DRAFT Outline - Preliminary Framework to Reduce Cyber Risks to Critical Infrastructure, July 1, 2013

NOTES TO REVIEWERS:
This draft is produced for discussion purposes at the upcoming workshops and to further encourage private sector input before NIST publishes a preliminary Draft *Framework to Reduce Cyber Risks to Critical Infrastructure*, ("the Framework") for public comment in October.

In the process of establishing this Framework, some areas have been identified where more information is needed. These include the lack of standards, guidelines, and practices to address privacy and civil liberties issues, as well as the scarcity of helpful metrics for an organization's cybersecurity effectiveness. Suggestions in these areas would be particularly useful and will be incorporated into the Framework in the coming months.

The material is and will remain a work in progress; NIST welcomes comments and other input to this work. Italicized text below the heading discusses what content will be included within that section; in addition some sections include preliminary text.

Table of Contents

This section will contain a high-level table of contents (level 1 headings only) for the rest of the document:

Executive Overview

This section is tailored to senior executives as an abbreviated description of the purpose, need, and application of the Framework throughout critical infrastructure sectors. The section is specific for business leaders on how cybersecurity risks to critical infrastructures can be managed within the enterprise's broader risks and business plans and operations. This section will illustrate how organizations can evaluate how prepared they are to deal with potential cybersecurity-related impacts on their assets and ability to deliver products and services.[1]

[1] A few examples below show examples of existing references for discussion at upcoming workshops on creating and identifying material to communicate the business need for cybersecurity to business executives and gain awareness of cybersecurity issues. (Note: Links are to external web sites and information not endorsed by NIST): The Financial Management of Cyber Risk; DHS's Cybersecurity Questions for CEOs; What Every CEO Should Know About IT Security eBook; Business Roundtable Report.

This section will be designed to be a separate standalone document that can be used independently or with the rest of the Framework.

Document Summary

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. President Obama issued an Executive Order on February 12, 2013, to strengthen that infrastructure against cybersecurity threats.[2] In this order, the President directed the U.S. Commerce Department's National Institute of Standards and Technology (NIST) to lead coordination of a voluntary Cybersecurity Framework that would reduce cybersecurity risks to critical infrastructures, relying on private sector input and existing standards, guidelines, and practices.

The purpose of this document is to define the overall Framework and provide guidance on its usage. The primary audiences for the document and intended users of the Framework are critical infrastructure owners and operators and their partners. However, it is expected that many organizations facing cybersecurity challenges may benefit from adopting the Framework. The Framework is being designed to be relevant for organizations of nearly every size and composition.

This Framework is intended to be used throughout an entire organization – from the senior executives who oversee an organization to the officials and staff responsible for managing critical infrastructure systems and information technology resources.

The Framework includes:

- A section for senior executives and others on how this Framework can be used to evaluate how prepared they are to deal with potential cybersecurity-related impacts on their assets and on their ability to deliver products and services. By using this Framework, these senior executives can manage cybersecurity risks within their enterprise's broader risks and business plans and operations.
- A Framework user's guide to help organizations understand how to apply the Framework.
- The Framework's core structure:
  - Five major cybersecurity functions and their categories, subcategories, and informative references;
  - Three Framework Implementation Levels associated with an organization's cybersecurity functions and how well that organization implements the framework.
- A compendium of informative references, existing standards, guidelines, and practices to assist with specific implementation

How to Use This Framework

Many comments advised that the Cybersecurity Framework would not be effective unless the very senior levels of management of an organization were fully engaged and aware of the vulnerabilities and risks posed by cybersecurity threats – and committed to integrating cybersecurity risks into the enterprise's larger risk management approach. Time and again, comments reflected that these senior executives – including boards of directors – need to integrate and relate cybersecurity concerns and risks to critical infrastructure to the organization's basic business and its ability to deliver products and services. It is clear that these officials are

---

[2] Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*

best positioned to define and express accountability and responsibility, and to combine threat and vulnerability information with the potential impact to business needs and operational capabilities.

This section describes a concise way for senior executives and others to distill the fundamental concepts of the Framework so that they can assess their risks and how they are being managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. It explains how to use the Framework so that organizations can answer the fundamental question, "How are we doing?" Then, they can move in a more informed way to strengthen their cybersecurity using a risk-based approach.

The Framework should be considered and used as a guide rather than as a detailed manual. It is a way for executives, managers, and staff to:

- understand and assess the cybersecurity capabilities, readiness, and risks of their organization;
- identify areas of strength and weakness and aspects of cybersecurity on which they should productively focus, and learn what informative standards, guidelines, and practices are available and applicable to their organization.

By doing so, the Framework should assist an organization to align and integrate cybersecurity-related policies and plans, functions, and investments with the enterprise's overall risk management – particularly throughout the critical infrastructure sectors on which the national and economic security of the United States relies.

The Framework offers multiple ways to consider an organization's cybersecurity position: by each major cybersecurity function and its categories, subcategories, and informative references; and by the Framework Implementation Levels and key cybersecurity roles.

It is also expected that many organizations that already are productively and successfully using appropriate cybersecurity standards, guidelines, and practices – including those who contributed suggestions for inclusion in this document – will continue to achieve the goals described in the framework by using those tools.

Framework's Risk Management Approach

This section describes the Framework functions, categories, and subcategories and explains how they relate to risk management. The remainder of the section will describe the approach of Framework Implementation Levels for key cybersecurity roles and for functions.

Cybersecurity Functions:
The Framework offers a way to take a high-level, overarching view of an organization's management of cybersecurity risk by focusing on key *functions* of an organization's approach to this security: Know, Prevent, Detect, Respond, Recover. These are broken down further into categories. For instance, for Prevent, categories include: identity and access management, physical security, and training and awareness.

Categories, Subcategories, and Informative References of Standards, Practices, and Guidelines:
The Framework identifies underlying key categories and subcategories for each of these functions, and matches them with informative references such as existing standards, guidelines, and practices for each subcategory.

A matrix showing the functions, categories, subcategories, and informative references is provided.

A compendium of informative references that include standards, guidelines and best practices is provided as an initial data set to map to functions, categories, subcategories, and informative references.

The Framework's compendium points to many standards[3] – including performance and process-based standards. These are intended to be illustrative and to assist organizations in identifying and selecting standards for their own use. The compendium also offers practices and guidelines, including practical implementation guides.

These standards, guidelines, and practices are intended to be informative resources; they reflect the recommendations of the private-public partners who helped to develop this Framework. Each organization using this Framework will need to decide which of these match their relative threats, vulnerabilities, and risks as well as the resources available. The goal will be to provide appropriate performance in terms of cybersecurity protection in view of the organization's overall management of risk. If alternative standards, guidelines, and practices are used, organizations should be certain that they provide that level of expected performance. NIST is seeking comments on if these alternative standards, guidelines, and practices should be included in the compendium.

Cybersecurity Framework Implementation Levels:
The Framework provides three implementation levels that reflect organizational maturity in addressing cybersecurity by implementing the Framework. Users are offered an approach that rolls up functions and Framework Implementation Levels in a way that allows them to assess their organization's cybersecurity risk and readiness viewed through their specific roles and responsibilities – whether they are senior executives, business process managers, or operations managers. This provides a high-level indicator and measure of an organization's performance that can be assessed in terms of managing risk. Organizations that are part of the nation's critical infrastructure are then positioned to evaluate appropriate implementation levels. In developing this framework, it has been deemed likely that not all critical infrastructure organizations necessarily need to be at a particular level; that is a decision to be made by sector and organization.

DRAFT – Illustrative Framework Examples

This section contains illustrative examples that demonstrate the concepts described in the earlier sections.

Framework Development Process

This Framework is being developed through a private-public partnership, with a broad mix of companies, not-for-profit organizations, and government agencies across different sectors of our economy participating. They are participating via responses to public notices, discussion at workshops held around the country, direct communications, and comments on the preliminary Framework documents. This process is being conducted in a transparent, open, and collaborative way in which NIST is a convener and coordinator and managing the process, including providing this document based on initial analysis and private sector input to date.

The Framework is designed and intended:

- To be an adaptable, flexible, and scalable tool for voluntary use
- To assist in assessing, measuring, evaluating, and improving an organization's readiness to deal with cybersecurity risks
- To be actionable across an organization
- To be prioritized, flexible, repeatable, performance-based, and cost-effective

[3] It should be noted that NIST standards – which rely on public input during their development – are included when they have been identified by stakeholders in the development of this Framework.

- To rely on standards, methodologies, and processes that align with policy, business, and technological approaches to cybersecurity
- To complement rather than to conflict with current regulatory authorities
- To promote, rather than to constrain, technological innovation in this dynamic arena
- To focus on outcomes
- To raise awareness and appreciation for the challenges of cybersecurity but also the means for understanding and managing the related risks
- To be consistent with voluntary international standards

Conclusion

This section provides a brief conclusion for the document. This conclusion will summarize the major points of the publication, and it will also discuss next steps and future work plans (e.g., communicating that this is a living document that will evolve over time).

Glossary

This appendix defines selected terms used in the publication.

Acronyms

This appendix defines selected acronyms used in the publication.