Section 1 Current Risk Management Practices

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

Organizations see the following challenges in improving cybersecurity practices across critical infrastructure:

a) Costs to secure infrastructure
b) Access to actionable intelligence
c) Information sharing
d) External dependencies

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

A cross-sector standards-based framework for critical infrastructure may face the following challenges:

a) Each sector has its own unique characteristics. A cross-sector standards-based framework will need to be generic enough to be applicable broadly and at the same time be customizable for the different requirements of different sectors.

b) A cross-sector standards-based framework will need to include a mechanism to apply the standards based on the risk thresholds of the sector.

c) A cross-sector standards-based framework may face adoption challenges as some sectors may have standards tailored specifically for the sectors that are potentially more granular and as a result more effective and valuable for the sector.

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?

Our organization leverages national and international standards, frameworks, and best-practices to shape its policies and procedures governing risk generally and cybersecurity risk specifically. Examples of cybersecurity risk management standards and guidelines leveraged by our organization include, but are not limited to ISO, NIST, ISACA, etc.

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

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

Organizations define and assess risk generally and cybersecurity risk specifically using international and national risk management standards and guidelines. . Examples of cybersecurity risk management standards and guidelines leveraged by our organization include, but are not limited to ISO, NIST, ISACA, etc.

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

People, processes and technology are all factored in overarching enterprise risk management activities.

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

Examples of cybersecurity risk management standards and guidelines leveraged by our organization include, but are not limited to ISO, NIST, ISACA, etc. Our organization drives for compliant and secure environments. Our approach is to adjust our control choice, design and implementation based on the applicable risk thresholds.

As a professional services organization, our organization uses numerous sector specific standards, guidelines, best practices, and tools to understand, measure, and manage risk at the management, operational, and technical levels of the critical infrastructure asset owners and operators. For example, for our electricity subsector clients, our organization leverages NERC Reliability and CIP standards, ES-C2M2, RMP, 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?

Our organization’s current regulatory reporting relating to cybersecurity includes FISMA, SOX, TBD, etc.

As a professional services firm, our organization assists clients in meeting sector specific cybersecurity regulatory requirements. Specific examples include NERC CIP within the electricity subsector, CFATS within the chemical sector, etc.

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?

Our organization leverages national and international standards, frameworks, and best-practices to shape its performance goals for managing cybersecurity risk. Examples of cybersecurity risk management standards and guidelines leveraged by our organization include, but are not limited to ISO, NIST, ISACA, etc.

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?

Conformity assessment needs to be addressed on a sector by sector basis. Organizations may be capable of engaging in self-assessment, facilitated self-assessments or third-party independent assessments. Where regulatory assessments are deemed necessary the risks to national security, criteria, process, costs, and incentives should be carefully analyzed with public-private collaboration.

Section 2 Use of Frameworks, Standards, Guidelines, and Best Practices

1. What additional approaches already exist?

As a professional services firm, our organization assists clients with their sector specific cybersecurity standards and best practices. These vary from sector to sector (e.g. CFATS, NERC CIP).

2. Which of these approaches apply across sectors?

Many sector specific approaches can be tailored according to the unique characteristics and needs of other sectors. The NIST guidelines are a good example of practices that can be tailored 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?

a) Standards and frameworks may be more useful if used with a risk-based approach.

b) Standards and frameworks may be subject to interpretation. Organizations benefit if these approaches are accompanied with guidance, mentoring, and facilitation.

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

Some approaches address sector specific needs. For example, CFATS addresses risks from different quantities of Chemicals of Interest, whereas DOE RMP addresses risks from both IT and OT which is an attribute of the electricity subsector.

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

Yes, sector specific development processes and voluntary programs will ensure sector-specific needs are addressed without regulatory burden.

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

Sector-specific agencies (SSA) and related sector coordinating councils (SCC) can facilitate public-private collaboration especially with respect to identifying and addressing the unique characteristics of their sector.

9. What other outreach efforts would be helpful?

NIST can leverage social media, speaking engagements, and C-level leadership engagement to facilitate outreach.

Section 3   Specific Industry Practices

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?

Adoption of above-listed practices varies according to the organization's nature, size, resources, goals, and compliance mandates.

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?

It is important to note that organizations may view practices prescribed by regulators as critical relative to other best practices that may from a risk-based perspective be equally important. Such situations may result in compliant but relatively insecure environments.

Our organization believes that a baseline implementation of the above-listed practices is generally necessary for a critical infrastructure organization. However, based on the fact that each organization has its unique characteristics and risks, the importance of implementing some practices (beyond the baseline implementation) varies across different organizations.

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

It is possible that based on the unique characteristics and risks of an organization, some of these practices may not be applicable for its business or mission needs. However, generally, a baseline implementation of the above-listed practices is needed to improve the cybersecurity posture of a critical infrastructure organization.

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

Practices that require substantial monetary investments, understanding of new technologies, and instituting cultural changes are the most challenging for organizations.

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?

Existence of methodology for proper allocation of business resources varies from sector to sector and depends on size and other functions of the organization. For example, our organization has resources dedicated to creating and maintaining 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?

People, processes and technologies facilitating the application of these practices may pose risks such as:

a) unauthorized use or retention of data;
b) inadequate notice;
c) problems with consent;
d) lack of consumers access to data;
e) inadequate controls to ensure integrity of data; and
f) lack of redress procedures

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

This will depend on the breadth and scope of the framework.

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

Risks to privacy and civil liberties should be managed in accordance with existing laws and best-practices (e.g. Federal Trade Commission’s Fair Information Practice Principles (FIPs), Privacy Act of 1974, Children’s Online Privacy Protection Act (COPPA), Gramm-Leach-Bliley Act (GLB), Health Insurance Portability and Accountability Act (HIPAA), etc).

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

The federal government should leverage practices identified in existing standards, guidelines, and assessment tools in shaping a new framework. The framework should also account for existing compliance mandates and interdependencies across sectors.