Dear NIST Cybersecurity Authors,

We at Schellman would like to express our appreciation for your ongoing efforts to improve and update the Cybersecurity Framework (CSF) to reflect the ever-evolving cybersecurity landscape. The proposed changes to the CSF 2.0 are commendable, and we are grateful for the opportunity to provide our comments and feedback to help make the framework more effective and practical for organizations.

As a cybersecurity assessment firm, we work closely with organizations across industries to help them enhance their cybersecurity posture and comply with regulatory requirements. The CSF has been a valuable resource for our clients, and we are pleased to have the opportunity to offer our insights and recommendations to further improve the framework.

- We strongly support the proposed changes to the Identify and Protect functions, as they aim to provide organizations with more specific guidance on how to identify and protect against emerging cyber threats. However, we suggest that NIST provide more detailed guidance on how organizations can implement these changes effectively, particularly for small and mid-sized organizations that may have limited resources and expertise.
- We recommend that NIST expand the Respond and Recover functions to include more detailed incident response and recovery planning guidance. Organizations face an increasing number of cyber attacks and need to be prepared to respond and recover effectively. Providing more detailed guidance on incident response and recovery planning would help organizations to improve their cybersecurity resilience.
- We recommend that NIST provide more detailed guidance on how to integrate the CSF 2.0 with other cybersecurity standards and frameworks, such as ISO 27001 and NIST SP 800-53. Many organizations are required to comply with multiple cybersecurity frameworks and standards, and providing more guidance on how to implement the CSF 2.0 alongside other frameworks would help to reduce the overall cost and effort required for compliance.
- We also suggest that NIST should develop more detailed guidance on how to measure the effectiveness of cybersecurity programs using the CSF 2.0. Organizations need to understand the effectiveness of their cybersecurity programs and be able to track their progress over time. Providing more guidance on how to measure the effectiveness of cybersecurity programs would help organizations to identify areas for improvement and optimize their cybersecurity resources.
- We strongly recommend that NIST specifies the minimum qualifications and experience requirements for assessors who perform cybersecurity assessments using the CSF 2.0. This will help to ensure that assessors have the necessary skills and expertise to conduct assessments effectively and provide accurate recommendations for improvement.
- We suggest that NIST requires assessors to have a certain level of independence from the organizations they are assessing. This will help to prevent conflicts of interest and ensure that assessments are conducted objectively and impartially.
- We recommend that NIST provides guidance on how to ensure the independence of assessors. This could include requiring assessors to disclose any potential conflicts of interest and ensuring that they have no financial or personal ties to the organizations they are assessing.
- We suggest that NIST requires assessors to follow a code of ethics or professional standards when conducting assessments. This will help to ensure that assessors maintain the highest level of professionalism and ethical behavior.

- We strongly recommend that NIST requires assessors to undergo periodic training and certification to ensure that they stay up-to-date with the latest cybersecurity threats, vulnerabilities, and best practices. Cybersecurity is a rapidly evolving field, and it is essential that assessors are up-to-date with the latest developments to provide effective assessments.
- We suggest that NIST provide more tailored guidance and resources for smaller organizations to implement the CSF 2.0 more easily, leverage third-party service providers, and promote the adoption of the CSF 2.0 with incentives and targeted outreach and education programs. Smaller organizations may have limited resources and expertise to implement the framework, and tailored guidance and resources would help them to overcome these challenges.
- We recommend that NIST align the CSF 2.0 with other international cybersecurity standards, such as ISO 27001 and the EU's General Data Protection Regulation (GDPR), and provide more guidance on how to use the framework in conjunction with other frameworks. Aligning the CSF 2.0 with other standards and frameworks will help to promote global cybersecurity best practices and facilitate compliance with multiple standards using a common framework.
- We suggest that NIST provide more specific guidance on emerging areas of cybersecurity, such as cloud security, IoT security, and supply chain security. These areas are becoming increasingly critical to the cybersecurity of organizations, and more.
- NIST should consider providing more detailed guidance on how to conduct penetration testing and vulnerability assessments in accordance with the CSF 2.0. These are critical components of a comprehensive cybersecurity program, and more detailed guidance on how to implement them effectively would be highly valuable.
- We suggest NIST provide examples of the systems that should be the subject of penetration testing and vulnerability assessments as well as what the goal of an effective test should be. Where applicable, an assessment of security controls should include technical testing.
- NIST should consider specifying the level of rigor that is expected of penetration testing. It would be helpful to organizations and assessment firms alike to have a shared understanding of what methodology should be applied.
- NIST should consider developing a certification program for organizations that successfully implement the CSF 2.0. This would help organizations to demonstrate their commitment to cybersecurity and differentiate themselves from competitors. Schellman and other cybersecurity assessment firms could also benefit from such a program by offering certification services to their clients.
- NIST should consider developing a set of case studies or examples of organizations that have successfully implemented the CSF 2.0. This would help to illustrate the benefits of the framework and provide guidance on how to overcome common challenges.
- IST should consider developing a community of practice for organizations and cybersecurity professionals who are implementing the CSF 2.0. This community could share best practices, provide guidance, and foster collaboration among organizations and professionals.
- NIST should consider developing a roadmap or implementation guide for organizations that are new to the CSF 2.0. This would provide a step-by-step guide on how to implement the framework effectively and would be especially valuable for small and mid-sized organizations that may not have the resources or expertise to develop their own implementation plan.

In conclusion, we commend NIST for its continued efforts to enhance the cybersecurity of organizations through the development and refinement of the CSF. We appreciate the opportunity to provide our comments and feedback and look forward to the release of the updated framework.

Thank you for your commitment to improving the cybersecurity posture of organizations, and please do not hesitate to reach out if you have any questions or concerns about our comments.