BR Business Roundtable

[redacted]

November 2, 2023

[redacted]

Comments of Business Roundtable on the Request for Comment on the NIST Cybersecurity Framework 2.0

Dear Ms. Pascoe:

This letter is submitted on behalf of Business Roundtable, an association of more than 200 chief executive officers (CEOs) of America's leading companies representing every sector of the U.S. economy. Business Roundtable CEOs lead U.S.-based companies that support one in four American jobs and almost a quarter of U.S. GDP. We appreciate the opportunity to respond to the National Institute of Standards and Technology (NIST) Request for Comment on the Cybersecurity Framework (CSF) 2.0.

I. Introduction

Business Roundtable member companies across sectors—from financial services to energy to business services—face significant and growing cyber threats. For approximately the last ten years, NIST's CSF has been a valuable resource for companies and other organizations as they address these risks. The voluntary and technology-neutral nature of the CSF has allowed companies to use it in a manner that is tailored to their own organizations, sectors and risk profiles. This approach also supports continuous innovation in information technology, operations technology and cyber-physical and other systems, which in turn drives tangible advances in cybersecurity capabilities and outcomes. The tailored approach to cyber risk management that the CSF facilitates remains the most effective way to address the cyber threats ahead.

Business Roundtable member companies have worked closely with NIST on the development, refinement and implementation of the CSF. From its conception through the current public comment process, our member companies have helped NIST to build and improve the CSF and develop Implementation Examples, Informative References and Framework Profiles that promote the adoption of the CSF across a wide range of businesses and sectors.

Business Roundtable applauds NIST's continuing work to refine and improve the CSF. The collaborative process that NIST used to develop CSF 2.0 draft—soliciting extensive private sector input along the way—has resulted in a significantly improved and more useful framework that will strengthen the nation's cybersecurity posture. Business Roundtable urges NIST to continue working to ensure that organizations of all types and sizes have the proper knowledge and tools to implement the CSF as effectively as possible.

Within this context, we appreciate the opportunity to provide feedback on CSF 2.0.

II. Business Roundtable Broadly Supports the Refinements Made to CSF 2.0.

Business Roundtable applauds the new and updated elements of CSF 2.0 that improve the usability and applicability of the framework, including expanding the scope of the framework and maturing the existing content.

Business Roundtable particularly appreciates the added emphasis on governance and supply chain risk management in CSF 2.0. Elevating governance to a distinct function underscores the integral role of effective management and oversight in minimizing cyber risk. Within the Govern Function, the expanded guidance on supply chain risk management will help organizations monitor, identify, assess and mitigate cyber risks throughout their supply chains.

Further, the introduction of Implementation Examples and the expansion of Framework Profiles, Informative References and the CSF Reference Tool will improve the framework's value to a diverse array of organizations at all maturity levels. We applaud NIST for designing these tools to allow organizations to better anticipate and respond to the cyber risks they face.

NIST should pay particular attention to how these new elements of the CSF are used in practice. To that end, we encourage NIST to monitor the effectiveness of the new Govern Function and the supply chain risk management provisions and to support the use of these provisions through appropriate guidance. Given the crosscutting nature of the Govern Function, sufficient implementation guidance for this function will be important. We would particularly encourage NIST to develop guidance that reflects the different needs of small and large organizations implementing the CSF.

III. Further Alignment with National and International Cybersecurity Guidance and Standards Will Strengthen the CSF.

Business Roundtable appreciates NIST's focus on aligning CSF 2.0 with other cybersecurity standards, frameworks and best practices. In a growing patchwork of cybersecurity requirements and standards, clear connections between the CSF and other frameworks, including the NIST Artificial Intelligence Risk Management Framework, will greatly increase the value of the CSF.

For example, as indicated in the current draft CSF, NIST should consider referencing other NIST publications and frameworks in relevant sections of the CSF 2.0 Core (e.g., SP 800-171, SP 800-161, SP 800-63). In addition, NIST should ensure that clear connections are made to other frameworks by using consistent terms and definitions, or by providing appropriate clarification when it is not possible to use consistent language.

Further, Business Roundtable encourages NIST to promote the CSF as a model for harmonizing cybersecurity requirements and guidance at the state and federal levels. Business Roundtable welcomes ONCD's recent Request for Information focused on harmonizing cybersecurity requirements and urges the Administration to pursue harmonization of cyber incident reporting as well. The CSF should play a central role in any harmonization efforts. In particular, Business Roundtable encourages NIST to engage with federal agencies and state governments to emphasize the importance of the risk-based approach taken by the CSF and to support its further adoption.

NIST should also continue to work with international stakeholders to promote CSF as a model for voluntary, risk-based cybersecurity governance. The adoption of interoperable international cybersecurity standards is key to the continued growth of the digital economy and managing international cyber threats. To this end, further use of the CSF across jurisdictions will strengthen global cybersecurity and facilitate efficient compliance with requirements in any particular jurisdiction.

In pursuing these steps, NIST should continue to include relevant external references as tools that companies can use to achieve the goals laid out in the CSF—not as integral parts of the CSF itself. NIST should make clear that cross references to relevant standards provide one way to achieve the goals of the CSF, but not the only way to do so. To avoid encouraging a checklist-based approach to compliance, NIST should be careful not to suggest that meeting any cross-referenced standards is required to achieve the goals of the CSF.

IV. Conclusion

Business Roundtable supports NIST's work developing CSF 2.0 and shares its goal of effectively managing cyber risk. We welcome the changes made in the CSF 2.0 draft and encourage NIST to continue building upon the strong foundation it has set. We appreciate the opportunity to respond and provide input during this process and look forward to continued engagement with NIST on these and other important topics. To discuss our response or any other matters you believe would be helpful, please contact Amy Shuart, Vice President of Technology & Innovation, Business Roundtable, at [redacted]