Comments Of The Edison Electric Institute

On The National Institute Of Standards And Technology ("NIST") Request For Information On Evaluating And Improving NIST Cybersecurity Resources: The Cybersecurity Framework And Cybersecurity Supply Chain Risk Management

Docket No. 220210-0045

The Edison Electric Institute ("EEI") submits the following comments responding to the National Institute of Standards and Technology ("NIST") request for information to assist in evaluating and improving its cybersecurity resources, including the "Framework for Improving Critical Infrastructure Cybersecurity" (the "CSF") and a variety of existing and potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains published in the Federal Register on Tuesday, February 22, 2022.[1]

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for about 220 million Americans and operate in all 50 states and the District of Columbia. Collectively, the electric power industry supports more than 7 million jobs in communities across the United States.

Protecting the North American electric grid and ensuring a reliable supply of power is a top priority for EEI members. Given that the industry has found common cause to work together to secure our shared infrastructure and work closely with government partners to understand the threat environment to better protect our systems, we welcome the opportunity to comment on the CSF.

EEI members are supportive of NIST updating the CSF to incorporate changes to the cybersecurity landscape as long as the foundational structure of the CSF remains intact. EEI also

[1] *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*, 87 Fed. Reg. 9579 (2022) ("RFI").

requests NIST's continued coordination with government agencies, expansion of its resources to guide coordination with vendors, contract language, and software bills of material elements.

I. COMMENTS

A. Use of the NIST Cybersecurity Framework

1. The Five Functions of the CSF Are Useful For Aiding in Organizing Cybersecurity Efforts, Actively Managing Risks, and Assessing Project Work Alignment

NIST requests feedback on the usefulness of the CSF for aiding companies in organizing cybersecurity efforts and actively managing risks through the CSF's Five Functions ("Five Functions"): Identify, Protect, Detect, Respond, and Recover. EEI members have found that the CSF has facilitated more comprehensive and mature, enterprise-wide approaches to cybersecurity. The CSF continues to be a beneficial guide that is flexible and widely used throughout organizations because it is written in a universal language and allows organizations to easily refine and develop their internal cybersecurity strategies and policies.

With respect to the Five Functions, EEI members have found it helpful to align project work to a Function category and underlying strategy. From a financial perspective, this alignment is beneficial for organizations to further assess investment decisions and the maturity level of a particular category. Use of the Five Functions continues to be effective in managing risks and could be implemented along with most organizations' cybersecurity efforts.

2. The Flexibility and Non-Prescriptive Nature of the CSF Allows for Improved Communications Within and Between Organizations and Entities

NIST seeks input on the current benefits of using the CSF. Specifically, NIST asks:

> (1) are communications improved within and between organizations and entities; (2) does the CSF allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks; and (3) what might be relevant metrics for

improvements to cybersecurity as a result of implementation of the CSF?[2]

The CSF is written in a universal, commonly used language that most business units can understand, requiring the less frequent need for subject matter experts ("SMEs"). Consequently, this helps improve internal communications and aligns expectations between organizations and people of various technical backgrounds. The flexibility of the CSF is also beneficial to organizations. It aids in addressing risk because it identifies issues and scope but is not prescriptive on how an organization could respond to a potential cybersecurity incident. The CSF also details risk mitigation strategies, the type of equipment in place, and its use, which is important to allow sufficient flexibility in addressing risk appropriately to specific facts and circumstances. While risk profiles could vary significantly across organizations, the flexibility inherent in the CSF remains applicable across various risk appetites.

EEI recommends that the collection of metrics for improvements to cybersecurity as a result of the implementation of the CSF be considered in other risk management resources as they may present unintended compliance challenges. Given that the CSF is intended to be guidance, the collection of metrics on the alignment to the CSF is unwarranted without a meaningful rationale and material benefit for using metrics. As previously mentioned, the foundational characteristics of the CSF are that it remains a voluntary guide and is not prescriptive. The addition of metrics into the CSF might have the unintended consequence of discouraging organizations and entities from using the tool due to concerns related to the perception that the CSF could become part of a larger regulatory construct. Therefore, it would be counterproductive to add metrics to a highly successful framework with unintended consequences, such as an organization's nonuse because of the presence of metrics.

[2] *Id.* at 9580.

3. Additional Getting Started Guidance Could Assist Entities More Efficiently Implement the CSF

NIST seeks feedback on whether any features of the CSF should be changed, added, or removed. There is potential for confusion with the vast number of resources NIST provides, including the CSF, the Special Publications, and the Informative References. EEI members recommend that NIST considers creating additional comprehensive getting started guidance or templates on implementation to assist entities more efficiently implement the CSF and other cybersecurity resources. Similarly, a "CSF 101" or "How To" training with simplified explanations, tailored by industry and sector, would be helpful for organizations in better understanding their risk profile, determining appropriate implementation tiers, and developing playbooks and tabletop exercises. Additional getting started guidance on effective implementation of the CSF could help educate those impacted by its adoption and make implementation more manageable.

4. The Modification or Change of the Structure of the CSF Could Have Potentially Significant Cascading Impacts on Many Organizations' Internal Procedures

NIST asks for input on the impact on the usability and backward compatibility of the CSF if the structure is modified or changed. EEI members support NIST's updating the CSF to account for the changing landscape of cybersecurity risks, technologies, and resources as long as the foundation of the CSF remains. Although the CSF is intended to be voluntary guidance, many organizations are committed to aligning with it and implementing significant elements of the CSF into their operational models. For organizations that have chosen to build their programs in alignment with the CSF, there could be overarching changes that could prompt potentially significant revisions and financial costs by those organizations. Such efforts to revise the internal

process to comport to new versions of the CSF could require a diversion of already scarce resources from ongoing tasks.

EEI members emphasize that the Five Functions are timeless and can accommodate changes in technology and landscape. Maintaining the flexibility and high level of the CSF will be critical to allow organizations to continue to implement it and scale into their programs.

5. Additional Guidance on Assessment or Maturity Model Mapping Could Improve the Usefulness of the CSF

NIST seeks information on additional ways to improve the CSF to make it more useful. EEI members recommend additional guidance on assessment or maturity model mapping to the CSF to improve the usefulness of the CSF because it could be valuable to show the relationships between NIST guidance and other materials produced by government agencies. Cybersecurity efforts are becoming and will continue to become duplicative without a clear relationship path or hierarchy. EEI members are subject to supply chain regulations and adhere to a variety of cybersecurity standards. It can seem like there are many potentially duplicative supply chain efforts. Maintaining harmony between the CSF, cybersecurity guidance, and existing mandatory standards will be important to sustaining the use of the CSF by the industry. An example of a potentially duplicative supply chain effort is the CISA Common Baseline Industrial Control Systems Performance Goals which identified nine categories of recommended cybersecurity practices as the foundation for preliminary control system cybersecurity performance goals that did not align with the CSF.[3] Under the Strengthening American Cybersecurity Act, critical infrastructure owners and operators are required to report to the Cybersecurity and Infrastructure Security Agency ("CISA") within 72 hours if they experience a substantial cyber attack, and if

[3] *Critical Infrastructure Control Systems Cybersecurity Performance Goals and Objectives* (Sept. 21, 2021), https://www.cisa.gov/control-systems-goals-and-objectives.

they make a ransomware payment to report within 24 hours.[4] Additional guidance on assessment or maturity model mapping will give organizations a better understanding of the value of the gaps being filled by the changes to the CSF and whether these changes will cause a strain on company resources.

B. Cybersecurity Supply Chain Risk Management

1. The National Initiative for Improving Cybersecurity in Supply Chain ("NIICS") Could Address Vendor and Software Management Challenges By Building on the Current Bill of Materials Work to Increase Trust and Assurance in Technology Products, Devices, And Services

NIST seeks feedback on the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address. The NIICS is a public-private partnership initiative created by NIST to address cybersecurity risks in the supply chain. Specifically, NIST asks now it can build on its current work on supply chain security, including software security work stemming from the Executive Order 14028, to increase trust and assurance in technology products, devices, and services.[5] Vendor and software management continue to be the greatest challenges that the NIICS could address. To that end, EEI recommends that NIST build on the current work on the minimum elements for a software bill of materials ("SBOM").

EEI members have vendor relationships spanning over several years and resetting vendor expectations has been one of the biggest challenges. Previous contracts contain language that may be insufficient because it does not align with cybersecurity requirements or does not have contract terms to support evolving industry practices, procurement considerations, resellers'

[4] S.3600 - 117th Congress (2021-2022): Strengthening American Cybersecurity Act of 2022, S.3600, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/senate-bill/3600.

[5] *Id.*at 9581.

responsibilities, or SBOM. Depending on the type of contract or business model within a complex supply chain, there are many different players, including the original equipment manufacturer, distributor, installer, integrator, and other third parties. Previous contract language did not address the responsibilities and obligations of each player, causing uncertainty and privity concerns as it relates to providing SBOMs. When asked to provide an additional level of information as it relates to the SBOM, hardware bill of materials, and software as a service ("SaaS") bill of materials, the vendor response can be unpredictable. Some vendors are not used to providing such a level of detail to their customers, usually due to resource constraints, while other vendors have the resources to provide many or most elements of their software components. Additionally, EEI members may experience difficulty in determining how to efficiently consume, view, and prioritize SBOMs across a vast inventory of installed components. The NIICS could reset the understanding and expectations of vendors by building on the current minimum elements for an SBOM work to provide prioritization and risk-based guidance on updated contract language and guide certification procedures for vendors and software to promote better cybersecurity practices.

2. Continued Coordination and Sharing of Lessons Learned With Appropriate Government Agencies and Vendors Following Cyber Events Could Mature Supply Chain Practices Across the Industry

NIST seeks input on the approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains that may be useful that can be utilized more broadly, potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, stakeholders, and extremely difficult areas. Communication and coordination among entities in the government are critical in efforts to prepare for and respond to potential threats to critical infrastructure. The vendor community may not have the

same opportunity for coordination. The cybersecurity programs and internal procedures of the vendor community could be further strengthened by also receiving lessons learned following cybersecurity events. Similarly, the continued coordination of NIST with other government partners to ensure appropriate cybersecurity alignments exist within the CSF and other materials is valuable to the industry. NIST could also consider harmonizing with cyber incident reporting requirements and standards including, the reporting requirements to CISA under the Strengthening American Cybersecurity Act and the CISA Common Baseline Industrial Control Systems Performance Goals. The continued coordination by NIST with the appropriate agencies to ensure the sharing of lessons learned following cybersecurity events with organizations and vendors could minimize duplication, aid in awareness, and mature supply chain practices across the industry.

3. NIST Guidance Can Be Further Improved by Addressing Life Cycle and Enterprise Usage in Open-Source Software

NIST seeks feedback on whether there are observed gaps in the existing cybersecurity supply chain risk management guidance and resources as they apply to information and communications technology, operational technology, IoT, and industrial IoT. Additionally, NIST asks whether these resources appropriately address cybersecurity challenges associated with open-source software and if there are additional approaches, tools, standards, guidelines, or other resources that NIST should consider achieving greater assurance throughout the software supply chain. The NIST Open Source Software ("OSS") code portal allows users to search and explore open source software developed by NIST and affiliated code collaborators. However, the code portal may not currently adequately address the OSS lifecycle and enterprise usage**.** The OSS code portal could be further improved by adding a page dedicated to and expanding on OSS lifecycle and enterprise usage.

4. Expanding The Supply Chain Risk Management Category and Creation of Contract Terms Beyond the Identify Function Could Be Valuable

NIST asks for information on how cybersecurity supply chain risk management considerations might be further integrated into an updated CSF, and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately developed.[6] Although the CSF's first Function, Identify, lists Supply Chain Risk Management as a category, EEI recommends that the category be extended to be included in the Protect and Detect categories because the process of supply chain risk management should not end at identification, given it is a continuous process. As previously mentioned, vendor and software management continue to be the greatest challenges because existing contract language may not align with cybersecurity requirements or may not support evolving industry practices. An extended Supply Chain Risk Management category will aid in resetting the understanding and expectations of vendors.

II. CONCLUSION

EEI appreciates the opportunity to share insights into and experiences with the CSF. As explained above, we support NIST updating the CSF to incorporate the changes to the cybersecurity landscape in terms of threats, capabilities, technologies, education, and workforce, the availability of resources to help organizations to better manage cybersecurity risk, and NIST's focus on increased awareness of and emphasis on cybersecurity risks in supply chains. EEI members ask NIST to consider that major changes to the structure of the CSF could have potentially significant cascading impacts on many organizations' internal strategies and procedures.

[6] *Id.*