Deloitte.

Deloitte & Touche LLP
[redacted]
www.deloitte.com

November 6, 2023

National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
Submitted electronically to cybersecurityframework@nist.gov

Email Subject: Deloitte's comments on the Draft CSF 2.0 Public Draft

Dear NIST Team,

We appreciate the opportunity to provide feedback to NIST, and below are Deloitte's comments on the Draft CSF 2.0 Public Draft. As one of the largest professional services organizations in the United States, Deloitte provides a vast array of information security and privacy services across approximately 2,800 engagements in major industries and 15 cabinet-level federal agencies. We serve our clients by helping them understand their level of cyber resilience based on their critical assets, their threat landscape, and the maturity of their cyber capabilities. Our comments reflect our deep experience helping clients manage cybersecurity risk across a broad range of industries and organizations.

We believe that many of the uses and challenges of CSF 1.0/1.1 are being addressed appropriately through the CSF 2.0 Public Draft and we support the approaches the draft outlines for retaining the current level of detail; integrating the CSF into larger risk management frameworks; and broadening the scope to include non-critical infrastructure sectors. We agree with the approach in the latest draft of the CSF 2.0 which includes implementation examples to help organizations better leverage CSF as a part of their strategic goal setting and integration into their enterprise risk management.

One change we would recommend as a part of these implementation examples would be to strengthen the language around the use of the examples, highlighting that they are intended to be flexible rather than to recite strict requirements. It is our view that many of the cited challenges that the CSF 1.0/1.1 faces are due to attempts to leverage CSF for uses beyond its intended purpose. In attempting to "implement" CSF in conjunction under detailed, prescriptive instructions, the core flexibility of the NIST CSF is lost. The use of CSF Tiers and CSF Profiles is intended to provide flexibility, and NIST would do well to emphasize this to mitigate the risk that the implementation examples are used within industry as strict requirements.

During our support of the development of the NIST CSF and carrying through numerous deployments across federal, state, and commercial, we have viewed the CSF as a flexible tool set to help organizations make strategic decisions on how they implement the cybersecurity concepts in their organizations. Using the CSF Tiers, organizations can set their own enterprise cybersecurity current standing and future goals to make strategic decisions. CSF profiles can then be used to customize the specifics of an implementation to align their overall strategy to cybersecurity functions, or to define an acceptable

basis for suppliers. These pieces do not provide implementation specifics on purpose but give an organization the ability to set goals which can then be mapped back to the right standards to match their unique environment and industry. There is risk that the implementation examples provided could be used as specific requirements which organizations may try to enforce without adapting to their organizational needs. We support the current path of CSF 2.0, which makes clear through implementation examples how CSF acts as a bridge between strategy and implementation rather than as a precise implementation standard on its own and believe strengthening that language would best serve to highlight the importance of flexibility in CSF 2.0 overall.

Additionally, we recommend that some supplementary high-level language be included around how organizations adopt emerging technology. Currently, CSF 2.0 does allow flexibility in how Profiles can be used for addressing emerging threats or technologies, but it is limited in its guidance. The cyber risk landscape is constantly shifting with the introduction of new technologies that often result in significant upheavals in how organizations do business. This has posed issues for cyber security organizations which often are left addressing technology only after it has matured. However, the scope, scale, and interconnectedness of many of today's emerging technologies—including post-quantum cryptography (PQC) and artificial intelligence (AI)—require organizations to stay ahead of the curve to best support the mission of their various enterprises. Deloitte recommends the CSF 2.0 include expanded language around how CSF Tiers and CSF Profiles can best be adapted to future technologies, with examples of how to approach adapting an existing CSF Profile to a new type of technology. By giving organizations the guidance for how to consider future trends, CSF 2.0 can be an invaluable resource and lead the way for organizations as they adapt to the emerging technology trends of tomorrow.

We look forward to seeing the continued growth of the NIST CSF.

Respectfully submitted,

Colin Soutar
Managing Director
Deloitte Government and Public Services
Risk & Financial Advisory, Cyber Risk
Deloitte & Touche LLP