Comments Of The Edison Electric Institute

On The National Institute Of Standards And Technology ("NIST") Request For Information On Evaluating And Improving NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

The Edison Electric Institute ("EEI") submits the following comments responding to the National Institute of Standards and Technology ("NIST") request for additional input and direction of the Cybersecurity Framework ("CSF" or "Framework") prior to crafting a draft of CSF 2.0, with potential significant changes to the CSF detailed in the "NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework" ("Concept Paper") published on January 19, 2023.

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for more than 235 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. In addition to our U.S. members, EEI has more than 65 international electric companies with operations in more than 90 countries, as International Members, and hundreds of industry suppliers and related organizations as Associate Members.

EEI supports updating the Framework to reflect changes in the cybersecurity landscape, such as the inclusion of a Govern Function, provided the foundational elements of the Framework remains consistent, flexible, and scalable. EEI members support of the expansion of the supply chain risk management concepts to reflect its importance throughout the Framework Functions, but caution NIST to carefully consider the potential unintended consequences of developing and incorporating metrics and measurements into the Framework. EEI also requests NIST's continued attention to the detailed input it received in response to the 2022 "Request for

Information On Evaluating And Improving NIST Cybersecurity Resources" as it makes further changes to the CSF.

I. COMMENTS

NIST requests additional input on the structure and direction of the CSF prior to drafting CSF 2.0. Specifically, NIST requests feedback on the following potential changes detailed in its Concept Paper: if the proposed changes reflect the current cybersecurity landscape; if the proposed changes are sufficient and appropriate; if there are other elements that should be considered under each area; if the proposed changes support different use cases in various sectors, types and sizes of organizations; if there are additional changes not covered that should be considered, if proposed changes would affect continued adoption of the Framework; and for those not using the Framework, if the proposed changes would affect the potential use of the Framework. EEI members support reviewing and updating the NIST CSF to reflect changes to the cybersecurity landscape, as illustrated in the EEI response to the 2022 "Request for Information On Evaluating And Improving NIST Cybersecurity Resources," and appreciate the opportunity to provide further input into this effort.

SECTION 1: "CSF 2.0 will explicitly recognize the CSF's broad use to clarify its potential applications"

NIST seeks to broaden use of the Cybersecurity Framework, and ensure that it is helpful to organizations regardless of sector, type, or size. The CSF continues to be a beneficial guide that is widely used throughout critical infrastructure organizations, and reviewing the Framework for broader applicability will enhance its existing value. Its flexibility and outcome-driven approach allow organizations to easily refine and develop their internal cybersecurity strategies and policies to address cybersecurity risk. The flexibility of the CSF also ensures its applicability across a variety of risk profiles and risk appetites, and allows users to take a risk-based approach in implementing mitigation strategies dependent on the specific circumstances within their organization and within their industry. Because it is written in a universal language, the CSF not only helps to improve internal communications and align expectations among business units and people of various technical backgrounds, but also to communicate effectively with key stakeholders outside of the organization as well.

SECTION 2: "CSF 2.0 will remain a framework, providing context and connections to existing standards and resources"

NIST aims to maintain the current level of detail and specificity in CSF 2.0 to ensure it remains scalable and flexible for a wide range of organizations. EEI supports NIST's efforts to ensure the CSF remains technology- and vendor-neutral. By preventing the Cybersecurity Framework from becoming overly prescriptive, NIST can ensure the CSF is adaptable and is able to be used to rapidly address emergent threats.

EEI members encourage NIST to map the CSF to other frameworks and references in a user-friendly way and are supportive of the development of readily available supplemental documents on the NIST website to assist in implementation of the Framework. Without such guidance, cybersecurity efforts and initiatives can be duplicative without a clear relationship path or hierarchy. 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. As NIST updates current resources and develops additional material, EEI members encourage NIST to review the Online Learning content page as well to enhance its usability. In addition, technology-specific mappings, such as for Zero Trust Architecture, can provide additional guidance and value by describing the relationship between the security capabilities of the technology and the desired outcomes in the CSF, but should be maintained outside of the Framework itself to maintain its technology-neutral stance.

SECTION 3: "CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation"

The NIST CSF is an important maturity measurement tool, and EEI members encourage the development of additional implementation guidance to support its use. However, the development of or adoption of sector-specific example Profiles might have the unintended consequence of potentially setting improper industry-wide benchmarks or even mandatory controls, leading organizations to measure against the example Profile instead of properly managing their specific cyber risk. Current and Target Profiles are important tools to enable companies to internally assess their programs and set goals for improvement. Any NIST-developed resources should be focused on providing further guidance to assist companies in developing their own Profiles, tailored specifically to the organization's business and other key characteristics. There is a broad range of diversity amongst organizations even within specific sectors that should be recognized and carefully considered as NIST develops additional implementation guidance. Any sector-specific guidance developed should at a minimum involve consultation and collaboration with key sector stakeholders throughout the process.

SECTION 4: "CSF 2.0 will emphasize the importance of governance"

Reflecting substantial input to NIST, CSF 2.0 will include a new "Govern" Function to emphasize cybersecurity risk management governance outcomes. EEI members have found that the CSF has facilitated more comprehensive and mature, enterprise-wide approaches to cybersecurity. The overall structure of the Framework and the Functions has provided a strong but flexible foundation for organizations to build their cybersecurity programs around. 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 cybersecurity programs in alignment with the CSF, any overarching changes to its foundation could prompt potentially significant revisions and financial costs by those organizations. With respect to the current 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. Consequently, changes to the Functions merit caution, however, EEI members support the addition of a Govern Function to the Framework, as it may help to capture some of the unique complexity that exists as part of a cybersecurity program. A Govern Function that consolidates and centralizes governance-related topics in each existing Function, as well as the expansion of Risk Management, are significant and important changes that will likely provide additional value to users of the Framework.

SECTION 5: "CSF 2.0 will emphasize the importance of supply chain risk management (C-SCRM)"

Cybersecurity risks in supply chains and third parties are a priority for EEI members. Although the CSF's first Function, Identify, lists Supply Chain Risk Management ("SCRM") 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. An extended Supply Chain Risk Management category will aid in setting a baseline level of understanding and expectations for vendors. Vendor and software management continue to be a challenge because existing contract language may not align with cybersecurity requirements or may not support evolving industry practices. In addition to the proposed changes, NIST should thoughtfully consider how SCRM integrates with existing business processes. For example, security assessments of supply chain partners must be closely coupled with organizational acquisition and contracting processes to be effective, and a high-level security maturity assessment for potential new vendors must occur as part of the Request for Proposal process to prevent the business from potentially moving froward with a vendor who does not meet the appropriate requirements. EEI members are subject to supply chain regulations and adhere to a variety of cybersecurity standards, so maintaining harmony between the CSF, cybersecurity guidance, and existing mandatory standards will be important to sustaining the use of the CSF by the industry.

SECTION 6: "CSF 2.0 will advance understanding of cybersecurity measurement and assessment"

As NIST develops resources for cybersecurity measurement and assessment, it should consider the organizational diversity of the CSF's users and incorporate the flexibility necessary for a broad range of implementations. Because of this diversity, any metrics or measurements developed should be maintained in supplemental material and should be considered examples rather than suggested best practices for adoption, to ensure that the CSF maintains its non-prescriptive approach. Any proposed example metrics should have clear rationale and benefit, and existing approaches to metrics development, such as outcome-driven metrics,[1] may be useful as NIST contemplates the possibility of developing supplemental example metrics for the CSF. Metrics should be driven by each organization's unique business model, priorities, maturity, and risk tolerance, and any examples would need to be tailored to suit those specific circumstances.

[1] *See, e.g.,* https://www.gartner.com/en/information-technology/glossary/outcome-driven-metrics

II. CONCLUSION

The NIST CSF has achieved widespread adoption and implementation in large part due to its flexibility and broad applicability. EEI supports the continued review and revision to the Framework to ensure it addresses the current cybersecurity landscape and support organizations worldwide in better understanding, managing, and reducing their cybersecurity risk. EEI members underscore that major changes to the structure of the CSF could have potentially significant cascading impacts on many organizations' internal strategies and procedures. Consequently, NIST should ensure that these changes are compatible with the foundational elements of the Framework. As NIST continues the update process, EEI supports the inclusion of a Govern Function and broader incorporation of supply chain risk management concepts, and encourages NIST to continue to recognize organizational and programmatic diversity as it develops example metrics and measurements. EEI appreciates the opportunity to continue to provide insights and input into the NIST CSF update process.