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]

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

---

[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.

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.

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?

[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.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

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?

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

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

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?

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

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?

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

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?

2. Which of these approaches apply across sectors?

3. Which organizations use these approaches?

4. What, if any, are the limitations of using such approaches?

5. What, if any, modifications could make these approaches more useful?

6. How do these approaches take into account sector-specific needs?

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

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?

2. How do these practices relate to existing international standards and practices?

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

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

5. Which of these practices pose the most significant implementation challenge?

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

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

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

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

10. What are the international implications of this framework on your global business or in policymaking in other countries?

11. How should any risks to privacy and civil liberties be managed?

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