan. 2012.

[19] Ponemon, Larry. Ponemon Institute IT Security Tracking Study Estimates. Feb. 2012.

[20] U.S. Department of Homeland Security. "Department of Homeland Security Budget in Brief: FY 2012. Oct. 2011." 6 Feb. 2012. Web. <http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf>.

negligent. Both assumptions are flawed.

As an initial matter, as discussed above, if a company is successfully attacked, that does not mean that it was negligent. In today's attack environment, highly sophisticated attackers are eventually going to be able to break into a system. If successful penetration and loss was the standard for negligence, then the U.S. Government, despite its adherence to the FISMA "Framework" of laws, would be negligent for the repeated attacks and losses that is has suffered over the years.

Regarding the notion that Framework adoption equals reasonable care, it rests on the unproven and unfounded assumption that adopting the Framework would somehow prevent attack and loss. However, we know that it would not be adequate to prevent today's more sophisticated attacks. Moreover, the notion that those organizations or companies that choose not to adopt the Framework are not exercising reasonable care is misplaced. Indeed, companies that have successfully fought off or mitigated today's sophisticated attacks might opt to keep their own measures in place rather than the Framework's precisely because these measures offer a greater level of cyber security.

11. What would be the impact of requiring entities to join the DHS Program prior to receiving government financial guarantees or assistance in relevant sectors? How can liability structures and insurance, respectively, be used as incentives? What other market tools are available to encourage cyber security best practices?

As discussed above, there are a number of market and economic tools for encouraging cyber security best practices – from the inherent market incentive for companies to maintain customer trust, and invest in the tools that will ensure continuity of service, to the policy enabled market tools that include direct investment, liability protection, regulatory relief, etc.

But assessing the "impact of requiring entities to join the DHS Program prior to receiving government financial guarantees or assistance in relevant sectors" is difficult to assess without knowing whether the DHS program itself will be structured in a way that will include the right incentives for fostering investment, harnessing innovation, and enabling the kind of flexibility across sectors.

12. Should efforts be taken to better promote and/or support the adoption of the Framework or specific standards, practices, and guidelines beyond the DHS Program? If so, what efforts would be effective?

This question seems to similarly rely on the assumption that a published Framework and correlated DHS program or another set of standards would alone prove adequate in defending critical infrastructure against the most sophisticated types of threats. Again,

this assumption is not supported by what we know of sophisticated threats, such as APT. We urge the Administration to ensure that any Framework of standards and best practices remains voluntary, and think incentives could help increase adoption of a voluntary framework.

13. In what way should these standards, practices, and guidelines be promoted to small businesses and multinationals, respectively, and through what mechanisms? How can they be promoted and adapted for multinational companies in various jurisdictions?

As discussed above, the U.S. Government will have to provide a menu of market incentives that would be attractive to each individual company at the business plan level and which would then motivate each company to invest in cyber security beyond what is currently business justifiable in the absence of such incentives (see responses to Questions 1, 3, 4, 6, and 9 for more complete discussions).

Moreover, rather than adapting standards to multi-national companies, the Administration should embrace international standards that multi-national companies are already embracing. As the Administration outlined in the policy priorities contained in the Administration's "International Strategy for Cyberspace,"

> *"International cybersecurity standardization, and its voluntary and consensus-based processes, serves collective interests. They foster innovation; facilitate interoperability, security, and resiliency; improve trust in online transactions; and spur competition in global markets."*

That is one of the reason the Administration concluded that we need strategies that encourage technological innovation and don't create new barriers to international trade.[21] As a party of this cyber security strategy, the Administration indicated, "The United States will work to sustain that free-trade environment, particularly in support of the high-tech sector, to ensure future innovation." The Administration also found that "Developing international, voluntary, consensus-based cybersecurity standards and deploying products, processes, and services based upon such standards are the basis of an interoperable, secure and resilient global infrastructure."

[21] Executive Office of the President. "International Strategy for Cyberspace." 1 May 2011. Web. <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.