Framework for Reducing Cyber Risks to Critical Infrastructure

On February 13, 2013, President Obama issued the Executive Order "Improving Critical Infrastructure Cybersecurity". The Executive Order tasks the Secretary of Commerce to direct the Director of the National Institute of Standards and Technology (NIST) to lead the development of a framework to reduce cyber risks to critical infrastructure. Consistent with existing NIST authorities, the Executive Order requires NIST to engage in an open public review and comment period.

NIST intends to issue a Request for Information (RFI) in the Federal Register to gather initial information on the many interrelated considerations, challenges, and efforts needed to develop the Framework.

To allow additional time for public review, a summary of the RFI is included below. Once the Federal Register publishes the RFI, this page will be updated with a link to the notice and additional information on how to submit information in response to the RFI. It is anticipated that the RFI will allow 45 days for responses to be submitted. If you have any questions, please contact NIST at cyberframework@nist.gov.

In accordance with the Executive Order, the Secretary of Commerce has directed the Director of the National Institute of Standards and Technology (the Director) to coordinate the development of a Framework to reduce the cyber risks to critical infrastructure. The Cybersecurity Framework will incorporate existing consensus-based standards to the fullest extent possible, consistent with requirements of the National Technology Transfer and Advancement Act of 1995[1], and guidance provided by Office of Management and Budget Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities."[2] Principles articulated in the Executive Office of the President memorandum M-12-08 "Principles for Federal Engagement in Standards Activities to Address National Priorities"[3] will be followed. The Framework should also be consistent with, and support the broad policy goals of, the Administration's 2010 "National Security Strategy", 2011 "Cyberspace Policy Review", "International Strategy for Cyberspace" of May 2010 and HSPD-7 "Critical Infrastructure Identification, Prioritization, and Protection".

The goals of the Framework development process will be: (i) to identify existing cybersecurity standards, guidelines, frameworks, and best practices that are applicable to increase the security of critical infrastructure sectors and other interested entities; (ii) to specify high-priority gaps for which new or revised standards are needed; and (iii) to collaboratively develop action plans by which these gaps can be addressed. It is contemplated that the development process will have requisite stages to allow for continuing engagement with the owners and operators, of critical infrastructure, and other industry, academic, and government stakeholders.

[1] Public Law 104-113(1996), codified in relevant part at 15 U.S.C. § 272(b).

[2] http://standards.gov/a119.cfm

[3] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08_1.pdf

In December 2011, the United States Government Accountability Office (GAO) issued a report titled “CRITICAL INFRASTRUCTURE PROTECTION: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use.”[4] In its report, GAO found similarities in cybersecurity guidance across sectors, and recommended promoting existing guidance to assist individual entities within a sector in “identifying the guidance that is most applicable and effective in improving their security posture.”[5]

[4] http://www.gao.gov/assets/590/587529.pdf

[5] *Id.*, at page 46.

[6] Organizational risk responses can include, for example, risk acceptance, risk rejection, risk mitigation, risk sharing, or risk transfer.

[7] Assessments determine whether the security controls selected by an organization are implemented correctly, operating as intended, and producing the desired results in order to enforce organizational security policies.

NIST believes the diversity of business and mission needs notwithstanding, there are core cybersecurity practices that can be identified and that will be applicable to a diversity of sectors and a spectrum of quickly evolving threats. Identifying such core practices will be a focus of the Framework development process.

In order to be effective in protecting the information and information systems that are a part of the U.S. critical infrastructure, NIST believes the Framework should have a number of general properties or characteristics. The Framework should include flexible, extensible, scalable, and technology-independent standards, guidelines, and best practices, that provide:

- A consultative process to assess the cybersecurity-related risks to organizational missions and business functions;
- A menu of management, operational, and technical security controls, including policies and processes, available to address a range of threats and protect privacy and civil liberties;
- A consultative process to identify the security controls that would adequately address risks[6] that have been assessed and to protect data and information being processed, stored, and transmitted by organizational information systems;
- Metrics, methods, and procedures that can be used to assess and monitor, on an ongoing or continuous basis, the effectiveness of security controls that are selected and deployed in organizational information systems and environments in which those systems operate and available processes that can be used to facilitate continuous improvement in such controls;[7]
- A comprehensive risk management approach that provides the ability to assess, respond to, and monitor information security-related risks and provide senior leaders/executives with the kinds of necessary information sets that help them to make ongoing risk-based decisions;
- A menu of privacy controls necessary to protect privacy and civil liberties.

Within eight months, NIST intends to publish for additional comment a draft Framework that clearly outlines areas of focus and provides preliminary lists of standards, guidelines and best practices that fall within that outline. The draft will also include initial conclusions for additional public comment. The draft Framework will build on NIST’s ongoing work with cybersecurity standards and guidelines for the Smart Grid, Identity Management, Federal Information Security Management Act (FISMA) implementation, the Electricity Subsector Cybersecurity Capability Maturity Model, and related projects.

NIST intends to engage with critical infrastructure stakeholders, through a voluntary consensus-based process, to develop the standards, guidelines and best practices that will comprise the Framework. This will include interactive workshops with industry and academia, along with other forms of outreach. NIST believes that the Framework cannot be static, but must be a living document that allows for ongoing consultation in order to address constantly evolving risks to critical infrastructure cybersecurity. A voluntary consensus standards-based approach will facilitate the ability of critical infrastructure owners and, operators to manage such risks, and to implement alternate solutions from the bottom up with interoperability, scalability, and reliability as key attributes.

A standards-based Framework will also help provide some of the measures necessary to understand the effectiveness of critical infrastructure protection, and track changes over time. DHS and Sector Specific Agencies will provide input in this area based on their engagement with sector stakeholders. This standards-based approach is necessary in order to be able to provide and analyze data from different sources that can directly support risk-based decision-making. A Framework without sufficient standards and associated conformity assessment programs could impede future innovation in security efforts for critical infrastructure by potentially creating a false sense of security.

The use of widely-accepted standards is also necessary to enable economies of scale and scope to help create competitive markets in which competition is driven by market need and products that meet that market need through combinations of price, quality, performance, and value to consumers. Market competition then promotes faster diffusion of these technologies and realization of many benefits throughout these sectors.

It is anticipated that the Framework will: (i) include consideration of sustainable approaches for assessing conformity to identified standards and guidelines; (ii) assist in the selection and development of an optimal conformity assessment approach; and (iii) facilitate the implementation of selected approach(es) that could cover technology varying in scope from individual devices or components to large-scale organizational operations. The decisions on the type, independence and technical rigor of these conformity assessment approaches should be risk-based. The need for confidence in conformity must be balanced with cost to the public and private sectors, including their international operations and legal obligations. Successful conformity assessment programs provide the needed level of confidence, are efficient and have a sustainable and scalable business case.

This RFI is looking for current adoption rates and related information for particular standards, guidelines, best practices, and frameworks to determine applicability throughout the critical infrastructure sectors. The RFI asks for stakeholders to submit ideas, based on their experience and mission/business needs, to assist in prioritizing the work of the Framework, as well as highlighting relevant performance needs of their respective sectors.

For the purposes of this notice and the Framework, the term “standards” and the phrase “standards setting” are used in a generic manner to include both standards development and conformity assessment development. In addition to critical infrastructure owners and operators, NIST invites federal agencies, state, local, territorial and tribal governments, standard-setting organizations,[8] other members of industry, consumers, solution providers, and other stakeholders to respond.

[8] As used herein, “standard-setting organizations” refers to the wide cross section of organizations that are involved in the development of standards and specifications, both domestically and abroad.

Request for Comment

The following questions cover the major areas about which NIST seeks comment. The questions are not intended to limit the topics that may be addressed. Responses may include any topic believed to have implications for the development of the Framework regardless of whether the topic is included in this document.

While the Framework will be focused on critical infrastructure, given the broad diversity of sectors that may include parts of critical infrastructure, the evolving nature of the classification of critical infrastructure based on risk, and the intention to involve a broad set of stakeholders in development of the Framework, the RFI will generally use the broader term “organizations” when seeking information.

Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials. Do not include in comments or otherwise submit proprietary or confidential information, as all comments received will be made available publically at http://csrc.nist.gov/.

Current Risk Management Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST’s goal of developing a Framework that includes and identifies common practices across sectors.

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

The greatest challenge that exists will center on the migration from the current ad-hoc infrastructure based Security Best Practices and compliance based programs, shifting to the paradigm of a threat and risk based approach for information and systems (contextual) criticality. The threat landscape has matured and continues to evolve. The tactics are more advanced, therefore the challenges lies with changing our tactics, strategies and even how we think about threats vectors, protections and remediation’s. There are many organizations that are not very good at communicating the value of this approach and the tangible results that can be attained when compared to the “book of security” that was written 15+ years ago.

Another method that presents challenges is the idea that Security by Compliance and checking the box on all of the compliance/regulatory requests make you secure. A progressive security posture based on Compliance and Regulatory obligations is not a Strategic Program; it is tactical at best and riddled with opportunities for missed steps and vulnerabilities. This is another educational component that limit forward movement for the paradigm shift.

Funding can be a challenge as well, but this can generally be overcome by being able to communicate the business value for enacting a better security program. In this value to communications should be aligned with business objections, shifting the mindset from cost center to enabler, and marketability of the program.

The lack luster perspective of most solution providers that agree it’s acceptable to have a patient zero,

because that's how we learn.
Management of the un-patchable, unknown and un manageable are other challenges, which will require systems / software manufactures to be more accountable to the quality, flexibility and scalability of products/solutions that are delivered to ensure it can take advantage of improvements of products, procedures and technologies. There are very little business aligned incentives to move from legacy to maturing solutions.

The focus for "critical infrastructure" is another inhibitor of progression, as the critical infrastructure is usually not self-contained and must interact with "non-critical infrastructure" classed components. I.e. you are only as strong as the weakest link in the chain.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?
One of the more visible challenges is centered on the willingness to share intelligence and the narrowed scope to Critical infrastructure only. This infrastructure is not self-contained and the standards may be marginally effective given they are centered on Hardware not the information and the path(s) and/or mechanisms by which the information travels.

3. Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?
The policies and procedures that govern risk involve threat modeling based on the stages by which an attacker would execute a threat; mapping and defining the controls based on the people, process and technology components. The discovery of the gaps will lead to a risk statement that is aligned with the business objectives, actors, and criticality of the information possessed/utilized/transmitted in the attack vector.

The policies are communicated by a guerilla marketing tactics, gamification/reward, and continued tactical testing exercises (red team exercise, advance threat simulations, penetration testing and table top exercise). The oversight is governed through executive steering committee meeting to discuss program effectiveness through metrics mapping to business enablement initiatives. Roles and responsibilities are clearly defined at this oversight level.

The procedures are developed using domain disciples (i.e. Architecture principles, complementary technology evaluations, policies follow-up/remediation activities) in conjunction core Security Control Disciplines (i.e. Access Management, Device Management/Control, Data Management/Security etc.)

4. Where do organizations locate their cyber security risk management program/office?

Organizations typically bury this function with the Information Technology Organization. Although, significant movement to identify a responsible person with in the role of a CSO/CISO is occurring; This role drives security posture improvements and security strategy. Security governance and information technology governance are typically in a maturation process. These processes are generally defined but not consistently applied. As these processes are applied they need to explicitly demonstrate value to the stakeholders (i.e. users and business) and involve degrees of transparency. Transparency in this context ideally describes the simplicity for user application and the business alignment for the proposed solution identifying business benefit and risk (threat) mitigation.

5. How do organizations define and assess risk generally and cyber security risk specifically? Generally,

organizations use compliance or regulatory mandates as a basis for defining risk. Again, very tactical to the system/applications etc. scoped by said regulation/compliance obligation. Risk is assessed by the deployment, and age of the technology, lack of policies, procedures and/or guidelines. There are disparate definitions of cyber-risk / cyber-intrusion therefore, it is organized in to the same risk process that exists or is executed on an ad-hoc basis due to reactive nature of the organization.

6. To what extent is cyber security risk incorporated into organizations' overarching enterprise risk management?
This is not common place as of yet. It is maturing, but generally enterprise risks are aligned with IT application controls in conjunction with associated systems. People, process and technology components for protection of electronic pathways, information management and information transport mechanisms rarely appear and if they do appear it is again aligned with a compliance or regulatory obligation. The alignment needs to be more encompassing identifying the value to thwart business risk (i.e. risk to brand, risk of distrust/unsecure, consumer churn, loss of assets) and then transition this paradigm to Threat Vector Identification, Detection, Analysis and Remediation tactics. These tactics combined with the other People, Process and technology components create the Security Strategy.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels? ISO 27001, PCI –DSS, SOX, COBIT, SANS 20 Controls, ITIL, HIPPA-HITECH, DATA Security Statutes (PI, PII)/Orders and organizational sponsored frameworks (i.e. SANS, OWASP, etc.)

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity? Data Breach Statutes for various states, On-line Protection Acts, Patriot Acts, GLBA, CALEA, HIPPA-HITECH, DATA Security Statutes (PI, PII)/Orders, and Organizational Sponsored frameworks.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors? SAS and IAS offerings, Payroll Services, Technological Innovations (medical monitors and dispensers), and Military Defense Technologies. Physical building and data center controls are applicable as well.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk? Most companies utilize their critical crisis plans, incident response plans, business continuity and/or disaster recovery plans to indicate/define acceptable operations criteria given this operation would be under duress. One common goal of all of these programs is to maintain critical systems availability and critical business processes even though operating in a degraded manner.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience? The report usually contains a summary of event details, summary of remediation, lessons learned, groups/team/business function/process affected and high-level timing for execution of remediation efforts. In rare cases in

place controls are reported/likelihood for exploitation and potential company exposure. The reporting experience has been inconsistent, from praise that control were effective to why didn't we do more.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?
I believe these organizations should be involved to ensure we are creating a framework that can be consistently applied and provide aggregation of information and represent it in a consistent context. This will keep conversations/applications relevant in hope of eliminated the "I'm special" or "unsure/doesn't apply to me" syndrome. The international conformity is a bit more complicated, as they (mutli-nationals) are more strict and explicit with their safe harbors, privacy laws/or lack of privacy than the United States at the moment. This will require more discussion.

Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. What additional approaches already exist?
Data Centric protection frameworks are emerging and not widely applied or adopted in Security Strategies. The traditional approaches utilize frame works for a combination of specifically scoped risk approaches and specifically scoped requirements from international and regulatory bodies such as the following: PCI-DSS, ITIL, COBIT, GLB, SOX, ISO, British Standards, OCTAVE, Data Security Statutes, Information Privacy Statutes, Breach Notification Regulations, Critical Infrastructure Questionnaires, Industry Best Practice Organizations (i.e. SANS, OWASP, CSI etc) and Industry Certification Organizations (CISA, CISSP, CSP). The large majority of the above do not apply a holistic view. This is specifically scope and not aligned with a comprehensive plan/strategy.

2. Which of these approaches apply across sectors?
British Standards, ISO, Data Security, ITIL, Industry Best Practice Organizations, Industry Certification Organizations, SOX generally, ISO, Breach and Privacy Statutes generally will be applied across sectors but they do not represent a holistic view and are not aligned with a comprehensive plan/strategy. Keep in mind PCI was implemented/created for a specific industry but many others have taken it on based on it's inclusion ins statutes and alike. It is also noteworthy that OWASP was a generic set of approaches that has been mapped to multiple industries and even legislation for privacy.

3. Which organizations use these approaches?
I would venture to say all organizations pepper these approach/standards through the tactics utilize to enforce and enact some level of Security disciple and governance. Just like business strategy the applications to security strategy and programs are not consistent and are in varying degrees across industry and company.

4. What, if any, are the limitations of using such approaches?
The limitations of these approaches are exploited by the following principals:

- The large majority of the above do not apply a holistic view. This is specifically scope and not aligned with a comprehensive plan/strategy.

- They don't address the migration from the current infrastructure based Security Best Practices, shifting to the paradigm of a risk based approach information criticality approach. The threat landscape has matured and continues to evolve. The tactics are more advanced, therefore the challenges lies with changing our tactics, strategies and even how we think about threats vectors, protections and remediation's.

5. What, if any, modifications could make these approaches more useful?
I would address development of a Security Strategy and define the comprehensive risk assessment

criteria and approach. This will further position for the change from Infrastructure Centric to Risk Based and Data Centric approaches with business alignment. This perspective for the advanced threat vector analysis will allow for common application based on the competencies of people, process and technology. This would make the approaches more useful and more measurable.
6. How do these approaches take into account sector-specific needs?
They do not address specific sector needs.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?
There should exists a baseline for standards, the first line of measurement, then specific industry items based on the standards development initiatives. Once this is achieved there are requirements for the baseline and co-developed industry components. Apply the controls to systems, applications, data etc.. Anything above and beyond previously mentioned would be voluntary.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?
Ensure normalization of the input has occurred in an effort to align a baseline, industry and above and beyond standards. They will also provide the body for organizing the periodic review of the standards and helping to call to order analysis of the threat vectors and landscape to ensure the approach remains relevant. Measurement analysis will also be correlated at the agencies as another mechanism for discerning effectiveness.

9. What other outreach efforts would be helpful?

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

Separation of business from operational systems;
• Use of encryption and key management;
• Identification and authorization of users accessing systems;
• Asset identification and management;
• Monitoring and incident detection tools and capabilities;
• Incident handling policies and procedures;
• Mission/system resiliency practices;
• Security engineering practices;
• Privacy and civil liberties protection.

1. Are these practices widely used throughout critical infrastructure and industry? I would say yes but in varying degrees of depth and implementation. I.e. some would say they have incident handling process and procedures, but they are rarely tested and may be written in a cumbersome way that does not match the “real world” handling of said incident.

2. How do these practices relate to existing international standards and practices? The domains are pretty consistent with the exception of Privacy and civil liberties protection. Privacy is definitely a concern, civil liberties are another matter. Some of the domain names may not exist but the components are embedded under other cap stone headings.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?
Separation of business from operational systems;
• Use of encryption and key management;
• Applications Security;
• Sound Architectural Principals and Execution;
• Identification and authorization of users accessing systems;
• Asset identification and management;
• Monitoring and incident detection tools and capabilities;
• Incident handling policies and procedures;
• Mission/system resiliency practices;
• Security engineering practices;
Technological Mechanics and Mechanisms (i.e. Components Vendors/Partners for Items consumed by Critical Infrastructure and alike.)

4. Are some of these practices not applicable for business or mission needs within particular sectors?

I would say they are all applicable and there are some missing. The domains of application security, organizational security (People and Process) and systems architecture for example are missing and should be considered.

5. Which of these practices pose the most significant implementation challenge?
They all have some unique challenges and depending on the maturity of the organization, and company philosophy the simplest domain could present the lion share of challenges. The other challenge may reside in the applicable of all to a business sector or industry vertical.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

Standards and guidelines are used to support/guide the implementation of the practices. The standards and guidelines act as the first line of governance and a means for communications for what is acceptable. It should also be noted that there is a hidden danger with this approach. The danger is realized through the implementation of the standard or guideline just as it is written and it tends to shift to a Compliance based implementation. It may lose the intended result as new threats are introduced, thus the shift to Compliance has been achieved; Compliance does not mean Security.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

Organizations generally have methodology and means for allocation of business resources. Whether they are proper or not can be argued. Most organizations process require you justify/sell/socialize why this funding in a lot of cases should be re-directed to fund this initiative. If a compelling case is sold and approved the resources are generally put behind to ensure creating and maintenance of these standards as they are seen as strategic moving forward and not tactical. Audits will programmatically occur to help provide additional assurance of resource allocations and effectiveness. We also view insurability will have somewhat of the same influences as Companies will be urged/required to purchase policies, in order to realized a favorable premium you will have to subscribe to standards and prove they are in place.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

Organizations tend to have escalation processes that occur organically and the formally process will need to be revised to align with the organic process and augment to ensure steps are handled appropriately. These risks more often than not will involve more than just the technical practitioners. We need our solution set to demonstrate machine automation, intelligence, and scale dynamically, executing an advanced set of algorithms and logic.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?
Privacy risks are summarized by the following: Information regarding the incident being disclosed inappropriately and the said incident being used negatively against the organization leading to further litigation and costly reporting.

The consistency of the application of these standards is subjective and how do you defend against it should something unfortunate occur. Will adopting these standards, and to what level of consistency, will be fiscally advantageous to us should be have a situation. How does it affect the companies' insurable status and stature? This position is closely aligned with question 7 above.

10. What are the international implications of this framework on your global business or in policymaking in other countries?
This framework will need to accepted by various international groups and ensure it aligns with their existing practices/laws/statutes. The framework will also have to be coordinated with other federal and multi-national alliances/taskforces/and committees for cyber security.

11. How should any risks to privacy and civil liberties be managed? I don't believe there is a one size fit all approach to this one. This one unfortunate has significant legal under tones and will require case by case management and interpretations of how the risk aligns with country / state expectation and if force majeure or whether negligence or gross negligence clauses were active. It may also require alignment of privy and civil liberties reporting.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?

The following core practice should be considered:

User Access and Entitlement Management
Comprehensive Risk Assessments
Threat Vector Modeling
Contactor/Agreement Modeling
Business Process Re-engineering/Review
Data Protection Practices for Risk Identification and Reduction
Threat and Vulnerability Management Practices
Metrics and KPI
Data Classification
Forensics
Policy Definition
Security Education/Measurement
Security/Risk/Technology Governance
The process / methodically that was utilized to synthesize/normalize the data generated by the RFI, this will serve as the mechanism for making additional updates/modifications.