The Internet Security Alliance

Response to the

National Institute of Standards and Technology's Oct 29th, 2013 Request for Public Comment: "Preliminary Cybersecurity Framework"

December 13, 2013

Contact:
Larry Clinton, Internet Security Alliance (ISA) President & CEO
Phone: (703) 907-7090
Email: lclinton@isalliance.org or admin@isalliance.org
Web: www.isalliance.org

About the Internet Security Alliance (ISA):
ISA is a multi-sector trade association with membership from virtually every one of the designated critical industry sectors, including substantial participation from the aviation, banking, communications, defense, education, financial services, health care, insurance, manufacturing, security and technology industries. ISA focuses exclusively on cybersecurity and cybersecurity related issues as is embodied in its mission, which is to create a sustainable system of cybersecurity by combining advanced technology with economics and public policy.

Founded in 2000 in collaboration with Carnegie Mellon, ISA is also unique in that combines the thought leadership that might be found in a "think tank," with advocacy one would expect from a trade association, and operational security programs that might be found in a professional association.

I. Positive Aspects of the NIST Framework

1) It provides a good starting point around notions of cybersecurity maturity by using profile tiers.

2) The Framework has largely incorporated existing security measures that were suggested at the NIST sponsored workshops and through previous calls for submission, including the measures articulated in the Verizon-Secret Service "Data Breach Investigation Reports" as well as aspects of those articulated in the ISA-ANSI publications: "Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask" and the "Financial Management of Cyber Risk: An Implementation Framework for CFOs.".

3) It is headed in the direction of utilizing a risk management framework.

4) It is striving to develop a common lexicon for cybersecurity and cybersecurity maturity.

5) The functional categories of identify, protect, detect, respond, and recover are seemingly appropriate and they are appropriately not too prescriptive.

II. Where the Framework Needs Work – Principal Concerns

1) ***Framework Applicability*** – In reviewing the Framework, it is not entirely clear which types of organizations the document is intended to apply to. Is it solely applicable to critical infrastructure as the Executive Order directs and the introduction to the Preliminary Cybersecurity Framework seems to suggest? Or is it applicable to just a segment of the critical infrastructure, such as smaller, less mature organizations? Or is it applicable to all organizations that utilize cyber/information technology systems within their business operations as has been suggested by various governmental officers? It would be helpful for the Framework to state in its introductory paragraphs who the primary audience is intended to be for this document, the intended secondary audience, etc.

2) ***Cost-Effectiveness of NIST Framework Measures -*** There is no indication that these measures are cost-effective (and no analysis to that point) as directed by the Executive Order, and there is no analysis or assistance as to where to spend the next marginal dollar. Studies show that number one reason for poor cybersecurity in CI is cost. This could be accomplished with a priority rating discussed next.

3) ***Prioritization of NIST Framework Measures -*** There is also no prioritization amongst the measures provided.

- 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.
- Use data, including, but not limited to, data from existing regimes, such as NIST 800-53, Verizon Report, and SANS 20 Critical Security Controls, for high, medium and low priority rating. This rating will be updating annually based on threat data. We recommend that US-CERT be the office accountable for updating those priority ratings.

4) ***Beta Test Proposal*** - A great deal of effort has gone into designing a basic cybersecurity Framework. This Framework now deserves the same sort of systematic testing that any private sector entity would undertake prior to a releasing a new product or service. ISA recommends a systematic "Beta Testing" of the Framework.

When the Framework's design phase is complete, a new systematic testing phase ought to begin. Indeed, since the primary purpose of the Framework is to assist in securing critical infrastructure from potentially serious attacks, the need for the testing is, if anything, magnified.

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.

While the specific design of the testing will 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 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.

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 (see attached for more detail):

- 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.

However, the selected assessing entity must not have any current contractual obligations that might represent potential conflicts of interest.

Since the Framework is widely understood to be largely completed, the process of designing the testing procedure, identifying the representative sample participants and making plans for launching the tests can begin immediately and testing ought to be able to begin afterward. The length of the testing period ought to be jointly determined by the participating entities based on what is reasonably required to yield reliable and valid data as to success, costs, benefits and other metrics determined by the sector partnership process.

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.

The process being proposed here is markedly different, and far superior from both scientific and security perspectives, than what is currently being advocated by NIST and others in the government entities.

Currently, Government is suggesting that a group of, as yet unidentified, "early adopters" will step forward and publically declare that they are "adopting" (a currently undefined term) the Framework and will then provide "feedback." One option is that appropriate Governmental agencies or organizations ought to be "early adopters" of the Framework and also report to their appropriate oversight committees a metrics based cost-benefit analysis of

their implementation of the Framework, including the adaptability of their findings in government to the private sector as well as state and local governments. In terms of approximate costs and impact of adoption, a simple mapping like this could be useful:

- White House = Small Business
- HHS or Commerce = Medium Business
- DHS or DoD = Large Business

In addition to the troubling ambiguity as to what the Government's "early adopter" plan means or consists of, there are numerous other drawbacks to its proposal. To begin with, those companies that would step forward "early" after the Framework design is completed will logically be those for which "adoption" is easiest----quite likely the companies that long ago adopted many of the aspects of the framework independent of the NIST effort. As a result, these entities, many of which might be better characterized as "already adopters," are not the appropriate target audience for the Framework, since their behavior may well predate the existence of the Framework. Moreover, they are most likely companies with economies of scope and scale that permit high security investments. And, again, as such, they are not the true target of the framework from the point of view of increasing security behavior.

In addition, the "feedback" procedure is unspecified and unsystematic. Since this procedure does not require or facilitate any cost benefit analysis, this fundamental element of the President's EO will not be reliably tested. Since there is no mechanism in this process to deploy the incentives called for in the President's EO, there is no method to determine their effectiveness. And because this is a completely self-selected sample, there is no basis to believe that any feedback provided by these entities would not be politically motivated (many have already received personal urging directly from the President), entirely subjective, or in any way reliably determined.

Instead, ISA is proposing instead an organized, scientific process that utilizes the existing official partnership structure to systematically and independently determine key elements of the President's EO which are not achievable under the current government plans.

5) ***Cross-Sector Security Standards Identification –*** According to the Executive Order, the "Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure." In reviewing the Framework, it is not clear whether such an effort was undertaken to identify common controls to critical infrastructure. Was such an effort undertaken? And if it was undertaken, such cross-sector controls should be explicitly enumerated and used as the so-called "Framework Core"; sector coordinating councils (not NIST or DHS) could add additional controls that are more sector specific.

6) ***Changes to Framework Core*** - The following additions could be helpful in terms of conveying prioritization (Figure 1 at the end of the document):

- **Create a new Column:** Add a Column for Criticality to define the company's relationship to critical infrastructure. This would also relate to section 9 of the EO 13636.

Criticality	Description
White	Critical Infrastructure at Greatest Risk, where a cybersecurity 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.

- **Subcategory:** Since these are actually IT controls, the "subcategory" nomenclature should be discarded and the existing community terminology of "controls" should be utilized instead, with a definition that is listed in NIST 800-53, Rev 4.

- **Maturity Rating (Tiers):** Recommend using existing CMMI-style levels to rate maturity. Changes from tiers to "maturity rating." Assessment and characterization phase could be more robust.

- **Informative References:** This should include audit frameworks from current laws, regulations, and policies (LRPs). It will enable industry to see overlapping controls requirements for various LRPs and set a framework to consolidate audit criterion, and eventually reduce the amount of audits a company must have. This additionally will benefit with streamlining regulations.

7) ***The Critique that the Framework is too "IT/Ops" Focused, and Not Enterprise-Wide Should Be Addressed*** – The Framework seems more "IT/Ops" focused than providing any meaningful guidance to those in different roles, such as the General Counsel, CEO, Board of Directors, Human Resources, Communications Dept., etc.

- During past conversations, NIST stated that it had received feedback not to organize around or become prescriptive with respect to departmental roles and responsibilities. ISA agrees, but at a high level, there can be some endorsement for an enterprise-wide risk management model that calls for a cross-functional teams that cuts across the varying departments and silos of the organization (no matter what the size) so that cybersecurity risk is identified and analyzed through the widest possible lens. This notion should be explicitly stated, as some smaller entities may still be stuck in the "IT/Ops" only mindset. To address this concern, the following statement (or something similar could be added to the Risk Management Strategy Section:

> "Develop a risk management strategy that includes, among other things, the establishment of a cross-enterprise Cyber Risk Team that draws personnel from across the organization's different departments or functions. Such a team should be led by a senior executive (or Board Committee), or similar position that has cross-departmental authority, and should meet with appropriate and regular frequency."

8) ***Delete the Appendix B: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program" Contained within the October Draft of the Preliminary Cybersecurity Framework*** – The "Appendix B, Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program" ("Privacy Methodology") within the October "Preliminary Cybersecurity Framework" contains a prescriptive list of steps that are duplicative of other standards and policies

and, in fact, may conflict with other existing legal requirements. In addition, broadening the Privacy Methodology to include civil liberties (in addition to privacy) and "minimization" requirements may impose impractical burdens on private organizations that effectively operate as a "privacy tax," which in turn would quell a voluntary "adoption" of the Framework. Accordingly, Appendix B should be stricken from the Framework.

9) ***Definitions to Add to the Glossary Appendix, Appendix E*** – In terms of developing a common lexicon, there are a number of definitions that have been noticeably absent and should be included within the Glossary Appendix:

- Cybersecurity: Cybersecurity includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. (Whitehouse Cyberspace Policy Review 2009)
- Where do we define Cyber risk? How does cyber risk differentiate from business risk? Does this document cover all risk?
- Cyber risk, expressed as a function : Threat x Consequence x Vulnerability – Risk Transferred = Net Financial Risk
- Where do we define cyber activities (line 286)? How does this differ from regular IT operations?
- What are cybersecurity outcomes (lines 224 & 288)?
- Breach (as distinct from cybersecurity event – many people during the conferences were using the term to not only mean an initial intrusion, but data exfiltration as well; others, however, were using it to mean just an intrusion)
- Threat, Vulnerability, Consequence

10) ***International Concerns*** - Because of a lack of involvement from the international business community, it could be that this becomes a "U.S." document.

11) ***Include Discussion or List of Various Risk Response Possibilities*** - The document lacks a discussion within its risk management category describing the ways that an entity could respond to risk, i.e., whether you should mitigate the risk, plan for a contingency, transfer the risk through a mechanism such as insurance, avoid the risk, or accept the risk.

12) ***Third Parties and Interconnectivity*** – The document does not seem to adequately address third party/interconnectivity risk in that it doesn't ask the following questions: Have we addressed the risk posed by third-parties, vendors, etc., by drafting contracts that describe warranties and indemnities, which document the security measures in place, the required time to response, the backup/recovery procedures, the financial remedies, etc.

- Additionally, despite the provision of some granular controls, there is no call for third-party application testing, code review, or even software and OS patching/updating. This should be made explicit in some place.

III. Where the Framework Needs Work – Other Issues

1) Section 2.3 for Coordination should be further developed to explain the interaction with senior level executives. Recommended language is as follows;

   a. "Senior executives with cross-departmental authority, such as CEOs or owners, CFOs, etc.,must take strategic control, not operational control, of the cyber system that is the nerve center of their corporate operation. These executives must appreciate, or learn, if need be, the true role that technology plays in the modern organization, including the financial risks that technology places on the organization and the steps that must be taken to manage risk appropriately."

   b. "It is unrealistic to expect that senior executives would be able to determine all of the questions, let alone all of the answers, to the multiplicity of cyber issues that are generated within their organizations' various departments. Yet the financial importance of cybersecurity and its many ramifications means that senior executives cannot afford to delegate the subject entirely to specialists or to junior managers. This means that executives should take the step of forming and leading a Cyber Risk Team that can address cybersecurity from a strategic perspective. This team will need to obtain input from the affected stakeholders and relevant professionals, assess this input and feedback, and make key strategic decisions from an enterprise-wide perspective...The affected stakeholders should be drawn from [across the enterprise's different] departments or functions...."

2) As drafted, the Cybersecurity Framework calls for testing in updating in some, but not all, of the five functional areas. Rather than spelling out review, testing, and updating in a piecemeal fashion, perhaps it would be better to draw or mention that this process would be an entirely iterative process wherein all strategies, plans, etc., should be regularly reviewed, tested, and updated and inform one another in a dynamic fashion.

3) PR.IP-8 Indicates a desire to go back "online" immediately; this should be reconsidered because there are times when being down to investigate may be more appropriate from an overall security standpoint than rushing to get back "online." (e.g., Stuxnet).

   a. This could be addressed in the Identify section of the Framework, with this particular caution.

   b. Similarly this could be addressed in calling for a recovery/continuity plan that "defines emergency procedures, fallback procedures, temporary operational procedures, and resumption procedures."

4) As part of the Protect function, there should be some more discussion about how to recruit, teach, test, award/penalize, retain/let go of employees based on their cybersecurity behavior.

5) As part of the Identify function, there probably should be more of an explicit measure that asks the question(s): do we have policies (privacy or otherwise) in place, and, if so, are we following them?

6) Also under the Identify function, there perhaps should be a provision calling for a cost analysis of a potential cybersecurity event, including if the event is mishandled.

7) The document may also want to consider mentioning that for certain entities they should contemplate having a rapid response "Crisis Working Group" that includes representatives from "communications, IT, privacy, compliance, legal, investor relations, major business units impacted, human resources, and government affairs," that can be operational or at least available for contact 24/7.

8) The document should also consider a discussion of a layered defense (defense-in-depth) approach.

   a. "Given that the risk management processes are hampered by imprecision, and that IT security is by nature constantly evolving, organizations must create layered defenses to ensure critical data, systems,

and processes are protected by a defense-in-depth approach. Iterative risk assessments will reveal other defensive countermeasures that can serve to reduce further the probability of IT security incidents.[1]"

9) Further articulation on continuous process improvement (CPI) instead of having it defined in two separate functions, CPI should be throughout the core.

   a. "Cybersecurity is an ever-evolving field. Even with broad application of the program and suggestions herein, strong financial incentives still favor the attackers. Thus, organizations can expect new threats to emerge in an attempt to circumvent the defensive measures that they have put in place. Organizations will need to continuously monitor and improve upon their cybersecurity policies over time to maximize their security and, ultimately, their profitability.[2]"

10) This document lacks answering the question; "Where do we start?" There needs to a section addressing those businesses that are just setting foot into cybersecurity by including how to establish a baseline and set benchmarks.

11) Section 2.2 Framework Profile: This should be a *Risk Assessment* or benchmark risk assessment. The Target Profile would be a *Target Risk Maturity Level.* The intent of the Framework is to relate/frame cybersecurity into a "risk management" mindset. We believe this is where it starts. This profiling should be a risk assessment.

12) Add another appendix for list of references.

IV. Questions Going Forward

1) What does it mean to adopt the Framework as it relates to incentives and the voluntary program? Has that been further analyzed and coordinated with the DHS Integrated Task Force and White House team?
   a. How does a company qualify for an incentive?
   b. Can individual sectors (not regulated agencies) adjust the framework and still meet the qualification for incentives?
2) If there's an incident, will DHS or another government entity respond? Further articulate current government responsibilities in this area. What organizations already exist and where do they fall in responsibility?
3) Where is threat input and prevention included in the process?

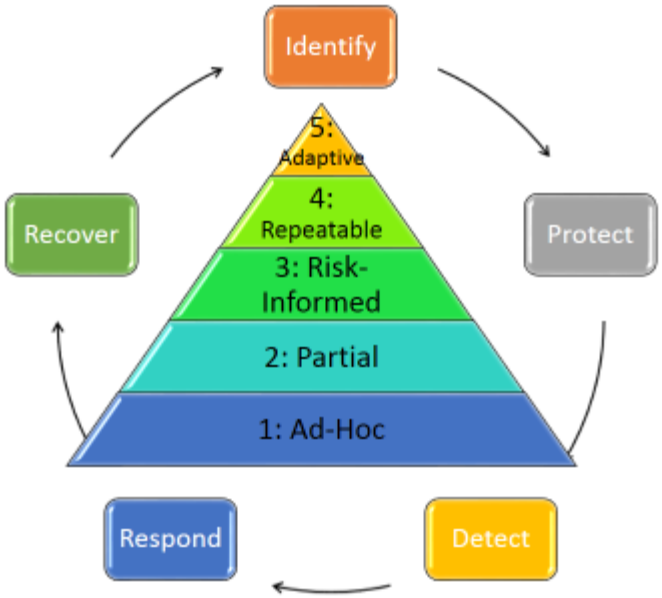
[1] Internet Security Alliance and American National Standards Institute. "The Financial Management of Cyber Risk: An Implementation Framework for CFOs." Rep. *ISAlliance.org.* ISA, 2010. Web. 13 Dec. 2013. <http://www.isalliance.org/isa-publications>.

[2] *Ibid.*

Figure 1: Depiction of Recommended Changes to Framework Core

Framework Core						
Crticality	Function	Category	Subcategory	Priority Rating	Maturity Rating	Informative References
White	Identify (ID)	Asset Management	IT Controls	High	CMU CMMI	Include Audit Criteria
Red		Business Environment		Med		PCI
Yellow		Governance		Low		FISMA
Green		Risk Assessment				GLBA
Blue		Risk Management				SOX
	Protect (PR)	Access Control				ISA
		Awareness and Training				ISO
		Data Security				Etc.
		Information Protection Processes and Procedures				
		Protective Technology				
	Detect (DE)	Anomalies and Events				
		Security Continuous Monitoring				
		Detection Processes				
	Respond (RS)	Communications				
		Analysis				
		Mitigation				
		Improvements				
	Recover (RC)	Recovery Planning				
		Improvements				
		Communications				

Figure 2: Recommended Revised Depiction of Cybersecurity Process



ISA recommends including this image, Figure 2, as a visual depiction of the cybersecurity framework process. The framework core is shown as a cyclical process in this diagram. The core isn't specific to any tier and should be a continuous process improvement.

The Ad-Hoc Maturity Level, Level 1, is the starting point for many organizations that are beginning to address cybersecurity. It is the foundational level and represents a security baseline of cybersecurity, wherein the bulk of the "man-effort" and investment takes place. It is the most labor and cost intensive tier.

As an organization's cybersecurity matures, as represented by movement upward up the tiered stack, the amount of "up front" expenditures in terms of personnel and dollars spent decreases. As the cybersecurity of the organization matures, it will advance to "Tier: 2 Partial." From there, consists of achieving "Tier 3: Risk-Informed," followed by "Tier 4: Repeatable," and ultimately "Tier 5: Adaptive."