Coalition for Cybersecurity
Policy & Law

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

January 19, 2018

VIA EMAIL: cyberframework@nist.gov

Andrea Arbelaez
National Institute of Standards and Technology
100 Bureau Drive
Mail Stop 2000
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"), regarding the second draft update of the Framework for Improving Critical Infrastructure Cybersecurity ("Framework"). 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.[1] 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 Cyber Supply Chain Risk Management ("SCRM"), Vulnerability Disclosure, 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 specificity regarding information sharing in the Implementation Tiers. The Coalition also reiterates its recommendation that NIST remove SCRM as a new category in the Framework Core, instead incorporating relevant concepts into the existing categories and subcategories. The Coalition further recommends that NIST

[1] 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.

incorporate references to the specific NIST publications that address electronic authentication procedures to provide additional guidance to organizations seeking to implement these controls.

In its request for comments, NIST indicated three questions for which we provide our responses here:

Question 1: *Do the revisions in Version 1.1 Draft 2 reflect the changes in the current cybersecurity ecosystem (threats, vulnerabilities, risks, practices, technological approaches), including those developments in the Roadmap items?*

With the exception of our specific recommends below, the Coalition generally believes that Version 1.1 Draft 2 is a thoughtful and measured approach that carefully considers the complexities of cybersecurity risk management. As a result of NIST's transparent and inclusive development process, this update represents an important evolution across several areas, without disrupting the value of Framework Version 1.0. Additionally, we believe that the Roadmap continues to serve a critical function in providing context, explanation and insight into the current and future state of the Framework and the processes surrounding it.

Question 2: *For those using Version 1.0, would the proposed changes affect their current use of the Framework? If so, how?*

The Coalition believes that the proposed changes in Version 1.1 Draft 2 represent important enhancements to the Framework that extend its usefulness by incorporating highly relevant topics such as Supply Chain Risk Management and Vulnerability Disclosure. From that perspective, the impact to use of the Framework will be demonstrated by the inclusion of the new Categories and Subcategories in the management of risk at any organization for which they are relevant.[2]

Question 3: *For those not currently using Version 1.0, would the proposed changes affect their decision about using the Framework? If so, how?*

Consistent with our response to Question 2, the Coalition believes that substantive enhancement to the Framework will likely result in increased adoption.[3]

Implementation Tiers. We recognize and appreciate the changes that NIST made to the Tiers, based in part on our previous recommendations.

While Draft 2 has extended information sharing language in the *External Participation* criteria, we note that it is only directly mentioned in Tier 1. We recommend that details regarding information sharing be included in the all the Tiers, in a manner that reflects the increasing sophistication of active participation from Tier 1 through Tier 4. The Coalition believes that additional details ("would help organizations more effectively use the Implementation Tiers.

[2] Comments provided by individual Coalition members may have additional detail regarding their specific response to this question.

[3] Comments provided by individual Coalition members may have additional detail regarding their specific response to this question.

Supply Chain Risk Management. The Coalition continues to support the inclusion of SCRM in the updated Framework. We believe 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, as stated in our previous comments, the Coalition does not believe that SCRM should be included as a separate and new Category in the Framework Core. Rather, the Coalition further urges NIST to eliminate the SCRM Category and incorporate relevant SCRM concepts into existing Categories, creating new subcategories where and if necessary.

Vulnerability Disclosure Programs. The Coalition commends NIST on adding the **RS.AN-5** sub-category and associated Informative References to Draft 2. The Coalition recommends that NIST retain this sub-category as it will assist organizations in preparing to respond to both internal and external vulnerability disclosures. Additionally, we recommend that NIST retain the discussion of coordinated vulnerability disclosure in the draft Roadmap version 1.1.[4]

While the included Information References are helpful, we note the absence of ISO 29147 and 30111 standards[5] despite their mention in the Roadmap. We recommend inclusion of these standards in the Framework itself, as informative references to RS-AN.5. This will make it clear that the subcategory covers coordinated vulnerability disclosure, help users implement the processes, and reduce the risk of users conflating it will other incident management activities.

Identity and Access Management. The Coalition applauds the inclusion of even greater detail regarding identity management and authentication in Draft 2 update. However, the Coalition reasserts that NIST should 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.

Additionally, we recommend the following changes that the subcategory level:

"**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties, including for users with enhanced privileges."

While we recognize that privileged users are included in the original text of **PR.AC-4** by default, the risk posed by such users warrants particular attention to ensure they aren't considered out of scope. This language would also ensure that PR.AC-4 is consistent with the Access Control section of NIST SP 800-53 Rev 4.[6]

---

[4] Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, Dec. 5, 2017, pg. 5, https://www.nist.gov/sites/default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf.

[5] ISO/IEC 30111:2013, Information Technology – Security Techniques – Vulnerability Handling, International Standards Organization, Nov. 1, 2013, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231. ISO/IEC 29147:2014, Information Technology – Security Techniques – Vulnerability Disclosure, International Standards Organization, Feb. 15, 2014, http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170.

[6] Specifically AC-2(7) ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES and AC-6(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

"PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor, analytics) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)"

Authentication technologies are advancing rapidly, including the use of analytics.[7] We recommend adding it to the example list to make it clear that analytics is an acceptable method when implemented correctly.

Roadmap. The Coalition is requesting that NIST include a new subsection in Section 4 of the Roadmap on "Secure Software Development Processes and Practices."

Software applications are increasingly integrated into our commercial and infrastructure processes to improve efficiencies. The global economy, critical infrastructure and government operations have increased their dependence on software. However, this makes software applications a prime target for hackers.

Many organizations fail to integrate security methods into their development lifecycle.

Recommendation action items:

- NIST can partner with leading software assurance organizations and other stakeholders, to develop risk-based, scalable guidance on effective secure software development processes and practices including: developer education, threat modeling, architectural risk assessment, code scanning an analysis, penetration testing, and continuous tracking of known vulnerabilities and attack vectors.
- NIST can work with industry and other stakeholders to develop a CSF profile focused on secure software development.
- NIST can work with international governments to promote policies that enable continued innovation and flexibility in secure software development, while strengthening security.

Finally, we note that ISO is currently developing a standard on secure application development, ISO 27034, which will address many of these best practices.

Conclusion. The Coalition thanks NIST 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.

[7] Both Gartner and Forrester have flagged the importance of analytics to a "best practices" approach to authentication this past year. See https://www.gartner.com/doc/3722317/new-approach-establishing-sustaining-trust and https://www.forrester.com/report/The+Future+Of+Identity+And+Access+Management/-/E-RES136522