The Institute of
Internal Auditors
Elevating Impact

February 23, 2023

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

RE: IIA Comments Regarding NIST Cybersecurity Framework (CSF) 2.0 Concept Paper

Dear Sir /Madam:

The Institute of Internal Auditors (The IIA), a founding member of The Committee of Sponsoring Organizations of the Treadway Commission (COSO), thanks the National Institute of Standards and Technology (NIST) for the opportunity to share comments on its Cybersecurity Framework (CSF) 2.0 Concept Paper.

For over 80 years, The IIA and its now more than 230,000 members across the globe have aided sound governance and risk management efforts in public- and private-sector organizations, encouraging strong internal controls and an enterprise-wide approach.

The IIA recognizes the tremendous value that NIST's many publications — especially including SP 800-53r5, SP 800-63, and SP 800-207, all of which are mentioned in the CSF 2.0 Concept Paper and throughout various IIA Global Technology Guides (GTAGs) — bring to the global understanding of enterprise technology. The IIA expects that the CSF 2.0 will also be a useful resource for organizations of all types, so we support the proposed changes that recognize the CSF's broad applicability.

One suggestion relevant to section 2.6 of the CSF 2.0 Concept Paper is that the GTAG "Auditing Identity and Access Management," which makes extensive references to NIST, ISACA, and CIS frameworks, may provide useful process-based context for NIST's effort to: "explore updates to the CSF's Identity Management, Authentication, and Access Control Category (PR.AC), including a potential re-ordering of Subcategories, to reflect the components of the digital identity model and phases of the digital identity lifecycle more clearly."

Regarding section 4.0 of the CSF 2.0 Concept Paper, The IIA concurs with NIST's proposal to add a "Govern" function to the CSF, but recommends clear delineation between the roles of the governing body, management, and independent assurance providers as described in The IIA's Three Lines Model:

- Strategic, entity-level oversight and direction provided by a governing body [governance].

- Responsibility for designing processes and solutions, and allocating resources, to meet objectives and mitigate inherent risks [first line management].
- Responsibility for assessing residual risks and suggesting improvements to control designs or resource allocations [second line management].
- Responsibility for providing independent assurance to internal and external stakeholders — primarily the governing body — that first and second line management processes are adequately designed and implemented [third line assurance from internal audit].

The IIA's *International Standards for the Professional Practice of Internal Auditing (Standards)* defines governance as (emphasis added): "The combination of processes and structures implemented **by the board** to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives." Additionally, COSO's *Enterprise Risk Management – Integrating with Strategy and Performance* describes enterprise risk management as "the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value."

Accordingly, we suggest that NIST categorize processes for which the governing body is responsible as "governance," while processes for which management is responsible should be considered part of an enterprise risk management system, regardless of whether the organization refers to them by that name. As explained in the Three Lines Model, internal audit provides independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management.

One critical aspect of governance that should be addressed in 2.0 that the CSF v1.1 does not mention is the need for independent assurance to promote trust between the governing body, management, and other stakeholders. This principle applies to all organizations, but NIST has a particular role to play as the body designated to establish guidance for U.S. federal agencies, as described, for example, in the May 2021 Executive Order on Improving the Nation's Cybersecurity. The IIA believes that formally recognizing the role that independent assurance plays in effective governance and risk management processes would benefit not only the federal agencies that rely on NIST guidance as statutory requirements (in many cases), but also the many other organizations globally that use the CSF as a model.

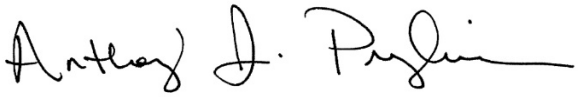
The IIA regularly integrates NIST's technical expertise into our internal audit guidance: In 2022, The IIA published two GTAGs explicitly aligned with four of the five Functions identified in the CSF v1.1. "Auditing Cybersecurity Operations: Prevention and Detection" and "Auditing Cyber Incident Response and Recovery" made extensive use of and references to objective, risk, and control concepts covered in the Protect, Detect, Respond, and Recover functions in the CSF. Additionally, when the GTAG "Assessing Cybersecurity Risk – The Three Lines Model" is

The Institute of
Internal Auditors
Elevating Impact

refreshed, it will be explicitly aligned with the CSF's Identify function, in a similar manner as the other two GTAGs.

We welcome the opportunity for further discussion and ask that you please contact Mat Young, the IIA's Vice President of Global Advocacy, Policy, and Government Affairs at Mat.Young@theiia.org with any follow-up questions or concerns.

Sincerely,



Anthony J. Pugliese, CIA, CPA, CGMA, CITP
President and Chief Executive Officer
The Institute of Internal Auditors, Global Headquarters