April 25, 2022

Submitted via the Federal eRulemaking Portal

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

Re: Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

The Coalition to Reduce Cyber Risk, Inc. ("CR2") submits these comments in response to the request for information issued by the National Institute of Standards and Technology ("NIST") regarding the Cybersecurity Framework evaluation and improvement ("CSF 2.0"). CR2 appreciates the opportunity to provide feedback and looks forward to working with NIST as the CSF 2.0 is developed and accompanying NIST at international engagements to promote the CSF 2.0 when those engagements take place.

CR2 members include global organizations that represent numerous sectors, including financial services, IT, and communications, that are committed to security, trust, and economic growth and opportunity. CR2 members have deep expertise in cybersecurity and enterprise risk management, as well as unique insights into cross-sector independences and global interconnectivity, which drive the need for consistent, foundational approaches to cybersecurity risk management across sectors and geographies. As such, CR2 has set out to work collaboratively with public and private sector entities to improve cybersecurity risk management practices that will both enhance cybersecurity and support economic growth.

To advance cybersecurity risk management practices that will both enhance cybersecurity and support economic growth, CR2 has worked with public and private sector entities in several dozen countries around the world. As a coalition, we strongly agree with NIST's objectives in updating the CSF to strengthen the framework to account for a new cybersecurity landscape, including new threats, capabilities, and technologies, since the CSF was last updated in April 2018.

As the CSF 2.0 is developed, we recommend NIST keep in mind the following:

The CSF is an effective tool to aid organizations' cybersecurity efforts and the flexible, voluntary nature of the framework has greatly helped in its adoption. As NIST drafts CSF 2.0, the existing standards, guidelines, and best practices included in the framework should be supplemented in areas that cybersecurity has evolved in the last three years, rather than a total revision of the framework. CR2's core mission is to promote principles of cybersecurity risk management that are grounded in industry experience, have a successful track record, and include traits such as clarity and consistency, risk-based, outcome focused, and agility. Coupled with that, CR2 believes in an open, collaborative, and iterative approach to support the adoption of frameworks for cybersecurity risk management. The CSF aligns with these principles and as such CR2 has promoted the CSF during engagements with foreign countries that are updating their cybersecurity strategies or policies. Most recently, CR2 recommended alignment or adoption of the CSF in comments to the European Commission on the NIS Directive Update and to Colombia on the Cyber Decree for the country.

Changes to existing CSF categories and subcategories should be minimal and where necessary should address compatibility and provide clear guidelines to supplement other USG guidance. The CSF has formed the basis for many cybersecurity programs, both domestic and international. As such, any changes to the existing CSF categories and subcategories should be minimal and thoroughly considered. As NIST adds additional resources and categories to CSF 2.0, NIST should

consider adopting a single, comprehensive framework covering both cybersecurity and technology controls due to the inextricable nature of cyber and technology. This would give organizations a holistic integrated solution to work with. To maintain the integrity of the CSF, NIST could include a filter to enable distinction between cyber defense and general technology control practices. Additionally, NIST could address concerns regarding risks outside of purely cybersecurity by mapping the CSF 2.0 to the following:

- Unified Compliance Framework (UCF): UCF Mapping Report for Improving Critical Infrastructure Cybersecurity
- CMMC 2.0
- Other NIST standards such as NIST SP 800-171 and other relevant international accepted standards such as the ISO/IEC 27000 series

CR2 would like to be a partner in ensuring the adoption of CSF 2.0 internationally. Given that CR2 has promoted the CSF internationally, both in our own initiatives and in partnership with NIST, CR2 would welcome the opportunity to serve as a partner and resource to increase international use of CSF 2.0. As NIST notes in the request for information, there are numerous examples of international adaptations of the CSF by other countries. Given the importance of 1) making sure countries that have adopted the CSF continue to use CSF 2.0 and 2) promoting the CSF 2.0 with new countries, CR2 recommends the following steps:

- NIST should identify the barriers to foreign adoption of the CSF 2.0 and tailor messaging and education to counter these barriers. From CR2's conversations, we believe a common barrier is the natural inclination to develop something at the national level for a security issue. That inclination, combined with the wrong assumption that flexible, outcome-driven policies are softer than prescriptive approaches, should be countered in messaging around the CSF 2.0. When NIST is meeting with foreign governments to promote the CSF 2.0 we recommend

messaging and deliverables that note how a flexible, outcome-driven approach, framed in terms of what security outcomes need to be achieved, has relevance across organizations and sectors and is more flexible and effective over time. As NIST knows, technology capabilities, including those used for security, are dynamic, and malicious cyber actors are also continuously evolving their techniques and tactics, making adaptability and flexibility essential for effective cyber risk management.

- NIST should conduct workshops with foreign governments and companies to identify different ways the CSF can be used and how it can integrate with other international standards.

- Mapping to standards in key jurisdictions and translating the framework into many different languages sparked adoption of the CSF and we recommend NIST do the same for the CSF 2.0.

- Workshops and events in region to promote the CSF were highly effective. CR2 recommends NIST do the same for CSF 2.0 and partner with regional organizations on these events to drive regional participation. Leveraging international organization partners for workshops and event, and general promotion of CSF 2.0, will help drive international participation, international adoption, and international trust in the CSF 2.0.

- Even ahead of the implementation stage of CSF 2.0, CR2 recommends that NIST start engagement with foreign countries and international organizations now to take their input and allow their input to shape the CSF 2.0.

CR2 would welcome any collaboration or partnership in carrying out any of these recommendations.

Future, and in development, U.S. government policies on cybersecurity should be aligned with the CSF and CSF 2.0. The U.S. government has many cybersecurity

initiatives underway. No matter the vector of cybersecurity updates, from Executive Orders to legislation to agency specific regulation, there must be alignment with the CSF. The CSF should be leveraged to avoid duplication and fragmentation which only decreases overall security and readiness.

CR2 thanks NIST for the consideration of these recommendations and continued work to promote risk, outcome-based security in the U.S. and internationally. We look forward to working with NIST to encourage international adoption of the CSF 2.0.

Respectfully submitted,

The Coalition to Reduce Cyber Risk