Before the
DEPARTMENT OF COMMERCE AND NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Washington, D.C. 20554

In the Matter of:	)	
	)	
Views on the Framework for Improving Critical Infrastructure Cybersecurity	)	**Docket No. 151103999-5999-01**
	)	
	)	
	)	
	)	

COMMENTS OF THE COALITION FOR CYBERSECURITY POLICY & LAW

The Coalition for Cybersecurity Policy and Law ("Coalition") submits the following comments in response to the Request for Information ("RFI") that the National Institute of Standards and Technology ("NIST") issued on December 11, 2015 regarding the uses of and potential updates to the Framework for Improving Critical Infrastructure Cybersecurity ("Framework" or "Cybersecurity Framework").

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.[1] We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity, and we are supportive of voluntary efforts to increase the sharing of cybersecurity threat indicators to help decrease response time and prevent incidents from occurring.

From the perspective of the Coalition, the Framework has been a success. The challenge for NIST under both Executive Order 13636 and the Cybersecurity Enhancement Act of 2014 has been to enhance the cybersecurity of critical infrastructure by facilitating the development of voluntary, industry-led standards, guidelines, and best practices, and encouraging the widespread adoption of those standards, guidelines, and best practices. Three years after the issuance of Executive Order 13636, and two years after NIST's publication of Version 1 of the Framework, it has emerged as a flexible, adaptive, and voluntary construct for the protection of critical infrastructure in the United States. Equally as important, in spite of its voluntary nature, the Framework has achieved a substantial degree of acceptance and adoption by critical infrastructure industries in the United States. The Cybersecurity Framework is driving the use of products and services provided by the Coalition's members, which is a positive development for the security of the nation's critical infrastructure.

[1] The views expressed in these comments reflect the consensus views 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.

The Coalition's comments focus on issues raised in the February 12, 2014 NIST Roadmap for Improving Critical Infrastructure Cybersecurity ("Roadmap"), and on the use of the Framework Implementation Tiers. In particular, the Coalition believes that increasing international coordination and collaboration will be vital to the continued success of the Framework. This includes beginning discussions of long-term governance of the Framework. The Coalition also urges focus and progress on standards in the critical areas of authentication and supply chain management. Finally, the Coalition suggests revisiting, expanding and perhaps revamping the Framework Implementation Tiers to make them clearer, more robust, and more user-friendly, and leveraging the proposed budget increase for purposes of the continuing evolution and awareness of the Framework.

I. Roadmap Issues

A. Governance

NIST has been an able and effective steward of the Cybersecurity Framework. NIST's efforts have brought clarity and focus to the daunting task of securing the information technology systems that run our nation's critical infrastructure, and have undoubtedly improved the security of that infrastructure in the short time since the issuance of Executive Order 13636.

At the same time, as NIST itself recognized in the Roadmap, NIST's strengths going forward will be to encourage "organizations to become even more actively engaged in cybersecurity issues, and to promote – and assist in the use of – the Framework as a basic, flexible, and adaptable tool for managing and reducing cybersecurity risks." The Framework itself, however, is a "living document," to evolve with substantial input from the security and critical infrastructure industries. In the Roadmap, NIST states that it will continue to serve as the "convener and coordinator" of the Cybersecurity Framework through at least Version 2.0, but that eventually it intends to transition management of and responsibility for the Framework to a non-governmental entity.

The Coalition does not believe it is necessary to begin exploring any governance change for the Framework until after the issuance of Version 2.0 of the Framework, and perhaps not until the issuance of Version 3.0. Indeed, we do not support any such transition until at least the next version is issued. Nonetheless, to the extent that NIST determines it is important to begin exploring a transition in the relatively near future, NIST should begin to consider the key issues relating to a potential spin-off of governing responsibility to a third-party non-profit entity.

There are a number of important issues on governance which must be resolved. First, no matter the governance structure of the Framework, NIST must ensure the entity overseeing the Framework guarantees it will remain unlicensed, and use of the Framework will remain free. It is not uncommon for industry standards organizations to license their work product, and to allow the use of that work product only after payment of substantial fees. Such an approach would run directly counter to the goal of

strengthening cybersecurity by encouraging widespread use of the Framework. NIST must ensure that the Framework is never subject to such licensing restrictions, and its use will remain forever free and unrestricted.

Second, NIST should explore the point at which the Framework would be considered sufficiently stable, recognized, and integrated into existing practice that its governance can be transitioned safely to a third-party non-profit. As emphasized above, NIST has been a very effective developer and manager of the Framework, and the Coalition urges that NIST remain in that role for the foreseeable future. But NIST should begin the exploration of the conditions necessary to allow an effective, non-disruptive transition to a third-party non-profit entity.

Finally, NIST should begin to explore the characteristics that a third-party non-profit entity should have in order to take over governance of the NIST Framework. From the perspective of the Coalition, it will be critical to ensure that the organization designated to manage the Framework reflect the views of the critical infrastructure and security industries. Furthermore, it will be important the entity have the expertise necessary to arbitrate the debates that are almost certain to arise out of the continued evolution of the Framework. In this respect, the successor organization and its authority should be structured in a manner very similar to the position NIST currently holds with respect to the current version of the Framework. The process that led to the current Framework was successful because NIST led an open process in which it solicited full input from all stakeholders, fully considered those comments, and then exercised its expertise to resolve all issues raised, and to come up with a final, workable Framework that has reasonably broad support in the industry.[2] It will be important any successor organization have the expertise and authority to leverage the same type of process for future iterations of the Framework. NIST should begin the process of exploring the operational and procedural attributes that should govern a third-party non-profit entity's activities in order to allow such an entity to be an effective overseer of future versions of the Framework.

B. International Alignment

The Coalition agrees with the Roadmap's assessment that "[d]iverse or specialized requirements can impede interoperability, result in duplication, harm cybersecurity, and hinder innovation" and can "hamper the ability of organizations to operate globally and to effectively manage new and evolving risks." The Coalition members provide security products and services on a global basis, and can attest to the importance of coordinated, consistent standards and interoperability. Indeed, it is

[2] In this regard, it will be important for the governing organization to strike the appropriate balance between competing industry interests and still insure that it can publish its updates in a timely manner. The process for determining the successor governing structure will have to carefully and appropriately balance these important considerations. We realize that this will not be an easy task, which is the main reason we believe this decision should be made in a process requiring an abundance of stakeholder participation and public due diligence.

because of the international presence of so many industry participants that an industry-led oversight process can assist in promoting international standardization and alignment.

NIST can take an important step towards increasing international alignment and integration by holding at least one, and preferably more than one, feedback meeting co-hosted by NIST, or another US government agency, along with foreign partners in an international location. When it developed version 1.0 of the Framework, NIST held regional feedback meetings in various parts of the United States, and these meetings helped shape the version 1.0 Framework in productive ways. In its development of version 2.0 of the Framework, NIST should leverage the experience from these regional meetings, and hold at least one international feedback meeting.

The goal of such an international feedback session is at least twofold. First, it serves to recognize the important point that there are users of the Framework outside of the United States, and that NIST is attuned to their input as well. Second, it will help influence the development of comparable frameworks in other countries. Having one framework to govern all cybersecurity practices, both domestically and internationally may be difficult to achieve as other countries are likely to want to develop their own approaches to addressing this important issue. Nonetheless, holding at least one international feedback session would send the message that NIST cares what the international community thinks, and seeks to reflect the global nature of technology development in future versions of the U.S. Framework. This approach would help in future efforts to align the NIST Cybersecurity Framework with frameworks developed by other countries.

C. Authentication

As the White House recognized in the Cybersecurity National Action Plan ("CNAP"), progress on identity management is a priority in order to make IT systems more secure. At the same time, identity management remains a challenge for many organizations. In few other areas of cybersecurity practice are the trade-offs between facilitating ease of network use and imposing security hurdles to such use as pronounced as they are in identity management. Similarly, in few other areas are the approaches to securing the IT system as varied or as complex, even within the same organization.

As reflected in the CNAP, multi-factor authentication processes reflect best practices and have the potential to significantly improve security. Multi-factor authentication processes have increasingly been used in recent years to protect an entity's most sensitive IT assets (at least where technologically feasible). However, there continue to be barriers to the implementation of multi-factor authentication processes, including, among other things, the continued use of legacy systems that do not support such authentication methods, the lack of standardized approaches to multi-factor authentication, and security assessments in specific contexts that judge ease of use (or at least lack of inconvenience) to be more important than heightened security practices.

The Coalition urges NIST to pay close attention to these issues, particularly the barriers to adoption of multi-factor authentication processes, as it updates the Framework. The Coalition anticipates that standards governing authentication will continue to evolve over the coming years, and will continue to drive improvements in this aspect of network security. Indeed, since the issuance of the Framework, important work has been done to advance the development of authentication standards, including the work on Identity Ecosystems by the National Strategy for Trusted Identities in Cyberspace, and NIST's Electronic Authentication Guideline, SP 800-63-2. Furthermore, the CNAP announces that multi-factor authentication will be central to a new National Cybersecurity Awareness Campaign that will focus on assisting consumers to make their accounts and other aspects of their online presence more secure.

The Coalition urges NIST to continue its efforts to support and develop more complete standards for authentication of individuals and automated devices, and to explore tying its ongoing authentication initiatives with those reflected in the CNAP. The Coalition also urges NIST to incorporate those evolving standards into the informative references set forth in the Cybersecurity Framework Core. Users of the Framework would then have the flexibility to adopt the appropriate referenced standards for use in strengthening their authentication practices. Finally, the Coalition urges NIST to leverage aspects of the CNAP to help address barriers to adoption of multi-factor authentication processes. In this regard, the Information Technology Modernization Fund appears particularly well-designed to help overcome the high up-front costs associated with retiring and replacing legacy systems that have security shortcomings.

D. Supply Chain Management

The Framework Core incorporates consideration of an entity's position in the overall supply chain when identifying cyber assets to be protected, but, in its current state, does not address the security of the supply chain through which such an entity acquires its IT infrastructure. The Roadmap subsequently identified supply chain issues as an area of potential focus in future iterations of the Framework.

Like other security risks, supply chain vulnerabilities present security risks to critical infrastructure owners, operators, users, and suppliers, and should be addressed, at least at a high level, and with maximum flexibility, through the Framework. Since the adoption of the Framework, important new work has been done on addressing supply chain vulnerabilities, including Supply Chain Management Practices for Federal Information Systems and Organizations, SP 800-161. This work has been informed and supplemented by more recent NIST efforts, particularly its October 2015 workshop on Best Practices in Cyber Supply Chain Risk Management. This work addresses myriad areas, including vendor selection and controls, detection and prevention of vulnerabilities in hardware and software, and implementation of controls on software design, loading, and testing processes.

Standards developed by NIST and others provide a starting point for considering how management of supply chain risks might be relevant to the use of the Framework

Core once the market has more experience with their use. The Coalition suggests incorporating relevant standards into the informative references, which will help companies use the Framework voluntarily to demonstrate that they have managed risk in their supply chain in more detail than they do today. Broader adoption and use of these standards and other recent commercial best practices can serve to inform the discussion of how to better protect the cyber supply chain, and how to incorporate new supply chain standards into the Cybersecurity Framework at an appropriate time.

II. Framework Implementation Tiers

One of the more difficult aspects of the Framework for entities to implement has been the adoption of an appropriate Framework Implementation Tier. The Tiers are meant to reflect an organization's cyber risk management achievement or risk target level. The lowest level, Tier 1, reflects an organization that is largely reactive in its cybersecurity posture, and that manages cyber risk in an informal, ad hoc manner. The highest level, Tier 4, represents an organization that is the opposite – that is proactive in managing its cyber risks, that has thorough and formal cybersecurity policies and procedures, and that is able to confront effectively the shifting cybersecurity threats to its business processes.

The Tiers are used in differing parts of the Framework evaluation process. The first is in the creation of a Target profile. This is the profile which describes the organization's agreed-to level of acceptable risk in each of the categories/subcategories. The second is in the assessment process. Organizations are able to identify the appropriate tier reflecting their cyber risk management posture after conducting an assessment using the Framework.

This dual use needs to be better clarified in the Framework. Indeed, in the experience of the Coalition members, the Framework Implementation Tiers have caused no small degree of uncertainty, largely because the criteria for designation at each of the given Tiers are fairly amorphous and imprecise. Difficulties also arise from the fact that the stringency of cybersecurity practices can sometimes vary within an organization.

For example, the difference between Tier 2 – Risk Informed and Tier 3 – Repeatable is not necessarily clear. The Tier 2 risk management process description states, in relevant part, that

> Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.

By contrast, the Tier 3 risk management process description states that the "organization's risk management practices are formally approved and expressed as policy" and that its "cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements

and a changing threat and technology landscape." This criterion appears to be very similar to the criterion in Tier 2 that prioritization of cybersecurity activities is "directly informed by organizational risk objectives, the threat environment, or business/mission requirements."

In addition to being unclear with respect to how risks are internally communicated and managed under the different Tiers, the Framework is silent on another very important aspect of an entity's risk maturity level – its participation in the cyber threat identification and information sharing ecosystem. There are now a host of industry/sector-specific 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. An entity with a mature risk management culture will have ongoing and productive interactions with its cyber ecosystem – including one or more ISACs, CERTs, or other, similar entities, as well as the government itself in some instances -- in order to share information about threats that it has identified, and to improve its protective posture against threats identified by other, similar entities and by the government. Furthermore, such an entity will have an appropriate internal process for managing information flows to and from the government and relevant ISACs, CERTs, and other organizations, and for incorporating such information into its cyber defenses. It is important that NIST's definitions of the various Tiers incorporate the myriad ways in which an entity fits within, and leverages information from, the broader cyber threat identification and information sharing ecosystem.

As the Framework evolves, it would be very helpful for NIST to clarify the criteria defining the different Framework Implementation Tiers, and to incorporate the cyber threat identification and information sharing elements outlined above. Additional rigor around what each Tier represents would facilitate the adoption of the Framework, and make it more effective in improving cybersecurity practices among critical infrastructure owners and operators.

III. Efforts to Promote the Framework

The President's proposed $5 billion increase in funding for cybersecurity programs reflects an awareness of the seriousness of the cyber threats facing the United States, and the importance of sound cybersecurity practices, both on the part of the government and the private sector. The Cybersecurity National Action Plan, in turn, reflects a recognition of the need for large-scale cyber awareness programs, and the promotion of strong cybersecurity practices, in helping businesses and the public at large to improve their protections against cyber threats.

The Coalition urges NIST to explore ways to leverage the proposed budget increase, and the widespread recognition of the need for cyber awareness, to promote the widespread use of the Cybersecurity Framework. NIST has done excellent work promoting the Framework to date, as reflected in the increasing awareness of the Framework. However, more progress can be made. Accordingly, the Coalition urges

NIST to utilize this process to review the Framework as well as opportunities from the proposed budget increase to raise awareness and promote the use of the Framework.

Furthermore, in NIST's ongoing efforts to evolve and promote the Framework, it may be important for NIST to provide additional clarity for certain entities about how to use it, and to incorporate into that guidance lessons learned from uses of the Framework to date. Indeed, for some entities that have fewer resources, particularly smaller and mid-size businesses, the Framework should be revised to provide clearer direction about how to proceed in securing vulnerable IT systems. Such an approach in the ongoing evolution and promotion of the Framework will make it easier to use, and therefore advance the goal of increasing its adoption.

IV. Conclusion

The Coalition thanks NIST for the opportunity to comment in this important effort. We look forward to working with you at your workshops and as the rest of this process moves forward.