Internet Security Alliance

Response to

NTIA March 16th 2015 RFC:

"Stakeholder Engagement on Cybersecurity in the Digital Ecosystem"

EXECUTIVE SUMMARY

Numerous studies from PWC/CIO Magazine, CSIS MacAfee have found that the primary issues preventing a sustainably secure cyber system are a combination of cost and complexity. The President's own signature policy paper on cyber security, the "Cyber Space Policy Review" confirmed this conclusion when it held that "many technical and network management solutions that would greatly enhance security already exist in the marketplace but are not always used because of cost and complexity."[1]

The actual data that the market has generated from recent cyber breaches provides stark examples as to the complexity of the economic forces surrounding digital security and how easy it is for policy makers to make incorrect assumptions about these complex forces.

For example there were wide-spread predictions of doom including damage to shareholders for companies like Target and Sony in the wake of their high profile breaches. However, contrary to the predictions of many policy makers (and some in the media), the reality is that the stock price for both Sony and Target rose more than 20% following their breaches. A recent analysis in the Harvard Business Review[2] indicates these are not anomalous effects and a more extensive study by Nir Kossovsky in 2012[3] confirms this general finding with respect to stock price and corporate reputation effects.

This does not mean that cyber breaches are good for stock prices or share-holders, however it does illustrate that our assumptions about prioritization, cost-effectiveness, and incentives for promoting cyber security need to be tested. Future policies need to be based, as best as possible, on real data, not unfounded, even if logically sounding, assumptions.

We are now nearly two and a half years past the President's EO initiating his major policy effort on cybersecurity, and nearly a year and a half since the NIST Framework was finalized. Yet there has been virtually no work done to generate real data on the elements of the President's Order which would tell us about its cost-effectiveness or to guide future policy development on incentives. This contrasts unfavorably with DHS' efforts on their major information sharing initiatives termed STIX and TAXII both of which received extensive pilot testing before full implementation.

Commerce, acting through NTIA, has a golden opportunity to fill this gap and we urge them take it. Conceptual support for the more extended analysis and development of economics of cyber security including the complicated economic differences between the public and private sector (although admittedly not the degree of tactical detail we provide below) can be found in The President's Cyber Space Policy Review, Commerce's own "Green paper" on cybersecurity, the most recent version of the National Infrastructure Protection Plan, The President's 2013 Executive Order on cybersecurity, the House GOP Task Force Report on cybersecurity and white papers endorsed by the US Chamber of Commerce, Tech America, the Business Software Alliance, The Center for Democracy and Technology and, of course, ISA. If NTIA is looking for an initiative with broad stakeholder support, it's hard to find a concept that matches this proposal.

---

[1] "Cyberspace Policy Review; Assuring a Trusted and Resilient Information and Communications Infrastructure." Review. (n.d.): n. pag. *Whitehouse.gov*. Executive Office of the President, 2009.

[2] Upton, David. "The Flaws in Obama's Cybersecurity Initiative." *Harvard Business Review*. N.p., 20 Jan. 2015. Web. 2015.

[3] Kossovsky, Nir. "How to Manage Reputation Risk." *RMmagazine.com*. Risk Management Magazine, 2012. Web. 2015.

1. What security challenges could be best addressed by bringing together the relevant participants in an open, neutral forum to explore coordinated, voluntary action through principles, practices, and guidelines?

President Obama's, 2013 Executive Order (13636) on cyber security set a visionary and pragmatic course for national cyber security policy by eschewing the traditional regulatory model for one that focused on industry-government collaboration to promote the voluntary adoption of identified effective practices and standards. The President's Order was consistent with the published recommendations of multiple stakeholders including ISA, The US Chamber of Commerce, Tech America, the Business Software Alliance and the Center for Democracy and Technology [4][5][6] as well as the House GOP Task Force on Cyber Security[7] all of which had advocated a version of a modern "social contract" between industry and government in pursuit of sustainable system of cyber security.

The Social Contract model advocated by the broad stakeholders cited above, recognizes that it is not enough to identify effective standards and practices but that to achieve the implementation required to actually improve security on a voluntary basis the economic issues associated with improved security must be also addressed. The National Infrastructure Protection Plan (2013) highlights the complexity of the differing economic perspectives government and industry face in achieving their mutual goals.

The Department of Commerce Green paper articulates this challenge quite clearly:

> "Even the most effective means for cybersecurity are useless if entities do not adopt them. It is necessary to develop measures rapidly to better protect the Internet, but to date many solutions have failed to provide sufficient incentives for firms to ingrain cybersecurity best practices into their operations. …The challenge in cybersecurity is not that best practices need to be developed, but instead lies in communicating those best practices, demonstrating the value of implementing them, and encouraging individuals and organizations to adopt them."[8]

The President's 2013 Order specifically instructs Commerce and DHS to go beyond the mere identification of appropriate standards and practices (accomplished by NIST in creating their cyber security framework) by requiring that the Framework be prioritized, cost-effective and supported by a set off incentives.

> "The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall 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."[9]

In a recent article, Fellow for Internet Governance and Cybersecurity at Columbia University Benjamin Dean highlighted that the actual numbers related to cyber breach events tell a different story than is expected. For example, due to the convoluted economics of cyber security, the net cost of the data breach incident actually equaled about .1% of sales for the year. Similar findings were true for other breaches including Home Depot and Sony – who only lost about $15 million to their high-profile breach and who doesn't expect to suffer any long-term

---

[4] Internet Security Alliance. "*Improving our Nation's Cybersecurity through the Public-Private Partnership*". Rep. Internet Security Alliance, 2011.
[5] Internet Security Alliance. *"Cybersecurity Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress*". Rep. Internet Security Alliance, 2008.
[6] Internet Security Alliance. *"Social Contract 2.0: A 21st Century program for Effective Cybersecurity"*. Rep. Internet Security Alliance, 2009.
[7] Recommendations of the House Republican Cybersecurity Task Force". Rep. US House of Representatives, 2009.
[8] Commerc, The Department Of. *CYBERSECURITY, INNOVATION AND THE INTERNET ECONOMY* (n.d.): n. pag. *NIST.gov*. US Department of Commerce, 2011. Web.
[9] EO 13636; Section 7(b)

consequences. As a result, these companies are able to invest less in information security because in the event of a breach, other parties (banks, customers, etc.) bear the lion's share of the costs of the breach.

> "This is a huge problem because as we plough billions of dollars into intelligence agencies, supposedly to keep us all safe from 'cyber-attacks', it has the effect of further weakening the already low incentives for companies to invest in information security themselves…. This does not mean organizations should do nothing at all – but does highlight the need for verifiable and reliable data on which to begin making these complex policy decisions."[10]

We are currently operating without this necessary data.

While the Commerce Department, through NIST, did an admirable job in creating the Framework the crucial economic issues (prioritization, cost-effectiveness, incentives) required under the President's Order as well as being required for long term effectiveness have not been adequately addressed.

Fulfilling this essential element of the vision in the President's Executive Order is precisely the challenge that the multi stakeholder process NTIA is proposing ought to undertake.

We believe that by a following the process laid out below, which is a version of the process NIST utilized creating the Framework itself, substantial progress can be made in a comparatively short time and the effects of this process will far exceed those of any of the more micro topics outlined in the NTIA notice.

Moreover, it will fulfill the requirements set down by the President of the United States in his Executive Order on cyber security.

NTIA and the Department of Commerce should build upon the work of the NIST Framework to facilitate sector by sector pilot tests of the use of the Framework and identify what elements are cost effective for discrete segments of industry which may be best prioritized by smaller companies and identify a menu of market incentives to encourage private sector use of the framework. This process would be organized by NTIA and conducted through the existing partnership structure of the Sector Coordinating Councils (SCCs) and their government counterparts, the Government Coordinating Councils (GCCs). This proposal is described in more detail below.

Why is this topic a good fit for a multistakeholder process, and would stakeholders reasonably be expected to come to some consensus?

Virtually any private sector entity that launches a new service goes through a research and development phase, such as the formation of the NIST Framework, and then pilot tests it with its target audience before full rollout. It is this critical pilot test step that has been skipped in implementing the President's Executive Order

Independent research has consistently shown that the primary problem with cyber security for critical infrastructure is economic – not technical. Sources as varied as PWC, McAfee/Intel, Ponemon, CIO Magazine, President Obama's Cyber Space Policy Review, the Center for Strategic and International Studies (CSIS) and the SANS Institute have all reported similar findings.

The reality is that, although the private sector is investing heavily in cyber security (private investment in cyber security has more than doubled over the past 5 years to more than $100 billion -- DHS entire budget is about $60 billion), a commercial level of security is inadequate to meet national security goals.

However, notwithstanding the fact that multiple studies point to economics as the principle problem to be solved in the cyber security space there has never been a targeted program focused on how to address this fundamental problem.

---

[10] Kassner, Michael. "Data Breaches May Cost Less than the Security to Prevent Them." *TechRepublic*. Tech Republic, 9 Apr. 2015. Web. 2015.

The fact that a wide cross sector of industry has advocated for such a program and there has been bi-partisan support for such an effort as is evident, suggests that the likelihood of achieving consensus is high, especially if, as we advocate, the program leverages the existing partnership model, is properly segmented and scaled (e.g. by industry sector) and is focused on the specific requirements of the President's Order (prioritization, cost-effectiveness and incentives)

There has been a consistent call to identify appropriate incentives for cyber security. A number of private sector and government sources have already been cited and the previous work of the Department of Commerce upon which the current initiative is based also came to this conclusion recommending that Commerce:

> "Develop incentives for I3S to combat cybersecurity threats -- The Department of Commerce should work with industry to create, through public policy and public/private partnerships and other means, new incentives for firms to follow nationally-recognized standards and practices as consensus around them emerges." [11]…(and) "The Department of Commerce and industry should continue to explore and identify incentives to encourage I3S to adopt voluntary cybersecurity best practices…. tax incentives, government procurement, and streamlined regulatory requirements would be most effective incentives to encourage adoption of best practices."

Unfortunately there has been little work on bringing industry and government together as was done with the NIST Framework process to define exactly what these incentives ought to be.

We advocate that the process be broken down by various sectors understanding that cost effectiveness, prioritization and may vary for various portions of industry. For example larger organizations with economies of scope and scale may easily accommodate the extensive risk management process outlined by the Framework whereas smaller entities may find the process cost prohibitive

Similarly with respect to incentives a streamlined permitting process may be more attractive to utilities whereas a procurement incentive maybe more attractive to the DIB etc. The process ought to also identify how an entity may qualify for them and how powerful they need to be. In addition, if data could be generated that indicate that various element of the NIST Framework were cost-effective in a commercial sense, it may well be that no incentive would be required to achieve broad adoption.

Finally, and especially for smaller enterprises, the existence of a massive scheme such as the NIST Framework may well be overwhelming. For these critical participants in the interdependent cyber security eco-system, prioritization is critical. For entities with less expansive economies of scope and scale they need to know where to spend their marginal dollar on security (training? New software? Shorter supply chain? etc. etc etc.)

All these objectives could be addressed through a "Pilot-Test" of the NIST Framework.

Pilot testing framework for its cost-effectiveness as well as prioritizing its elements for various industry segments (e.g. size or industry sector) and identifying Incentives for adoption would be a continuation of the multistakeholder process undergone to create the NIST Framework

A Great deal of work has already been done in this area, including by the Internet Security Alliance, and the Partnership for Critical Infrastructure Protection which made extensive presentations on this issue at a conference sponsored by DHS on the topic in 2013.There is general consensus amongst industry, at least at a high level, of what these incentives should be. If the Department of Commerce were to undertake this process of testing the NIST Framework and identifying incentives for its adoption, stakeholders would almost certainly be able to come to consensus around these items.

---

[11] Commerc, The Department Of. *CYBERSECURITY, INNOVATION AND THE INTERNET ECONOMY* (n.d.): n. pag. *NIST.gov*. US Department of Commerce, 2011. Web

I. Why would such a process would benefit the digital ecosystem as a whole;

Pilot-testing the NIST Framework for cost effectiveness, prioritizing it and creating a menu of market incentives tied to its use, in the process we suggest, would greatly benefit the digital ecosystem as a whole.

It has long been understood that in cyber security one size doesn't fit all. The Internet itself is a network of networks, many of which have idiosyncratic elements and unique characteristics. So too with the system's users who even at a broad class level, such as the "private sector" have wide diversities.

ISA is suggesting a coordinated program managed by government (DoC) in the same sense that NIST managed the Framework development program. The goal of the program would-be to coordinate and facilitate the implementation of the President's Order by leveraging the existing partnership model (specifically GCCs and SCCs) to develop data which will address the core economics of cyber security along the three identified lines in the President's Order (cost-effectiveness, prioritization and incentives)

Undergoing such a test would allow each sector to determine what portions of the framework are most effective at increasing overall Cybersecurity and which elements of the framework might be effective, but perhaps not cost effective. Understanding the cost implications of the best practices embedded in the framework gives stakeholders throughout the entire digital ecosystem --- especially smaller enterprises ---an economically based starting point for use of the framework, and for improving their security posture as a result. This will also enhance the voluntary nature of the system since private sector companies throughout the eco-system need little added incentive to adopt measures that have been verified as cost effective

The prioritization of the practices articulated in the framework would be particularly useful for small to medium businesses who tend to have extremely limited budget for cybersecurity and who are trying to determine where to spend their next marginal dollar. These small businesses are much more likely to prioritize marketing and sales over cybersecurity so prioritizing the Framework and being able to determine the "top 5" practices demonstrated to be most effective for improving security within any given sector would instantly make the Framework much more usable for smaller companies.

Increasing adoption for these smaller companies who might not prioritize cybersecurity over other business processes is particularly important considering these types of organizations are increasingly becoming the point of entry for APT attacks.

Target, for example, had fairly sophisticated security solutions deployed on their systems at the time of the attack. However, data was stolen from their system by means of compromised credentials of their HVAC vendor.

This focus on making small and medium sized businesses a priority for engagement was highlighted in the Department of Commerce green paper, as well wherein it states:

> "…small and medium-sized businesses are most in need of learning more about cybersecurity best practices. These businesses generally have few resources to stay abreast with cybersecurity developments; yet they possess sensitive data that they must protect."

Prioritizing the Framework and creating a menu of market incentives for its adoption would benefit these smaller organizations who might not think they have any valuable data to steal, but are likely interconnected with larger companies who do have more sought-after data.

II. How long a facilitated, participant led process on this topic should take to come to consensus;

The specific nature of these pilot tests ought to be determined jointly by using the established partnership system that is described under the existing National Infrastructure Protection Plan (NIPP). Specifically, ISA proposes that

each Sector Coordinating Council (SCC) in conjunction with its sibling Government Coordinating Council (GCC) design an appropriate testing plan for the Framework.

Utilizing the existing public private partnership structure described above, these tests should be able to be completed within six months to a year.

lll. What form would an actionable outcome take?

By using the existing partnership model described above to pilot test the NIST framework, stakeholders would produce detailed and specific actions for how to best use the NIST framework on a sector-by-sector basis. These detailed and specific actions would be prioritized – making them more actionable for organizations both large and small and for the entire digital ecosystem as a whole.

In addition to these actions and determining which elements of the framework are most cost effective, these pilot tests would identify the instances wherein security practices may be quite effective at increasing security but not cost effective. These tests would then be able to determine where market incentives for adoption of best practices are most needed; for which sectors; and for what type of companies.

Many of these market incentives listed below have been called for by the White House -- through various blog posts by White House Cybersecurity Director Michael Daniel -- and even by the Department of Commerce itself in its 2011 Green paper. These resulting market incentives for voluntary adoption of cybersecurity best practices and standards advocated by several government entities including the Department of Commerce, include:

Streamlining Regulation and Reducing Audits

To the extent that is possible, the federal government should streamline these redundant regulations where they exist which would allow private sector entities to better allocate resources to improving the overall security of their organization, and by consequence, the nation. Specifically, the Government might map the NIST Cybersecurity Framework to existing compliance regimes and allow companies who participate in the pilot test process, described above, to use it as a tool to "audit once, report out to various regulators many times". ISA as well as several other prominent trade groups, including the Business Software Alliance (BSA), US Chamber of Commerce, TechAmerica, and Center for Democracy and Technology, have advocated for years the need for regulatory streamlining which would save time and resources for both the private and public sectors.[12]

Again, the Department of Commerce itself advocated for this approach in its 2013 report on incentives to the president, which was mandated in EO 13636:

> "Once NIST has published the first version of the Framework and the Program is operational, the Administration, independent agencies, and Congress should use this information to inform discussions of specific regulatory streamlining proposals." [13]

In a recent statement, a large US bank indicated that requests from a multitude of regulators have increasingly become redundant. The bank continually receives the same requests from different regulators which has resulted in a 500% increase in the amount of resources spent synthesizing customized, but largely identical reports to accommodate these redundant requests.
A system of regulatory mandates applied to the broad and diverse private sector is not effective, and is actually counter-productive, in generating substantial improvements in private sector cyber security from both a national economic, as well as a national security perspective.

Recently, a large US defense contractor reported an annual decrease in the amount of penetration testing and security monitoring the organization conducts because the organization had to reallocate the staff, time, and resources previously spent on security to respond to regulatory requests and audits.

---

[12] Internet Security Alliance. "*Improving our Nation's Cybersecurity through the Public-Private Partnership*". Rep. Internet Security Alliance, 2011.
[13] Department of Commerce Recommendations to the President on Incentives; Summary. 2013

The regulatory agency model of governance was created during the 19th century to address the hot technology of that day—the railroads. And, while rail travel today is remarkably similar to what it was in the 1800s, the Internet, however, is characterized by nearly daily change. The process of developing effective regulations is inherently time consuming there is virtually unanimous agreement that any regulations specific enough to assure improved security quickly become outdated soon after their enactment.

Federal Grants & Tax incentives:

The federal government could provide additional grant funding and tax incentives that encourage establishing additional cybersecurity investments. Critical infrastructure industries can use grant funds for research and development, to purchase equipment, and to train personnel necessary for the adoption of cybersecurity best practices such as the NIST Framework. Again, this approach for providing grants and tax incentives has been widely endorsed by industry for years as evidenced in ISA's trade association white paper on the public-private partnership[14]

While tax incentives are often difficult politically, this approach may be targeted to smaller and medium-sized businesses. SMEs are a weak link in the cyber security supply chain and, without incentives, they may never perceive compliance with effective cyber security practices to be economically beneficial. These grants and tax credits would allow these smaller private sector entities to adopt or develop the best practices included in the NIST Framework that might be very effective for increasing their cybersecurity within their business or sector, but might be less cost effective.

One of the benefits of this approach is that there is no significant impact on the federal budget due to the fact that this money is already designated for distribution.

Fast-Track Patent Pilot to Promote R&D

R&D efforts at critical infrastructure companies are susceptible to the ongoing threat of trade secret theft from rouge cyber criminals and state-sponsored entities. The U.S. Patent and Trademark Office should explore building a Fast-Track Patent Pilot for private sector organizations who voluntarily adopt the best practices outlines in the NIST Framework. This, could provide a significant incentive for R&D-intensive critical infrastructure companies to adopt or otherwise use the Framework. This market incentive for adoption of voluntary best practices was specifically highlighted by the Department of Commerce in its incentives report to the President pursuant of Executive Order 13636[15].

SAFETY Act Designations

Government could update the SAFETY Act to better appreciate the cyber threat that has become more evident since its enactment. This Act can be expanded to standards and best practices, such as those found in the NIST Framework, as well as technologies that protect against commercial as well as terrorist threats.

By designating or certifying organizations under the SAFETY Act for developing or using cyber security technology, best practices, and standards, these organizations can similarly take advantage of marketing and insurance benefits, which can provide tangible business paybacks and encourage cyber security spending beyond what was justified by their initial business plans.

Leveraging Procurement Policy and Purchasing Power of Federal Government

Government could increase the value of security in the contracts it awards to the private sector, thereby encouraging broader inclusion of the level of security provided to government. In turn, this would facilitate broad

[14] Ibid
[15] Ibid

improvement of the cyber security posture among critical infrastructure owners and operators. The result of "building in" effective cyber security in products and services that are developed and delivered to the government at inception will not only insure the public's best interest but if such requirements were extended to secondary suppliers and sub-contractors as well, this initiative could have a significant effect on down-stream entities.

Such modifications to procurement policy might include:

- A federal acquisition incentive could include relief from certain other FAR regulations that might be overly burdensome and not germane for the supplied product or service if an entity adopts the Framework;
- Include indemnification or partial indemnification for claims arising from supplied products.
- Federal acquisition preferences, such as those utilized in the minority-owned business, woman-owned small business, and veteran-owned small business programs as described in The Veterans Benefit Act of 2003; Small Business: 15 USC 633 et seq; Women and Minorities: 15 USC 637; the Office of Federal Procurement Policy Act of 1974 (Pub. L. 93-400);

While this approach does have the potential for substantial benefits, government would need to enhance the value of its contracts because a number of the smaller organizations within the supply chain do not have the same massive incentive to adopt government specifications that some larger players do. While this approach has potential for real and immediate benefits, it is important that government realize that such compliance cannot be expected to come "for free." National security has a cost, and that cost is the government's responsibility.

IV. What pre-existing organizations and work already exist on the topic?

The model for the public private partnership which would be the basis for conducting these tests -- Sector Coordinating Councils (SCCs) and their public counterparts the Government Coordinating Councils (GCCs) -- is outlined clearly in the NIPP. These SCCs and GCCs are well established and have demonstrated their ability to function as collaborative as joint coordinating bodies for their sectors. Indeed, several of the Sector Coordinating Councils, including the ITSCC, have undergone similar exercises to identify incentives for adopting cybersecurity best practices for their sector. [16]

The previous work done on promoting the use of market incentives to increase adoption of cybersecurity best practices is quite comprehensive. The House GOP Task Force Report on Cybersecurity, the Cyberspace Policy Review, the President's Executive Order 13636 on Cybersecurity, and the NIPP all agree that in order to increase adoption of cybersecurity best practices, there needs to be a tailored menu of market incentives available to companies to make cybersecurity more cost effective.

The House GOP Task Force Report states:

> "We believe Congress should adopt a menu of voluntary incentives to encourage private companies to improve cybersecurity. Some incentives may have a cost and would have to be offset. Others do not. However, incentives should be largely voluntary, recognizing that most critical infrastructures are privately owned. Companies that do not own critical infrastructures could also utilize many of these incentives. We

[16] Internet Security Alliance. Testimony of Larry Clinton before the House Energy and Commerce Subcommittee on Communication and Technology. "Cybersecurity: Threats to Communications Networks and Private-Sector". Internet Security Alliance, 2012. < http://www.isalliance.org/congressional-testimony/>

Internet Security Alliance. Testimony of Larry Clinton before the House Subcommittee on Communications, Technology and the Internet. Internet Security Alliance, 2009. < http://www.isalliance.org/congressional-testimony/>

Information Tchnology Sector Coordinating Council. "IT SCC response to March 28, 2013 Notice of Inquiry of the Department of Commerce". IT SCC, 2013

also have to recognize that different companies and sectors will need different incentives – one size does not fit all. Committees should evaluate incentives that will be effective within their jurisdiction."[17]

Following the release of The President's Executive Order 13636 on Critical Infrastructure Cybersecurity, the Department of Commerce, Department of Treasury, and the Department of Homeland Security all submitted separate reports to the president on Incentives. As part of this process DHS in conjunction with the Partnership for Critical Infrastructure Security (PCIS) representing all 18 critical sectors held a conference on these themes, which generated a more extensive list of incentives. These rep[orts all had one central theme – government needs to make available to industry a broad set of tailored incentives to promote adoption of cybersecurity best practices. The type of pilot test we are proposing here would help identify and inform which incentives are needed in which sectors.

Additionally, the Department of Commerce in its report on incentives to the president specifically highlighted the need for such a broad menu of market incentives to be identified through the proposed NIST Framework pilot testing process:

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

2. Please comment on what factors should be considered in selecting the issues for multi stakeholder processes. IPTF also plans to draw on the Green Paper and earlier responses to past Requests for Public Comment; past respondents are invited to provide additional and updated viewpoints on IPTF efforts since those comments were provided. Implementing the Multistakeholder Process: Commenters also may wish to provide their views on how stakeholder discussions of the proposed issue(s) should be structured to ensure openness, transparency, and consensus building. Analogies to other Internet related multistakeholder processes, whether they are concerned with policy or technical issues, could be especially valuable.

From February 2013 to 2014 NIST conducted a much-praised program that resulted in the development of the NIST Framework.[18] The Order itself identifies the factors that should be considered in the multi-stak-holder process we are proposing. The Order stated

> "The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall 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."[19]

Despite praise and pledges of support from both industry and government hard data on the use of the Framework remains spotty at best. Indeed the most systematic study of Framework usage, a Pricewaterhouse Coopers survey

[17] Executive order 13636; Section 7(d)
[18] Framework for Improving Critical Infrastructure Cybersecurity. Rep. National Institute of Standards and Technology. *NIST.gov.* February 2014.
[19] EO 13636; Section 7(b)

found that less than 20% of major corporations had even discussed the use of the Framework and discussion of the Framework, let alone use, among smaller (i.e. under $1 billion market cap) companies was between %5 and %10. [20]

A student of the literature of cyber security might not be surprised by the lack of uptake of the NIST Framework as the cited studies clearly indicate that the simple existence of technical and management solutions are, by themselves insufficient to generate use.

The missing links in implementing the President's Executive Order are the as yet uncompleted, in fact arguably un-started, mandates that the Framework not just be created, but that it be demonstrably prioritized, incentivized and identified as to its cost-effectiveness.

It is unreasonably, and unsustainable to expect private entities to make uneconomic security investments on a continual basis is for such an eventuality that the EO calls for a set of incentives to be deployed to narrow the gap between commercial and public security. Again, lacking hard data it is difficult for policy makers to determine what elements of the Framework need to be incentivized or what degree of financial power needs to be embedded in the incentives

Again, lacking any hard data it is extremely difficult for particularly smaller players, to prioritize which elements of the vast NIST Framework they will be best off investing their limited funds in. Once again, this uncertainty will depress investment and hence security.

ISA proposes to fill the gaps between the NIST Framework and the vision of the President's Executive Order through a systematic "Pilot Testing" of the Framework.

Such a process, outlined in detail below, would allow the Department of Commerce to accurately answer questions relating to the topics discussed in this Request for Comment including:

- What elements of the framework require the most immediate attention to increase our nation's cybersecurity?
- Which best practices articulated in the Framework are most cost effective?
- Which best practices articulated in the Framework are *NOT* cost effective?
- Which elements of the framework are most effective for increasing security but are not the most economically practical for business?

3. Please comment on the best structure and mechanics for the process (es). If different security issues will require different process structures, please offer guidance on how to best design an appropriate process for the issue selected.

NIST Framework Pilot Test Proposal

The specific nature of these tests ought to be determined jointly by using the established partnership system that is described under the existing National Infrastructure Protection Plan (NIPP). Specifically, ISA proposes that each Sector Coordinating Council (SCC) in conjunction with its sibling Government Coordinating Council (GCC) design an appropriate testing plan for the Framework. These designs should determine at a minimum:

- What would "count" as "adoption" of the framework suitable, which, in turn, would be suitable for eligibility of access to the menu of incentives described by the President's Executive Order (EO);
- What aspects of the framework are cost-effective for deployment as suggested in the President's Executive Order; and
- Other goals as determined jointly by the SCCs in conjunction with the GCCs for each sector.

[20] Ponemon Institute. "Cyber Security Incident Response: Are We as Prepared as We Think?" Lancope. January 2014. Accessed April 21, 2014. http://www.lancope.com/files/documents/Industry-Reports/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf/.

While the specific design of the testing would be tailored to the unique characteristics of each critical infrastructure sector, there are some general themes that should or could be universally embraced. In ISA's initial test plan concept, we would anticipate government and industry collaboratively use the existing partnership structure to:

- Seek out private sector organizations that are generally representative of the target audience for which the Framework is intended for use as envisioned in the President's Executive Order;
- Solicit the voluntary participation of those organizations in the testing procedure,
- Identify the government agency that will provide the "install," educate the critical infrastructure end-user on the Framework intent and purpose, provide the knowledge and training on how to implement the Framework, and provide assistance to the end-user in:
    - Identifying the "golden nuggets" to be protected;
    - Selecting the right maturity level (tiering) for its organization;
    - Developing a sustainment plan;
- Engage the GCC or sector specific agency to assist any entity that volunteered in deploying the Framework and jointly set appropriate goals and metrics – possible metrics could include:
    - Measurements of "effort required";
    - Measurements of time to implement/maintain;
    - Measurements of cost to implement (people/equipment) and maintain;
    - Did it meet the agreed to outcomes;
    - Satisfaction of both end-user critical infrastructure owners/operators and government partners with respect to the effectiveness of the Framework;
- Deploy the aforementioned market incentives available for use for the participating entity;
- Conduct an assessment, sufficient to be representative of what would reasonably be required to determine success of the effort (as jointly determined by the government and industry participants); the assessment will, at a minimum, measure costs, benefits, effect of deployed incentives and any unanticipated or anticipated, deployment problems and make recommendations back to the partnership as to appropriate next steps such as streamlined process or needed additional incentives.

Under this proposal, it is assumed that participating critical infrastructure entities will be donating internal resources to this effort (which will be accounted for in the costs column) and government will be contributing resources to assist with deployment, so as to ensure the vision of the Framework is properly captured.

In this case, the market incentives described above, which may have significant attractiveness to critical infrastructure, but do not have significant budget impact for the federal government, become vitally important to broad-based participation.

Data from the tests would be anonymized so that no specific data related to any private sector entity would be made available. There should be no requirement that any participating entity publically acknowledge either its participation or the results of any testing.

This proposal would be an organized, scientific process that utilizes the existing official partnership structure to systematically and independently determine key elements of the Framework which are not achievable or otherwise cost-effective under the current government plans.

4. **How can the IPTF promote participation from a broad range of stakeholders, i.e., from industry, civil society, academia, and international partners? In particular, how can we promote engagement from small and medium-sized enterprises (SME) that play key roles in the digital ecosystem? How critical is location for meetings, and what factors should be considered in determining where to host meetings?**

Utilizing the existing partnership structure articulated in the National Infrastructure Protection Plan to engage each sector in a test of the NIST framework would ensure broad participation from industry, civil society, academia, and international partners.

The private-sector organizations involved with the sector coordinating councils have already demonstrated their willingness to participate in the public private partnership by means of volunteering their time to engage in such a venue. Typically, the companies involved with the sector coordinating councils represent a broad sample of their specific sector – from large enterprises to small and medium businesses as well.

These coordinating councils and their government counterparts are already well-established and well-respected within the domestic and international community. A coordinated effort by each sector's SCC and GCC to undertake the NIST Framework pilot test described above would ensure broad-based participation from industry, academia, and the international community.

5. What types of consensus outcomes can promote real security benefits without further adding to a compliance-oriented model of security?

By demonstrating what elements of the Framework are cost effective for discrete industry types Commerce will have identified cyber security process that will be voluntarily adopted by these industry types as industry routinely uses process that they know will be cost effective.

The process we identify may also generate data as to what elements of the Framework are effective from a security perspective, but perhaps are not **cost-**effective. This will generate information for policy makers upon which security practices ought to merit use of one of the incentive mechanisms identified above and to what **degree** of intensification might be required to generate future voluntary adoption,

Finally this process will generate data as to which elements of the Framework will generate the most success and hence ought to be adopted first for organizations operating with limited funds thus assisting with the critical prioritization that is an inherent part of any comprehensive risk management process.