The Software Alliance

BSA

[redacted]

Via e-mail to cyberframework@nist.gov

November 2, 2023

Mr. Stine,

BSA | The Software Alliance[1] welcomes the opportunity to provide feedback on the National Institute of Standards and Technology's (NIST) public draft of the Cybersecurity Framework (CSF) 2.0. We commend NIST for working on this important update to the CSF and appreciate your engagement with industry and other stakeholders as part of this process.

BSA is the leading advocate for the enterprise technology sector. Our members are among the world's most innovative companies and help to drive digital transformation by providing the solutions that make businesses and governments more competitive and effective, including cybersecurity, cloud computing, customer relationship management, human resources management, data analytics, manufacturing, infrastructure, and identity and access management tools and services.

Since it was first published in 2014, the CSF has served as a useful tool to help organizations – including BSA members – manage cybersecurity risk. We appreciate that the public draft adapts the CSF to the evolving state of technology and cybersecurity threats, and encourage NIST to ensure that it remains a flexible and voluntary framework for cybersecurity risk management. Our feedback builds on BSA's previous responses to NIST's Cybersecurity Request for Information, CSF 2.0 Concept Paper, and Discussion Draft of the CSF 2.0 Core.

<u>Our response specifically focuses on the following:</u>

- Ensuring that CSF 2.0 remains a voluntary and flexible framework, rather than a prescriptive model for compliance
- Supporting the expanded scope of CSF 2.0 to recognize its broad use, not limited to critical infrastructure
- Supporting the public draft's emphasis on cybersecurity governance
- Supporting the integration of supply chain risk management in CSF 2.0

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Palo Alto Networks, Prokon, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[redacted]

- Supporting clarified understanding of cybersecurity measurement and assessment

Ensuring that CSF 2.0 remains a voluntary and flexible framework, rather than a prescriptive model for compliance. One source of value of NIST's Cybersecurity Framework is that it is grounded in the principle of flexibility and that it is voluntary in nature. Organizations find this useful, as it enables them to tailor their cybersecurity risk management practices to the unique risks and threat environment they face. In order to preserve the nature and intent of the Framework, it must continue to focus on the principles of flexibility and voluntariness. To that end, we encourage NIST to underscore that the Informative References and Implementation Examples should be understood as separate from the Framework itself and are meant to serve only as examples of how the Framework *may* be implemented. We also encourage NIST to explicitly clarify that the Informative References and Implementation Examples are not *requirements* for cybersecurity risk management and are not meant to be used as a prescriptive model for compliance purposes.

Further, as the cybersecurity landscape and associated technologies evolve, we encourage NIST to provide the stakeholder community with a process for submitting Informative References and Implementation Examples. Such a process could support NIST's efforts to ensure that the Framework's examples remain up-to-date and represent the wide diversity of sectors leveraging the CSF.

Expanded scope of CSF 2.0 to recognize its broad use, not limited to critical infrastructure. Among the changes in CSF 2.0, we support NIST's decision to expand the Framework's scope beyond critical infrastructure. We believe this reflects the Framework's wide-ranging use across industries, sectors, and organizations both domestically and internationally, and its intended broad use moving forward. This change also underscores that managing cybersecurity risk should be a goal across all types of organizations, which is a shared interest across the cybersecurity community.

Emphasis on cybersecurity governance. As noted in our previous feedback to NIST, BSA supports the addition of a new Govern function in the Framework. Governance is a key component underpinning organizations' approach to cybersecurity risk and enterprise risk management more broadly. As a core function, Governance lays the foundation for an organization's strategy to manage and monitor cybersecurity risks. The CSF 2.0 public draft appropriately recognizes that the Govern function guides the implementation of the Identify, Protect, Detect, Respond, and Recover functions, and its categories and subcategories reflect many of the key activities organizations currently undertake to implement governance in practice.

Moreover, the Govern function supports long-running efforts to elevate and maintain cybersecurity risk management as a function undertaken by an organization's leaders. We appreciate that the public draft acknowledges the important role that organizational leaders play in cybersecurity risk management through the development and communication of mission priorities and objectives, which is integral to promoting a greater culture of risk awareness throughout an organization.

Integration of supply chain risk management. We support the public draft's integration of cybersecurity supply chain risk management (C-SCRM) throughout the Framework's functions – in particular through the inclusion of a new category in the Govern function focused on C-SCRM. We believe this approach acknowledges the relevance of C-SCRM across risk management activities and provides useful factors that organizations can take into account in managing supply chain risks and relationships with suppliers.

[redacted]

We also appreciate that the public draft acknowledges that C-SCRM "is a systematic process for managing exposure to cybersecurity risk throughout supply chains" while directing organizations to the guidance in SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. As noted in BSA's previous feedback to NIST, we agree that CSF 2.0 should highlight the importance (and challenge) of managing cybersecurity supply chain risks but should do so in a way that does not overwhelm the Framework. The value of the Framework is its ability to focus on the most important outcomes and activities that should serve as a foundation for organizations' risk management practices. We believe NIST's discussion draft provides an appropriate level of detail in its integration of C-SCRM considerations without departing from this objective.

Finally, while we understand the emphasis on C-SCRM in the CSF 2.0 updates, we highlight that there is an increased focus on C-SCRM in the U.S. government and other governments that has the potential to result in new supply chain reporting requirements for organizations. These types of requirements would introduce greater complexity to organizations' C-SCRM activities. While this is not a topic addressed in the CSF 2.0 public draft, when a final version of the Framework is published, we encourage NIST to focus on the many ways in which organizations already prioritize C-SCRM and note CSF's ability to help organizations of all sizes achieve greater maturity in their cybersecurity risk programs while avoiding such complexity.

Clarified understanding of cybersecurity measurement and assessment. As noted in BSA's response to NIST's CSF 2.0 Concept Paper, we support NIST's efforts to advance cybersecurity measurement and assessment in the Framework. We appreciate that the public draft gives organizations the flexibility to customize metrics and provides guidance on how organizations can use the Framework's tiers as a complement, rather than a substitute, to their individual risk management methodologies. As we have noted previously, measuring cybersecurity outcomes is extremely challenging because organizations undertake cybersecurity activities in a complex ecosystem in which multiple, diverse actors interact and adapt. We encourage NIST to note the inherent challenges and limitations of measuring such complex systems, including systemic risk.

* * *

BSA strongly supports NIST's work to update the Cybersecurity Framework and appreciates the opportunity to provide feedback on the public draft. We look forward to continuing to work with you on this important resource for the cybersecurity community.

Sincerely,

Olga Medina

Olga Medina
Director, Policy

[redacted]