Coalition for Cybersecurity
Policy & Law

Coalition for Cybersecurity Policy & Law
600 Massachusetts Ave, NW, Washington, DC 20001

April 10, 2017

VIA EMAIL: cyberframework@nist.gov

Edwin Games
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Comment of the Coalition for Cybersecurity Policy & Law on the Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity

The Coalition for Cybersecurity Policy & Law ("Coalition") submits this comment in response to the Request for Comments ("RFC") issued by the National Institute of Standards and Technology ("NIST") on January 25, 2017, regarding the draft update of the Framework for Improving Critical Infrastructure Cybersecurity ("Framework").[1] The Coalition appreciates the opportunity to provide feedback on the update to the Framework and to continue working with NIST to ensure that the Framework remains an important resource to guide businesses in the development of their cybersecurity practices.

The Coalition is comprised of leading companies with a specialty in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.[2] We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management, and we are supportive of efforts to identify and promote the adoption of cybersecurity best practices and voluntary standards throughout the global community.

The Coalition broadly supports NIST's efforts to update and improve the Framework. Specifically, the Coalition supports the additional clarity that the update has provided regarding the use of the Implementation Tiers, the addition of much needed guidance regarding both Cyber Supply Chain Risk Management ("SCRM") and cybersecurity measurement, and the inclusion of informative references addressing multifactor authentication. However, within each of these positive steps, the Coalition believes that there is additional room for improvement. The Coalition encourages NIST to provide further clarification regarding the use of the Implementation Tiers and the criteria for designation at each Tier. The Coalition also encourages NIST to remove SCRM from the Implementation Tiers and as a new category in the Framework Core, instead

[1] *See* 82 Fed. Reg. 8408 (January 25, 2017).
[2] The views expressed in this comment reflect the consensus view of the Coalition and do not necessarily reflect the views of any individual Coalition member. For more information on the Coalition, *see* www.cybersecuritycoalition.org.

incorporating relevant concepts into the existing categories and subcategories. The Coalition further recommends that NIST incorporate references to the specific NIST publications that address SCRM and electronic authentication procedures to provide additional guidance to organizations seeking to implement these controls. Finally, the Coalition reiterates its prior recommendations that NIST promote the Framework as a model for other countries to use in developing their own multistakeholder processes to promote more effective risk management, self-assessment of organizational maturity, and identification of relevant standards. We further suggest NIST should implement a formal review and updating process to improve the Framework on a regular and systematic basis.

Implementation Tiers. We applaud NIST's efforts to provide greater clarity to the integrated risk management program descriptions; however, we encourage NIST to revisit the Implementation Tiers before finalizing the update to the Framework, as more can be done to make the Implementation Tiers more useful, particularly for small and midsized businesses. Specifically, we recommend that NIST clarify the dual purpose of the Implementation Tiers and identify and catalogue the tools that are relevant to the implementation of the Framework. We also encourage NIST to clarify the criteria for designation at each of the Tiers for the risk management process and external participation descriptions.

The Coalition believes that additional clarity around the purposes of the Implementation Tiers and the tools that organizations can use to move from one tier to another will facilitate adoption of the Framework and thereby increase its use across various industry sectors. The Coalition encourages NIST to clarify that organizations can effectively use the Implementation Tiers to identify its Target Profile with due consideration for its size, the sensitivity of the information it maintains, and other relevant risk factors. Once an organization has developed a Target Profile, it can leverage the Implementation Tiers to assess progress against its Target Profile. NIST should explicitly call out the dual use of the Implementation Tiers, which will better enable organizations to understand their purpose and use.

The Coalition also encourages NIST to further clarify the criteria for designation at each of the given Tiers. As we noted in our earlier comments, the risk management process description for Tier 2 and Tier 3 are remarkably similar, making it difficult for companies to distinguish between the Tiers in practice. Removing this ambiguity would make the Framework more useful, which would likely further boost adoption by the business community.

The Implementation Tiers also lack important detail regarding an organization's participation in the cyber threat identification and information sharing ecosystem. The external participation description broadly addresses cyber threat information sharing; however, greater specificity about participation in Information Sharing and Analysis Organizations ("ISAOs"), Information Sharing and Analysis Centers (ISACs), Cyber Emergency Response Teams ("CERTs"), vendor and industry alliances, public-private partnerships, and other related initiatives that provide real-time information on, and assistance in resolving, specific cyber threats would help organizations more effectively use the Implementation Tiers.

Supply Chain Risk Management. The Coalition supports the inclusion of SCRM in the updated Framework. The Coalition believes that the discussion of SCRM activities and explaining how the updated Framework can be used to make risk-informed buying decisions by identifying security priorities and residual security risk adds significant clarity around how organizations can use the Framework to improve their SCRM. However, the Coalition does not believe that SCRM should be included as a separate and new Category in the Framework Core. Rather, the Coalition urges NIST to incorporate relevant SCRM concepts into existing Categories, creating new subcategories where and if necessary.

The Coalition is also concerned that calling out SCRM as a "property" within the Implementation Tiers is confusing because it is also part of a good Risk Management and Integrated Risk program. Creating a separate bullet raises the question of why other risk management elements (for example, incident response planning) are not also raised in the same way.

To further clarify the Framework's role in assisting organizations in making risk-informed buying decisions, the Coalition encourages NIST to include references to Supply Chain Management Practices for Federal Information Systems and Organizations, SP 800-161 in addition to references to Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53, in the informative references to enable organizations to build on the important new work that has been done on addressing supply chain vulnerabilities.

Vulnerability Disclosure Programs. The Coalition believes that critical infrastructure organizations should establish a coordinated vulnerability disclosure and handling process. Among other additions to existing subcategories,[3] NIST should create a new subcategory within the core of the Framework to include existing standards and best practices. For example, NIST could add a subcategory to Risk Assessment (ID.RA) – "*ID.RA-7: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from external sources*" – and cite ISO/IEC 30111:2013 and ISO/IEC 29147:2014 as "Informative References." The Coalition also recommends that NIST make clear that coordination with external security researchers or vulnerability finders and maturity in operationalizing external information for effect

[3] NIST could also incorporate coordinated vulnerability and handling processes by clarifying the scope of existing subcategories. For example: the "identify" function, at ID.RA-2, urges organizations to receive cyber threat intelligence and vulnerability information from "information sharing forums and sources." The Framework should make clear that the company should be prepared to receive and analyze vulnerability information from "information sharing forums *or any other external source*" (such as security researchers or accidental discoverers), not just information sharing sources with which the organization may have a formal arrangement (such as ISACs or ISAOs). ID.RA-2 could also cite ISO/IEC 30111:2013 and ISO/IEC 29147:2014 as informative references. In addition, the "protect" function, at PR.AT-3, includes awareness and training so that third party stakeholders understand roles and responsibilities. This should expressly encompass third parties that submit vulnerabilities to the organization, but who have no formal relationship to the organization (e.g., "suppliers, customers, partners, or *unaffiliated parties that submit vulnerability information*, etc."). Organizations should aim to make such third parties aware of (or able to easily find) desired communication channels, such as a public facing email address dedicated to receiving vulnerability disclosures, and any applicable security policies. As above, PR.AT-3 could list ISO/IEC 30111:2013 and ISO/IEC 29147:2014 as "informative references."

are included within the External Participation property of the Implementation Tiers.[4] In addition, in its Roadmap, NIST should include that it will convene stakeholders to discuss maturity levels for external and internal vulnerability disclosure and handling processes, utilizing relevant existing private sector resources as a starting point. The resulting guidance from that convening ultimately may be appropriate to include as an Informative Reference within the Framework as well.

Measurement. The Coalition believes that the ability to measure an organization's current cybersecurity posture and its progress towards identified goals is critically important to the Framework's usefulness to organizations. The Coalition supports NIST's efforts to address measurement for the Framework and to establish a common vocabulary for organizations to discuss measurement. Having a common vocabulary around measurement not only facilitates organizations' efforts to assess their own cybersecurity practices but also those of its partners and service providers. This information is essential for organizations to make risk-informed contracting decisions.

However, the Coalition encourages NIST to further develop, in documents outside of the Framework, the metrics that organizations can use to effectively measure their current position with respect to the Framework and that of relevant third parties. Towards this end, the Coalition recommends that NIST identify, catalogue, and validate metrics that organizations can use to measure their own implementation of the Framework as well as that of their partners. Without identifying these tools and providing some understanding of their efficacy, the additional clarity around measurement terminology will be of limited practical benefit to organizations.

Identity and Access Management. The Coalition applauds the inclusion of greater detail regarding identity management and authentication in the updated Framework. The Coalition particularly supports the inclusion of guidance regarding the use of multifactor authentication in the informative references, which we hope will transition the market away from passwords and other "shared secret" authentication techniques. Mature organizations increasingly use multifactor authentication processes to protect their most sensitive technology assets. However, significant barriers to the implementation of multifactor authentication processes remain, such as the continued use of legacy systems that do not support such authentication processes, the lack of standardized approaches to multifactor authentication including major differences in the quality of usability of multifactor authentication tools.. The Coalition believes that the inclusion of appropriate guidance regarding the implementation and use of multifactor authentication in the informative references will help organizations benefit from the important work that has been done to advance the development of authentication standards. However, the Coalition encourages NIST to incorporate its Electronic Authentication Guidelines, SP 800-63 in addition to NIST SP 800-53. The Coalition believes that NIST SP 800-63 provides important information and context that will facilitate organizations' adoption of the appropriate standard to strengthen their authentication practices.

[4] Please see comments filed by our individual member companies for more detail on how existing coordinated vulnerability disclosure and handling best practices and standards can be incorporated into the Framework. *See* https://rapid7.com/globalassets/_pdfs/rapid7-comments/joint-comments-to-nist-framework-revision-1.1---rapid7---041017.pdf.

International Promotion of the Multistakeholder Model that Led to the Framework. The Coalition considers the adoption of interoperable international cybersecurity standards to be critically important to the continued development of and innovation in the Internet economy. Coalition members operate on a global basis, and can attest to the importance of interoperable standards that allow for a consistent approach to cybersecurity across an organization and with partners and service providers that operate all over the world. As organizations increasingly operate on a global scale and rely on international service providers, interoperable standards are essential to organizations' ability to protect the information that they maintain across their systems and networks and to measure and evaluate the cybersecurity practices of their service providers. The Coalition believes that international alignment with the Framework would provide significant benefits for companies located in the United States, as it would facilitate their efforts to evaluate their global cybersecurity risks, make risk-informed cybersecurity decisions across their organizations, and apply a consistent standard to evaluate service providers. The Coalition encourages NIST to promote the Framework as a model for multistakeholder / public private partnerships that other countries can use when developing their own risk assessment frameworks including tenants such as openness, transparency, use of global standards, focus on security outcomes, and ability to integrate with existing risk management processes. For example, in 2015, a consortium of Italian cybersecurity academic and scientific entities led by the CINI Cyber Security National Lab released a "National Cyber Security Framework" that is modeled after the NIST Framework, with adjustments for tailoring to an Italian production context and a focus on small and medium enterprises. As other countries use the Framework as a model for the development of their own approaches, the Coalition believes that greater international interoperability will be a natural byproduct of processes that are aligned around the importance of incorporating the views of all relevant stakeholders across industry, academia, and NGOs.

Federal Alignment. The Coalition is concerned with the addition of a separate section of the document related to US federal government use. The coalition believes that including it unnecessarily makes the document more US-centric and it confuses NIST's dual missions of both creating guidance for federal agencies and convening the public sector to build frameworks. We would prefer to see a separate document for this information, even if that document is very brief.

Updating. As the Framework matures and adoption of the Framework increases both within the United States and as a model for other countries to use in developing their own frameworks, regular updating and revision will be critically important to the Framework's usefulness. While an ad hoc approach to updating the Framework may be sufficient in its infancy, the Coalition believes that a more formal approach to reviewing and updating the Framework will help ensure that it remains a useful resource to assist organizations in making risk-informed cybersecurity decisions into the future. The Coalition believes that NIST is currently in the best position to convene this updating process and to determine how frequently such updating should occur. As such, the Coalition encourages the Commission to create a formal updating process for the Framework.

Conclusion. The Coalition thanks NIST for for its leadership in coordinating this important effort and for the opportunity to comment. We look forward to continuing to work with NIST to further update and improve the Framework.