Response to NIST RFI

Section 1 – Current Risk Management Practices

1. *What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?* The greatest challenge will be preventing multiple sets of Standards for critical infrastructure entities to follow, especially if some of those Standards are created by groups unfamiliar with a given sector.
2. *What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?* The greatest challenge will be preventing multiple sets of Standards for critical infrastructure entities to follow, especially if some of those Standards are created by groups unfamiliar with a given sector.
3. No answer provided.
4. No answer provided.
5. No answer provided.
6. No answer provided.
7. No answer provided.
8. *What are the current regulatory and regulatory reporting requirements in the U.S. for organizations relating to cybersecurity?* Currently, the electric industry is governed by FERC approved and mandated NERC Standards/Requirements related to Cyber Security. These Standards are subject to ongoing compliance and enforcement action.
9. *What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?* The electric industry critical assets are interdependent with other critical physical and information infrastructures, including telecommunications, energy, financial services, and transportation sectors
10. No answer provided.
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?* Currently, our organization only reports to NERC regarding Cybersecurity.
12. No answer provided.

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

1. *What additional approaches already exist?* Currently, the electric industry is governed by FERC approved and mandated NERC Standards/Requirements related to Cyber Security.
2. *Which of these approaches apply across sectors?* These FERC approved and mandated NERC Standards/Requirements related to Cyber Security apply only to the electric industry.
3. *Which organizations use these approaches?* NERC has criteria regarding which organizations have to comply with these NERC Standards/Requirements related to Cyber Security. Generally, these criteria require all entities connected to the Bulk Electric System at greater than 100Kv to comply with these NERC Standards/Requirements related to Cyber Security. Additionally, further criteria are used to determine which specific components of these organizations are required to comply.
4. *What, if any, are the limitations of using such approaches?* These NERC Standards/Requirements related to Cyber Security were developed and approved by the electric industry and apply only to the electric industry. We are not aware of any limitations of this approach.
5. *What, if any, modifications could make these approaches more useful?* These NERC Standards/Requirements related to Cyber Security were developed and approved by the electric industry and apply only to the electric industry. We are not aware of any modifications that could be made to this approach to make it more useful. However, one concern we have is if an additional approach is developed requiring the electric industry to follow multiple approaches.
6. *How do these approaches take into account sector-specific needs?* These NERC Standards/Requirements related to Cyber Security were developed and approved by the electric industry and apply only to the electric industry. The combination of the Standard/Requirement drafting team and industry incorporated sector-specific knowledge and needs.
7. *When using an existing framework, should there be a related sector-specific standards development process or voluntary program?* It is not clear what is meant by voluntary program. However, I believe a sector-specific development process is needed to cover the unique aspects of each sector.
8. *What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?* In the electric industry, NERC serves this role. They serve as the responsible entity driving Standard development as well as the overall compliance and enforcement responsibility through their designated regional entities.
9. *What other outreach efforts would be helpful?* Unsure; however, keep it simple. Having multiple agencies creating Standards is discouraged. Critical entities should only have to follow one set of Standards.

Section 3 – Specific Industry Practices

1. *Are these practices widely used throughout critical infrastructure and industry?* Most of the above listed items are common practice for us. Key among those would be "Separation of business from operational systems"; "Identification and authorization of users accessing systems"; "Asset identification and management"; "Monitoring and incident detection tools and capabilities"; "Security engineering practices".
2. *How do these practices relate to existing international standards and practices?* We comply with the NERC standards/requirements which attempt to address some of the above listed practices. The NERC standards do not include all of these components; however, we also utilize some of these as security engineering best practices.

3. *Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?* No answer provided.
4. *Are some of these practices not applicable for business or mission needs within particular sectors?* For us, "Use of encryption and key management" within a private network does little to enhance the overall security posture because most of the other listed practices are followed. The encryption portion of this practice becomes critical if data traverses a public network.
5. *Which of these practices pose the most significant implementation challenge?* Encryption and key management on internal systems. Externally, this is common practice.
6. *How are standards or guidelines utilized by organizations in the implementation of these practices?* If these practices are addressed in a standard (such as NERC standards / requirements), they are implemented per the requirement. Otherwise, they are weighed against risk and benefit.
7. *Do organizations have a methodology in place for the proper allocation of business resources to invest in, create and maintain IT standards?* We have a dedicated IT staff and budget in place with an enterprise IT Security department. Our IT department reports up through the CIO to the CAO.
8. *Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity*? We have an incident response procedure and a cyber sabotage policy.
9. *What risks to privacy and civil liberties do commenters perceive in the application of these practices?* No answer provided.
10. *What are the international implications of this Framework on your global business or in policymaking in other countries?* We do not operate internationally.
11. *How should any risks to privacy and civil liberties be managed?* No answer provided.
12. *In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?* No answer provided.