

October 10th, 2014

The Internet Security Alliance

Response to the

National Institute of Standards and Technology's Aug 26th, 2014 Request for Information: "Experience with the Framework for Improving Critical Infrastructure Cybersecurity"

Awareness Question 1: What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?

Absent an impartial and systematic survey of the nation's critical infrastructure, it is not possible to answer this question with any degree of reliability or validity.

The closest such work we are aware of in the PricewaterhouseCoopers 2014 Annual Corporate Directors Survey, published in September of 2014, which contains some data on this issue.

The PWC survey reports that nearly 4 out of 5 (79%) corporate boards have not even discussed the NIST Framework, let alone used it, or directed their senior management to use, it for cyber risk management.

Moreover, the PWC survey reports that ""mega-cap company directors are four times more likely than small cap companies (less than \$1B per yr) to have discussed the NIST framework." This means only about 5% of smaller companies---the enterprises most vulnerable and in need of assistance ---have discussed the framework.

While these raw numbers may seem disheartening it is not clear how to fully assess them since we do not have a baseline we don't know if this is great uptake or not. ISA has commented previously (see appendix A) that the assessment of the NIST efforts would be greatly enhanced if clear goals were established which could be measured independently through sources such as PWC.

That being said given the tremendous and laudable efforts by the Administration ---from the White House through NIST ---to publicize the Framework with press events, roadshows and substantial voluntary industry partnerships including nationwide press provided by ISA and others (as will be described below) the fact that 4 out of 5 major companies have not even discussed the framework would seem disheartening, but perhaps not surprising.

As we have commented elsewhere (see appendix) and will repeat, if government sincerely wants to generate interest in a voluntary program aimed at the private sector, it must talk in the language of the private sector. The NIST framework is primarily a technical document. Industry is inherently focused on

economics. Notwithstanding the directives as laid out in the President's Executive Order the NIST framework is not clearly cost effective or prioritized from an economic point of view.

If the framework can be demonstrated to be cost effective, industry will naturally take note and adopt its principles ---because it is cost effective to do so. However, simply claiming that use of the framework is, or could be, cost effective, will not be sufficient ---- some hard evidence will immeasurably aid in raising awareness

This should not be understood as a criticism of what NIST has done either in developing or promoting the framework. Rather it is a pragmatic suggestion that we need to turn our focus away from the narrow technical view of cyber security and begin to work on the economic and cultural aspects. ISA is aware of, and applauds recent remarks by the White House senior advisor on cyber security Michael Daniel who has said exactly this and we look forward to working together in this direction.

ISA did poll its own membership in order to provide some hard data for this inquiry. ISA's membership includes organizations deeply involved in the critical infrastructure which is presumably the target of the NIST Framework including aviation, banking, communications, defense, education, financial services, information technology insurance, manufacturing security and manufacturing. This is not a random sample and therefore generalization maybe limited. However, the results may be indicative of the large generally sophisticated organizations from these critical infrastructure sectors.

Initial results of this survey showed Internet Security Alliance members have well established cyber security risk management processes, and for them, the Framework does not add additional value, and therefore they report that it has been an insignificant factor in their approach to risk management.

Additionally, awareness of the Framework is a necessary but not sufficient condition for the substantial behavior changes in cyber risk management needed to secure the Nation's critical infrastructure envisioned by the President's Executive Order.

Rather than using an imprecise estimate of awareness based on publicly attributable self-reports, NIST should construct a systematic, not for attribution, review of Framework related behavior within specified target audiences. Such a review could generate more reliable and valid data on the degree of awareness targets have of the Framework and more importantly observable changes in behavior based on its existence insights as to how expanded use can be motivated.

In initial comments ISA had suggested beta testing the Framework coincident with the overall roll-out. While a pure beta-test may not be feasible at this stage, the ability to construct a systematic analysis to generate reliable information upon which to base future Framework/EO related policy is still achievable. There remain great benefits to conducting a systematic analysis of the experiences of a core group of critical infrastructure operators in test-cases to determine how we can best affect the goal of stimulating behavior change as called-for in the President's Executive Order.

ISA suggests an initial starting point for such an endeavor would be a more precise delineation of the target audience than the extremely broad and vague term 'critical infrastructure.'" The vast differences in size, culture, regulatory environment, threat vectors and other differences within the mega-category of "critical infrastructure ---even within sectors makes this a difficult unit for analysis. More precise definitional work and targeted research will likely yield clearer answers as to the degree of traction the

Framework has achieved and is consistent with the overall risk management philosophy of the Framework itself.

A second core issue in determining the degree of traction the Framework has achieved, and may achieve in the future is the degree to which it is being used to effect cyber risk management behavior. At its core the Framework is primarily a compilation of already existing standards and practices much of which have been in use in large elements of the critical infrastructure for many years. Some research has suggested that as much as 90% of industry use at least some key elements of these practices and standards and have done so for years and these results are again supported by the ISA survey done in conjunction with the current RFI.

The key question for determining the Framework's traction in advancing the goals of the President's Executive Order to what extent the Framework is being used by critical infrastructure organizations that have not already adopted a sufficiently robust approach to cyber risk management.

In previous comments, ISA proposed that NIST measure the effectiveness of the framework by working with the Sector Specific Councils to find a group of critical infrastructure operators who do not already have a well-defined risk management process for a "beta-test." We propose, specifically, that each Sector Coordinating Council (SCC) in conjunction with its sibling Government Coordinating Council (GCC) design an appropriate testing plan for the Framework for organizations within their sector without a well-defined risk management process, with the goals of identifying:

- What should count as "adoption" of the framework, which, in turn, would be suitable for eligibility of access to the menu of incentives described by the President's Executive Order (EO) (perhaps based on the Framework "tiers");
- What aspects of the framework have been shown to be cost-effective when applied to well defined CI targets?
- Other goals as determined jointly by the SCCs in conjunction with the GCCs for each sector.

ISA also suggests that 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," i.e. 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 "crown jewels" 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 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.

Awareness Question 3: Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the framework?

ISA is not able to speak to all the critical infrastructure sectors, but is generally aware of substantial industry effort to promote and use the Framework. In addition to working directly with its membership to educate and inform with respect to the Framework ISA participates regularly with a wide range of industry associations who have formed an informal coalition to coordinate among themselves and the government to share information and promote the Framework.

ISA has aggressively reached out to key audiences to inform and promote use of the Framework.

At a more micro-level, ISA was asked to participate in the FCC-commissioned Communications Security Reliability and Inoperability Council (CSRIC) focusing on cyber security best practices, and serve as co-chair of the “Barriers to NIST Framework implementation” working group. Responses to this question are largely derived from ISA’s participation in the overall project and specifically its role as co-chair of the barriers to implementation Group, However, the comments made here are ISA’s alone and do not in any way presume to represent the CSRIC process or any of the specific participating companies.

CSRIC Working Group 4 has participation from over 80 Communications Sector organizations, which aim to “...demonstrate how communications providers are reducing cyber security risks through the application of the NIST Cyber security Framework, or an equivalent construct.”¹ To this end, participation has been collaborative and productive in identifying how the broad communications sector and sub-sectors (wireline, wireless, broadcast, cable and satellite) interacts with the voluntary framework developed by NIST.

The working group ISA chairs were charged with identifying the barriers to implementation amongst the organizations participating. ISA conducted a series of interviews with the leadership teams from each sub-sector. This project is still a work-in-progress and will be completed in March 2015. In working with these groups, ISA aggregated feedback on several barriers to Framework Implementation, which can be grouped into four distinct focus areas:

Financial Barriers:

- The financial barriers for small businesses, which are trying to decide where to spend their next marginal dollar and which have much more limited funds, are significant. These companies would benefit greatly from prioritization in the framework
- Determining the return on investment (ROI) for a technological process used by an organization to increase their cyber security posture is very difficult. Due to this, determining what technologies or processes to invest in becomes difficult. Money spent on security controls, which cannot be accurately analyzed to determine their value can result in more austere budget environments – thus creating more financial barriers to implementation.
- The time and resources it may take for an organization to systematically go through all 98 categories and sub-categories of the Framework should be taken into consideration when examining financial barriers. Since it is unclear what “framework implementation” means, the time and money it takes for an organization to determine what implementation means for them (both onetime cost and continuing costs) can be considered a significant barrier to implementation.

Technology Barriers:

- Uncertainty around the value of certain technologies. This relates to the financial barriers discussed above – particularly the barrier of the inability to determine return on investment of implementing a single technology solution or suite of technologies.
- The degree to which technology can be a barrier to implementation of the NIST framework is fundamentally a function of enterprise resources, as further tempered by the enterprise’s Tier position as well the risk management profile that the enterprise selects as in its best interests.

Consumer / Market Barriers:

- Consumers, who largely do not know or care about NIST Framework implementation, want to trust that the security is working for the products and services they use. Therefore, Framework implementation, assuming implementation results in actual increased security (which remains to be demonstrated) should serve as an incentive as far as the market is concerned. However, due to the uncertainty surrounding what constitutes as “framework implementation” and whether or not implementation actually increases security, this incentive is unclear.

Operational Barriers:

- The lack of ability to provide quantifiable metrics to demonstrate that implementing the framework actually increases security may serve as a barrier to future implementation. If companies don’t have metrics to demonstrate that actual security is being improved, not simply complying with all 98 sub-categories, companies will be less likely to implement the framework.

Awareness Question 5: What are the greatest Challenges and opportunities – for NIST, the federal government more broadly, and the private sector – to improve awareness of the framework?

In a speech on September 17 the President’s senior advisor for cyber security, Michael Daniel, declared that we need to fundamentally rethink our approach to cyber security and focus more on the economics and cultural aspects of the issue.

ISA completely agrees with this Mr. Daniel's assessment.

Moreover, Mr. Daniel's view is fully consistent with a large and growing set of independent research, which has consistently shown that the number one problem with respect to securing critical infrastructure is economic. Sources as varied as PWC, McAfee/Intel, CIO Magazine, and CSIS have all reported similar findings.

Digital economics is rapidly changing and generally poorly understood. Even comparatively recent reports from sources such as the US Department of Homeland Security in their so-called Cyber Security ecosystem report assert, without evidence or supportive reasoning, that profitability will drive adequate cyber security spending and hence there is no reason to address the economics of the issue.

Not only is this assertion wrong (if it were correct the problem would have self-corrected years ago) but in some respects the very opposite is the case. Many digital technologies and associated business practices that drive corporate innovation and profitability simultaneously can have the effect of undermining cyber security. The list of these technologies and practices is long and growing including the move from traditional voice to VOIP, the use of long international supply chains, cloud computing, BYOD (bring your own device) the "Smart Grid" and the Internet of Things.

Getting policy makers to appreciate the criticality of the digital economics in cyber security, understanding the nature of the digital economy in this regard and then designing and implementing policies that will both enhance security and promote the innovation, growth and productivity that our economy demands is by far the most challenging issue for the federal government in general, the Department of Commerce (where NIST lives) and NIST in specific to overcome.

Since its inception ISA has appreciated this aspect of the issue. Indeed the Mission Statement of the ISA is to integrate advanced technology with economics and public policy to create a sustained system of cyber security. The federal government might do well to adopt a similar mission, and perhaps it will follow Mr. Daniel's prescription.

ISA, both as an independent multi-sectoral trade group focused on cyber security and in its role as the Chair for the Partnership for Critical Infrastructure Protection (representing all 18 critical infrastructures) Task Force on cyber security market incentives, has long advocated a broad series of specific steps that can address the economics of this issue in a pragmatic fashion.

For example, ISA has called for the deployment of a menu of market incentives to promote good cyber hygiene associated with mitigating between 80-90% of cyber-attacks. ISA has also identified a smaller set of cyber security best practices that have been shown via independent research to not only be effective but cost effective. Finally ISA, in its aforementioned Handbook for corporate boards, has offered several cost effective strategies for organizations dealing with Advanced Persistent Threats.

These principles might be useful elements of a more targeted cyber information program for the federal government to pursue.

NIST might provide a useful service by adapting the same highly-praised model it used to develop the technical framework to the more difficult issue of determining overall cost effectiveness for the cyber security and specifically identifying incentives that can be applied to the differing cultures and economic characteristics of various portions of the critical infrastructure.

Finally, although there was a set of preliminary reports issued following the announcement of the President's Executive Order on cyber security, these reports were generally disappointing and the follow up has been almost non-existent. Mitigating some of the costs involved with voluntary adoption of the framework will increase awareness and overall implementation. Therefore, ISA suggests that the federal government resume the work on incentives that was initiated by the four government reports – U.S. Department of Treasury, Commerce, Homeland Security, and GSA/DOD – and called for in the President's EO.

There ought to be a wide range or "menu" of incentives that can be deployed, which may have significant attractiveness to critical infrastructure, but do not have significant budget impact for the federal government, such as:

- Process Preference – The Government could use Framework "adoption"/beta test participation as criteria for prioritizing who receives "fast-tracked" -
 - SAFETY Act designations and certifications;
 - Patent approval;
 - Security clearance;
 - Permitting and/or other Governmental approvals;
- Modification of the SAFETY Act to better encompass "cyber";
- Streamlined Compliance – The Government could map the Framework to existing compliance regimes and allow participating beta test entities to use it as a tool to "audit once, report out to various regulators many times";
- Procurement Advantaging –
 - 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);
 - Federal acquisition rebates as utilized in the "Indian Incentive Program" – <http://www.acq.osd.mil/osbp/sb/programs/iip/>
- Brand Recognition;
- Technical Assistance.
- For smaller organizations, the Small Business Administration should support those businesses that request assistance for using the voluntary Framework as a tool to address cyber risk.

Awareness 7: If your sector is regulated, do you think your regulator is aware of the Framework, and do you think it has taken any visible actions reflecting such awareness.

Adoption of the framework remains hampered by fears that independent regulators will use Framework documentation as discoverable material in examinations, leading to enforcement actions.

Registered investment advisors and broker-dealers, specifically, have a disincentive for adopting and implementing the NIST Framework – regulatory reprisals from the SEC and FINRA. The SEC Office of Compliance Inspections and Examinations (OCIE) began using the Framework this year as a foundation to conduct examinations of registered broker-dealers and investment advisers. The SEC OCIE examination questions track with the Voluntary Framework and apply an additional layer of compliance concerns for regulated advisors. The SEC and FINRA treat risk assessments and frameworks as discoverable material during the examination process. As a result, the RIA / broker dealer communities exercise caution before creating any documentation that can be used in examinations for enforcement action or findings of deficiencies.

ISA’s position remains that the government’s interest should not be in building a new “compliance regime” but rather in assuring the efficacy of intervention supported by a network of incentives based on good faith and merit.

Regulatory agencies, like the SEC, must give clear guidance that firms using the Framework, participating in good faith, will not face regulatory consequences as a result of their adoption or findings from Framework activities. Without regulatory amnesty, aggressive groups like the SEC hinder adoption of the Framework across industries.

Awareness Question 6: Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?

While it would be impossible to make a valid assertion about the current international reach of the Framework, we do see a growing appetite in the international community for a similar approach around the world.

Many countries have a “wait and see” attitude about the Framework. While there is genuine interest in what is happening domestically, they would like to see measurable change in both industry and government before committing to something like the Framework as part of their approach to increasing security.

Extensive compliance regimes for multiple countries with varying laws and underlying standards can divert critical security resources from core security tasks without appreciably increasing enterprise security.

There is a high demand for the creation of a single uniform international standard or framework to guide cyber security investments. In response to market need, the Internet Security Alliance is working with companies in the EU to assemble a group of international businesses to provide advice and comment on the emerging US Framework, and draw it toward being a more global resource.

Awareness Question 8: Is your organization doing any kind of outreach or education of cyber security risk management (including the framework)? If so, what kind of outreach and how many entities are you reaching?

ISA has been engaged in numerous public information efforts to inform about and advocate for the Framework, Perhaps the most notable of these is the column written by ISA's President advocating use of the Framework, which appeared in the Digital Security supplement to the September 19th edition of USA Today that was distributed to literally millions of reader's nation-wide.

ISA has also engaged in numerous events to inform and promote Framework usage with key target audiences

Cyber Risk Oversight Handbook for Corporate Boards

One notable example has been ISA's work, in conjunction with AIG, with the National Association of Corporate Directors (NACD). Obviously, as a voluntary program targeted toward the private sector, corporate boards, who design both the strategies and finances for their organizations are perhaps the ultimate target audience for the President's executive Order and the NIST Framework. In fact the initial drafts of the Framework attempted to articulate a higher level enterprise-wide Executive rationale for the Framework but this effort was largely abandoned in the NIST process at least in part to defer this development to the private sector. As the nation's primary organization of corporate directors, NACD is a key pathway to getting the message of the Framework up to the board level, and ISA was happy to fill this gap.

Working with AIG and NACD, the ISA board of directors constructed the first ever Handbook for cyber security risk management specifically targeted at corporate boards. NACD published the document and has reported downloads from their membership in the several thousand at this point.

The Handbook builds upon The Framework and uniquely places cyber security within the context that corporate boards and senior managers truly focus on – things like profitability, growth, innovation, and PE ratios – and explains how to integrate cyber security into the business decisions they need to make such as mergers/acquisitions/new product development. Through our partnership with NACD, we have cracked the "glass ceiling" and are actually reaching corporate boards with key cyber security insight and practical advice. The ISA sees it as the fulfillment of a long-time goal to have cyber security understood at the highest levels of enterprise not simply as an "IT issue" but as an enterprise-wide risk management issue.

One of the principles called for in the Cyber Risk Oversight Handbook is that directors should set an expectation that management establish an enterprise-wide cyber-risk management framework with adequate staffing and budget which follows ISA's earlier work in this field "The Financial Management of Cyber Risk, published jointly by ISA and ANSI in 2010. The Handbook builds on this earlier work to suggest directors use this model to set the expectation that management leading to implement a the NIST Framework in developing the company's cyber-risk defense and response plan.

Following The Handbook's publishing in June, the Department of Homeland Security endorsed the publication making it the first, and only, private sector document that has been included in government's program to promote adoption of the NIST Framework for cyber security created by the President's Executive Order.

Subsequently, the Institute of Internal Auditors (IIA) Research Foundation, in conjunction with ISACA published a research report entitled "*Cyber Security: What the Board of Directors Needs to Ask*". In constructing this document IIA and ISACA relied exclusively on the Cyber Risk Handbook jointly published by NACD, AIG and ISA. The IIA & ISACA document cites the Cyber Risk Oversight Handbook and used each of the 5 major principles as the basis for more detailed advice for corporate boards and their auditors. The American Bankers Association has also chosen to highlight the Handbook in their extensive "Cyber Security Awareness Month" program, which ISA will participate in as presenter.

The Endorsement by the IIA and ISACA was followed by an endorsement by the Chamber of Commerce, which has added the Cyber Risk Oversight Handbook to their list of resources in their Cyber Roundtable Booklet. These booklets are being used at workshops around the country, which aim to increase awareness on the framework and promote voluntary adoption, by private sector entities.

In addition to the Handbook being used as a resource in Cyber security events hosted by the U.S. Chamber of Commerce, ISA has been asked to present the Handbook at industry events across the country. Such events include an upcoming webinar on cyber-risk hosted by KPMG and NACD in New York as well as a conference designed to give investment advisor compliance professionals the necessary tools to help implement better cyber security practices hosted by Ascendant Compliance in California.

Awareness Question 9: What more can and should be done to raise awareness?

It is important to set appropriate expectations first. Our nation's cyber security problem is large, growing, and multi-faceted. Perhaps the most challenging aspects of the issue are how the growing interconnection of networks, sometimes referred to as the Internet of Things, is exacerbating the problem.

The early notion that it might be possible to cordon off a limited set of critical infrastructure for security is being challenged with the increasing realization this cordoning off process is far more difficult than initially conceived. We now have reports of sophisticated attackers using seeming beguine entry paths such as popular Chinese restaurants as a channel to compromise critical energy facilities.

In this environment the degree of awareness needed to secure even the subset of critical infrastructure is well beyond the ability of set of modestly funded government outreach programs even when coupled

with extensive private sector voluntary efforts as we have seen in the first six months since the Framework was launched.

The task grows exponentially larger if we elevate our goals to enhancing the economic security of our nation beyond the so called critical infrastructure and include protecting systems from the rampant theft of intellectual property, business process and personal data that is being compromised through cyber means. These attacks are already having a significant negative impact on R & D investment, innovation and eventually job creation and overall economic competitiveness.

Raising awareness to meet the true scope of the problem we need to address will require a more organic and self-generating program than we have yet put in place.

Specifically, broad and sustained adopting of the initial Framework and the expected modifications that will be made to address the ever evolving technical and threat vector environment are only practical if the target entities perceive the recommended steps are in their own economic self-interest.

Broad assertions of looming catastrophe have proven insufficient to this task, in part due to eth complicated, and poorly understood, characteristics of digital economics.

Instead, we need a much more concentrated and data supported effort to identify specifically which interventions are most likely to prove cost effective for defined target audiences. It is expected that there will also be instances where levels of security desired by the federal government for national interests may be higher and economically unsustainable for private entities focused on their commercial interests (as is appropriate under the laws governing public companies) In these cases economic incentives will need to be employed to assure the public interest of a broadly security digital infrastructure, just as market incentives have historically been provided to address other national interests such as in agriculture, transportation, and environment.

- 1) **Cost Effectiveness** -- The President's Executive Order, calling for the creation of the Framework by NIST and the private sector, outlined several criteria, which the framework must meet. While the current framework serves as a good starting point for organizations to begin assessing their approach to cyber security, there is still much that has not been done to ensure the framework meets the criteria called for in the President's Executive Order – specifically in relation to cost effectiveness. If the Framework was demonstrated to be cost-effective, as required by the Order, then awareness and its ultimate voluntary adoption could be expected on the part of most, if not all, reasonable owners and operators. Specifically, the President's Order stated that:

“The Cyber security Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach...” Section 7(b).

While NIST has received widespread praise for the openness of the process it used to construct the Framework, it has not (at least to date) met the criteria specified by the President that is detailed above. Indeed, some critics have claimed that the Framework fails to meet nearly all of the criteria for adequacy identified in the President's Order.ⁱⁱ Our focus here, however, is on the crucial area of cost-effectiveness.

Private sector operators (as well as government entities) routinely make security risk management decisions by including cost in their calculations. Indeed, independent research has consistently

demonstrated that cost is the single biggest factor in critical infrastructure cyber security decisions.^{iii, iv, v} No private sector entity can be expected to make uneconomic (i.e., non-cost-effective) security investments on a sustained basis.

As a result, the cost-effectiveness requirement in the President's Executive Order not only makes imminent sense, it is fundamental to the awareness and ultimate long-term success of voluntary adoption of the Framework.

The NIST Framework, as currently constructed, does not contain any analysis or data on the cost-effectiveness of potential implementation, either in whole or in part. Moreover, despite five nationwide workshops sponsored by NIST, each with multiple breakout sessions (and despite private sector representatives bringing the issue up constantly), there was not a single session at any workshop devoted to a serious analysis of this topic.^{vi}

- 2) **Case-Testing** -- ISA and entities as diverse as the Financial Services Sector Coordinating Council^{vii} and the California State Public Utilities Commission^{viii} initially called for a series of pilot, or "beta," tests, which would help clarify some of these outstanding issues on cost-effectiveness. While there has been no work to date on the part of NIST or the federal government to develop such a test, ISA believes a beta test could still be implemented amongst certain actors (including certain members of critical infrastructure who have not yet "adopted" the framework) and would constitute a significant advancement in the overall awareness of the framework and its ultimate voluntary adoption.

ISA suggested 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 proposed 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 would 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.

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 anticipated government and industry would 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 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.

Experiences Question 4: What expectations have not been met by the framework? Specifically, what about the framework is most helpful and why? What is least helpful and why?

- 1) **Conformity with established standards** – Rather than adopting existing language of cyber security risk management professionals, the Framework introduced the community to a new set of language, with tiers (instead of maturity models), categories and sub-categories (instead of controls and control-family). While we appreciate the thought that went into this model and the logical flow, for the sake of spurring wider adoption, reducing confusion, and conforming to international standards, we propose that the Framework employ language that is more universal in setting up the nomenclature.
- 2) **Gap Analysis** – Establishing tooling (similar to the C2M2) that aids organizations in understanding controls relevant to their risk profile, and then providing a way to conduct a gap assessment and closure would be very helpful.
- 3) **Accrediting independent assessors** – Establishing a process and accrediting companies that assess and certify organizations for their degree of adoption and maturity level as part of gaining access to a menu of incentives, would be helpful.
- 4) **ISO 27001** -- Adding ISO 27001 cross-references and gaps (as incorporated in Appendix H) are very helpful. These may require some effort to maintain the baselines, but we believe it will be well received by the international community, which is largely ISO oriented.

- 5) **FISMA** – Adding references to FISMA classifications into Framework appendix resources would also be very helpful to tie out minimum control requirements for applications and servers into the framework itself.
- 6) **Prioritization** -- As referenced above, the framework fails to meet the requirements for cost-effectiveness and prioritization called for in the President’s Executive Order. NIST’s potential audience for this document will not adopt/map/adhere to the Framework unless decision makers can be convinced that it will either make their lives easier or there is some value/advantage to doing so. Accordingly, there should be some thought around making it easy. This can be accomplished by prioritizing the controls and processes outlined in the framework core.

ISA suggested creating a new column for criticality to define the company’s relationship to critical infrastructure, which would also relate to section 9 of the EO 13636 dealing with the identification critical infrastructure at the greatest risk. Prioritizing the framework would make the document more useful for smaller organizations by saving them time and resources, which would otherwise be used on determining which areas of the framework to consider first. Additionally, prioritization would make the framework more usable for mature organizations (who adopted the controls specified in the framework long ago) that largely see the document as too daunting to begin applying the controls to their suppliers.

ISA has suggested using data, including, but not limited to, data from existing regimes, such as NIST 800-53, 2014 Verizon Data Breach Report, and SANS 20 Critical Security Controls, for high, medium and low priority rating. This rating will be updating annually based on threat data.

Criticality	Description
White	Critical Infrastructure at Greatest Risk, where a cyber security incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.
Red	Industry at High Risk (e.g., Defense, Financial, Energy,) that will impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety.
Yellow	Industry at Medium Risk will undermine State and local government capacities to maintain order and to deliver minimum essential public and services; damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services.
Green	Industry at Average Risk that will have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources.
Blue	Non-regulated Industries.

Experiences Question 8(c): Are organizations leveraging Section 3.5 of the Framework (“Methodology to Protect Privacy and Civil Liberties”) and, if so, what are their initial experiences? If organizations are not leveraging this methodology, why not?

Section 3.5 of the Framework was based on a proposal the Hogan Lovells law firm put forward as a more reasonable alternative to the privacy methodology included in the Preliminary Cybersecurity Framework, which was overbroad and in some cases went beyond what is required by US law. NIST dropped the originally proposed privacy methodology and adopted an approach similar to that recommended by Hogan Lovells.

Section 3.5 identifies a methodology for how an organization might consider privacy and civil liberties implications that may result from cybersecurity operations. ISA recommends that NIST conduct a systematic analysis of the experiences of a core group of target audiences with Section 3.5 to develop reliable information upon which to base future privacy methodology recommendations. Establishing this test group is consistent with ISA’s aforementioned recommendation in Awareness Question #1 which deals with the establishment of a group of target organizations for case testing The Framework.

ⁱ http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_IV_Working_Group_Descriptions_9_2_14.pdf

ⁱⁱ SANS. “SANS NewsBites – Volume XV, Issue: 69.” Newsletter. SANS, Aug. 2013. Web. 24 Jan. 2014.
<<http://www.sans.org/newsletters/newsbites/newsbites.php?vol=15&issue=69>>.

ⁱⁱⁱ PricewaterhouseCoopers. “The Global State of Information Security: 2008.” Rep. PricewaterhouseCoopers, 2007. Print.

^{iv} Baker, Stewart, Shaun Waterman, and George Ivanov. “In the Crossfire: Critical Infrastructure in the Age of Cyber War.” Rep. McAfee.com. McAfee, 2010. Web. 30 Apr. 2013.
<<http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf>>.

^v Domenici, Helen, and Afzal Bari. “The Price of Cybersecurity: Improvements Drive Steep Cost Curve.” Rep. Ponemon Institute-Bloomberg Government Study, 31 Jan. 2012. Print.

^{vi} Starting with workshop 1, final agendas for each workshop can be accessed through the following hyperlinks:
Workshop 1 Final Agenda: <<http://www.nist.gov/itl/csd/upload/CSF-April-3-FinalAgenda.pdf>>.
Workshop 2 Final Agenda: <http://www.nist.gov/itl/csd/upload/final_agenda_eo_cm_u_may29-31_2013.pdf>.
Workshop 3 Final Agenda:
<http://www.nist.gov/itl/csd/upload/3rd_cybersecurity_workshop_final_agenda.pdf>.
Workshop 4 Final Agenda: <http://www.nist.gov/itl/csd/upload/Framework_agenda_final_090613.pdf>.
Workshop 5 Final Agenda: <http://www.nist.gov/itl/csd/upload/5th-workshop_Framework-Agenda.pdf>.

^{vii} Financial Services Sector Coordinating Council. “Preliminary Cybersecurity Framework Comments.” Letter. NIST, Dec. 2013. Web. 24 Jan 2014.
<http://csrc.nist.gov/cyberframework/framework_comments/20131213_charles_blauner_fsscc.pdf>.

^{viii} California Public Utilities Commission. “Response to the National Institute of Standards and Technology, U.S. Department of Commerce, ‘Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework.’” Letter. NIST, Dec 2013. Web. 24 Jan. 2014.
<http://csrc.nist.gov/cyberframework/framework_comments/20131216_christopher_villarreal_cpuc.pdf>.