Edison Electric Institute's Comments Regarding the National Institute of Standards and Technology's Cybersecurity Framework 2.0

Pursuant to the request for public comment included in the National Institute of Standards and Technology's ("NIST") release of its draft version of the Cybersecurity Framework ("CSF") 2.0 (hereinafter "CSF 2.0" or "Framework") on August 8, 2023, the Edison Electric Institute ("EEI") respectfully submits the following comments. CSF 2.0 is an updated version of CSF 1.1, the revised version of CSF 1.0—a tool NIST first released in 2014 to help organizations understand, reduce, and communicate about cybersecurity risk. CSF 2.0 reflects changes in the cybersecurity landscape and makes it easier for all organizations to put the CSF into practice. EEI appreciates NIST allowing interested stakeholders the opportunity to comment on the various updates it proposes to make to the Framework.

I. IDENTIFICATION OF COMMENTER

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for nearly 250 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 Members, which are comprised of foreign electric companies with operations in more than 90 countries, and hundreds of industry suppliers and related organizations, which makeup EEI's Associate Members. EEI member companies' approach to cybersecurity is driven by factors unique to their operational environment—including (but not limited to) their fiduciary responsibility; operating safety; regulatory requirements; and threat-informed, risk-based analysis.

EEI supports the updates NIST proposes to make to the Framework, such as the addition of a Govern Function and the expansion of the cybersecurity supply chain risk management concepts in reflection of its importance throughout the Framework Functions. EEI, however, requests NIST allow for feedback regarding the Implementation Examples ("Examples") after organizations have had time to utilize them. EEI appreciates NIST's responsiveness to industry concerns and comments regarding the Framework and welcomes opportunities in the future to collaborate further on the CSF as it continues to evolve to address the ever-changing cyber threat landscape.

II. COMMENTS

NIST requests additional input on various aspects of the changes and implementation process reflected in the CSF 2.0 draft prior to its final release. Specifically, NIST requests feedback on whether the modifications reflected therein address current cybersecurity challenges faced by organizations, comport with existing practices and guidance resources, and is responsive to stakeholder comments received to date. NIST also seeks suggestions about potential improvements to the Framework, including revisions to Functions, Categories, and Subcategories, as well as submissions of omitted cybersecurity outcomes. Additionally, NIST requests feedback on the format, content, and scope of Examples; suggestions of possible Examples; the appropriate level of abstraction between Subcategories and Examples; and the best way to showcase final modifications from CSF 1.1 to CSF 2.0 to ease transition to the updated version of the Framework.

A. Outcomes Addressing Current Cybersecurity Challenges

NIST requests feedback on whether the cybersecurity outcomes address the current cybersecurity challenges that organizations face. The CSF 2.0 provides "guidance for reducing cybersecurity risks by helping organizations to understand, assess, prioritize, and communicate about those risks and the actions that will reduce them."[1] According to NIST, those actions, in turn, "are intended to address cybersecurity outcomes described within the CSF Core."[2] In addition to cybersecurity outcomes (arranged by Function, Category, and Subcategory), examples of how those outcomes may be achieved (Implementation Examples) and references to additional guidance on how to achieve those outcomes (Informative References) are also set forth in the Framework Core. As NIST stated, the outcome statements in the Core reflect activities across sectors, are technology neutral, and are not a checklist of actions to perform; rather, the specific actions to achieve a cybersecurity outcome will vary by organization and use case, as will the individual responsible for those actions. The outcomes are set forth at a high level to enable them to be understood by a broad audience, including those who may not be cybersecurity professionals, and are "sector- and technology-neutral"[3] for the purpose of providing organizations "the flexibility needed to address their unique risk, technology, and mission considerations".[4]

Similar to the incumbent Framework, EEI views the updated CSF as a beneficial guide, which EEI anticipates will continue to be widely used throughout critical infrastructure

[1] National Institute of Standards and Technology (2023) The NIST Cybersecurity Framework 2.0 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 ipd. at p. 1, https://doi.org/10.6028/NIST.CSWP.29.ipd (hereinafter CSP 2.0).
[2] *Id.*
[3] *Id.* at 8.
[4] *Id.* at 1.

organizations, such as the electric companies comprising EEI membership. In EEI's opinion, broadening the applicability of the Framework will enhance its existing value. Its flexibility and outcome-driven approach allows organizations to easily refine and develop their internal cybersecurity strategies and policies to address cybersecurity risks. Due to its 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. EEI supports the broadened scope of the CSF 2.0 to cover organizations from all sectors and encourages NIST to continue to seek out industry feedback on future versions of the Framework. EEI also agrees with the concerted effort being made by NIST 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 readily usable by organizations to rapidly address emergent threats.

B. Suggestions on improvements to the draft, including NIST's proposed revisions to the Framework's Functions, Categories, and Subcategories

NIST proposes to add a new Function (namely, the Govern Function) to the Framework. The Govern Function, as set forth in the Framework, "is cross-cutting and provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations."[5] As stated in the Framework, "Govern directs an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; and the oversight of cybersecurity strategy."[6]

---

[5] *Id.* at 5.
[6] *Id.*

EEI members support the addition of the Govern Function. This new Function provides a foundational layer that goes beyond technical and operational considerations and allows organizations to establish a cybersecurity strategy that aligns with their respective missions and broader risk appetites. EEI members have found that the CSF has facilitated more comprehensive and mature, enterprise-wide approaches to cybersecurity. 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. The overall structure of the Framework and the Functions have provided a strong but flexible foundation upon which organizations can build their cybersecurity programs. In future updates to the CSF, NIST may wish to consider addressing geo-political realities within the Govern Function subcategory "Roles, Responsibility, and Authorization" when determining access roles for personnel for sensitive positions within critical infrastructure. For personnel with direct access to vital aspects of critical infrastructure, EEI recommends that NIST emphasize the need for stronger security considerations, such as background checks for these personnel, as foreign adversaries have been increasingly targeting critical infrastructure sectors, and have been targeting the energy sector in particular.

EEI previously recommended expanding cybersecurity supply chain risk management to Categories beyond the Identify Function to include the Protect and Detect Functions. The current version of NIST CSF 2.0 includes cybersecurity supply chain risk management within the Govern Function Supply Chain Risk Management (GV.SC) Category and its Subcategories. By expanding this Category and its related Subcategories to include cybersecurity supply chain risk management within the Govern Function, NIST has recognized the importance and complexity of this issue, which 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 support evolving industry practices.

C. Feedback on the format, content, and scope of Implementation Examples; suggestions of possible Examples; and the appropriate level of abstraction between Subcategories and Examples

EEI supports the addition of Examples but requests the opportunity to provide feedback at a later time, after organizations have had a chance to utilize them. In addition, EEI recommends that NIST emphasize the need for organizations to tailor their respective approaches to fit their specific environmental requirements in recognition that a provided Example that may not fit their individual organizational needs. Much like the Framework itself, the application of any Example must be tailored to the unique characteristics of the organization or business itself. EEI members would welcome the opportunity to provide further feedback in the future after having time to familiarize themselves with and utilize the Examples provided. For critical infrastructure organizations, it may be beneficial for NIST to create a high-level, generic example of a hypothetical critical infrastructure company that includes enterprise IT, operational technology, telecommunications, and other lines of business. This Example could demonstrate what the target profiles would look like for each line of business, and alignment with the target profile for the company overall.

D. Feedback on the transition from CSF 1.1 to CSF 2.0

Throughout the update process, NIST has provided valuable information and ample opportunities for engagement. The NIST CSF 2.0 webpage has been a useful resource in understanding the process, finding webinars and workshops, and tracking the timeline. These resources add additional value to the CSF as it allows for user-friendly engagement and a clear source of information. To further assist with the transition, EEI suggests that NIST provide recorded webinars or videos that show the changes from CSF 1.1 to CSF 2.0. EEI also recommends that NIST showcase these changes by providing a side-by-side comparison of the table for CSF 2.0 Core Function, Category Names, and Identifiers and the CSF 1.1 Table 1: Function and Category Unique Identifiers. With the addition of the Govern Function and the redistribution of Categories, providing a visual comparison may help organizations better understand those changes.

III. CONCLUSION

The NIST CSF has achieved widespread adoption and implementation in large part due to its flexibility and broad applicability. EEI supports NIST's revisions to the Framework. In EEI's opinion, the proposed updates will help to ensure the Framework addresses the current cybersecurity landscape and support organizations worldwide in their efforts to better understand, manage, and reduce 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. 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 in the development of Examples and allow for feedback once organizations have had time to utilize the Examples. EEI appreciates the opportunity to continue to provide insights and input into the NIST CSF update process.