Enterprise Cloud Coalition ECC

December 10, 2021

National Institute of Standards and Technology
Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930
Email: scrm-nist@nist.gov

RE: ECC's Response to Questions for Reviewers in Draft (2nd) NIST SP 800-161 Rev. 1

Dear NIST CSD Team:

The Enterprise Cloud Coalition (ECC) appreciates the opportunity to submit comments to the National Institute of Standards and Technology (NIST) Computer Security Division (CSD) team on the second draft version of Special Publication (SP) 800-161 Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2nd Draft)*.[1]

ECC is comprised of enterprise-focused and cloud-based U.S. companies with shared business models based on processing data on behalf of other companies without monetizing user data for advertising. Taking advantage of the cloud-native features and functionality available through our solutions, ECC companies are directly involved in building and advancing technology that promotes innovation while providing ethical and consumer protection-related benefits to enterprises and their customers or users. As a result, ECC promotes those policies and standards that emphasize the privacy and security of data and information.

With many of the updates to SP 800-161 relevant to efforts associated with Executive Order 14028, *Improving the Nation's Cybersecurity* (Cyber EO) and other efforts focused on the nation's technological resiliency through improved cybersecurity supply chain risk management (C-SCRM), this standard has the potential to impact the way software is designed, developed, and ultimately deployed for the next technological generation. With such a large potential impact, ECC commends NIST for seeking feedback from members of industry and the public.

This response addresses the explicit questions asked by NIST that should be helpful in finalizing SP 800-161 and any other efforts related to better managing cybersecurity risks associated with an organization's supply chain.

Answers to Specific Questions

Does the revised structure of the document with added Audience Profiles fill the need to account for the different audiences who may read the document?

Yes, the revised structure and added Audience Profiles are helpful in providing focus and relevant context to those being targeted by this document. The consistent structure of the content under each profile is also worth commending, as it will allow for a certain degree of mapping between the profiles themselves and specific job titles or work roles at an entity intending to implement a C-SCRM plan.

[1] National Institute of Standards and Technology (2021) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2nd Draft). (U.S. Department of Commerce, Washington, D.C.), NIST Special Publication (SP) 800-161 Rev. 1, 2nd Draft, 28 October 2021. https://doi.org/10.6028/NIST.SP.800-161r1-draft2

Two additions to the profiles would provide additional value and benefit: (1) a mapping of the Audience Profiles to the relevant work roles identified in section 3.4 of the NIST SP 800-181 Rev. 1, *Workforce Framework for Cybersecurity*,[2] and (2) whether applied to each Profile or to all of them generally, a list of other standards, reports, white papers, and related documents referenced that would be helpful for individuals that are new or novice practitioners, as well as topics, issues, or other standards that could be useful to those who are more advanced. Such an addition would also be helpful for public and private sector entities who are looking to identify skill gaps and those who are developing training programs as part of their organizational professional development plans necessary to achieve desired levels of internal competency and capability.

ECC encourages NIST to continue expanding on current and future Audience Profiles to make this document accessible to as many individual users of this guidance as possible. Doing so will encourage wider adoption of these practices by providing the necessary context and additional resources required to make C-SCRM an integral part of strategic thinking throughout an organization. It will also provide an opportunity for the public to provide more refined feedback, whether for interim revisions or future updates, by drafting them with certain audience profiles in mind.

Within Appendix G C-SCRM Activities in the Risk Management Process – Does the discussion of materiality in the Criticality Analysis section sufficiently address the topic as an issue or key aspect to many organizations?

Yes, the Supplemental Guidance in Appendix G provides sufficient discussion on the importance of a Criticality Analysis within a general C-SCRM plan as well as the ways in which such an analysis can be developed to provide maximal value.

An addition to the discussion, whether under the outcomes outlined in the bullets associated with performing the analysis in the Assess Step (lines 9277 to 9288) or under the considerations to take when assigning criticality levels (lines 9295 to 9309), content associated with the role of a criticality analysis in developing and maintaining a continuation of operations plan, disaster recovery plan, or similar document would be helpful. As has been discussed throughout this document, NIST's Criticality Analysis Process Model,[3] and other relevant standards and guidance referenced in Appendix J, shocks to the supply chain are one source of potentially catastrophic impacts to an entity's operations. Such an addition would both introduce a concept (i.e., disaster recovery planning) that should be part of a broader risk management approach for an entity as well as provide an additional reason why a criticality analysis is important.

ECC recommends that NIST emphasize the benefits of a criticality analysis to general operational resiliency through the expansion of Appendix G to include relevant content and, if applicable, new references that will help organizations better understand where such an analysis fits within their general risk management efforts, not just their C-SCRM efforts. Doing so will also provide the opportunity for public and private sector entities undergoing cloud migration efforts, especially those in the federal government attempting to comply with the Executive Order (EO) on Improving the Nation's Cybersecurity (Cyber EO),[4] to realize an additional benefit of their efforts, as enterprise-wide use of the public cloud, regardless of the delivery model, will be able to better withstand supply chain-related shocks among other disruptions.

Does the EO Appendix strike the right level of guidance given NIST's directive to publish "preliminary guidelines, based on the consultations described in subsection (b) of this section and drawing on existing documents as practicable, for enhancing software supply chain security and meeting the requirements of this section"?

---

[2] National Institute of Standards and Technology (2020) Workforce Framework for Cybersecurity (NICE Framework). (U.S. Department of Commerce, Washington, D.C.), NIST Special Publication (SP) 800-181 Rev. 1, 16 November 2020. https://doi.org/10.6028/NIST.SP.800-181r1

[3] National Institute of Standards and Technology (2018) Criticality Analysis Process Model: Helping Organizations Decide Which Assets Need to Be Secured First. (U.S. Department of Commerce, Washington, D.C.), NIST Internal Report (NISTIR) 8179, 11 April 2018. https://doi.org/10.6028/NIST.IR.8179

[4] Exec. Order No. 14028 (2021) Improving the Nation's Cybersecurity. (Executive Office of the President, Washington, D.C.) 86 FR 2663-26647, 17 May 2021. https://www.federalregister.gov/d/2021-10460/

Yes, the EO Appendix provides useful guidance and context for what are to be "preliminary guidelines" for protecting the software supply chain. The use of tables, references to figures or sections within the document, and the "Key Takeaways" boxes throughout the appendix are also worth commending, as it will allow for a better understanding of the ways in which each of these Cyber EO-inspired efforts are complementary to one another.

In addition to providing guidance on "[t]he EO through the lens of SP 800-161 Rev. 1," NIST should consider additional context through the reverse lens. In other words, how will the number of upcoming efforts associated with NIST's tasks under the Cyber EO be impacted by the lessons learned in developing SP 800-161. While it is very helpful to understand agencies and departments informed NIST and what particular projects have been most influential (i.e., those listed in lines 8152 to 8157), it would be useful to understand how NIST will help inform others. For example, is NIST working with the Federal Acquisition Regulation (FAR) Council on their proposed rules currently under review, the Office of Management and Budget (OMB) in developing their guidance to implement the Section 4 guidelines, or with the Cybersecurity & Infrastructure Security Agency (CISA) as they work to prioritize the C-SCRM practices that must be implemented across the federal government but take time to put together. Such an addition would provide a level of transparency and allow for a degree of planning that will better prepare industry for not only collaborating with NIST and the federal government on these future efforts, but also help make it easier to apply them to industry-standard practices by improving the ability to understand the role of C-SCRM in cybersecurity generally.

ECC recommends that NIST provide a full picture of SP 800-161 in the current cybersecurity landscape by expanding on Appendix F to include additional Cyber EO-related guidance that outlines how other efforts will be impacted by SP 800-161 and NIST. Doing so will not only help the federal government itself prepare for upcoming work but will also help industry develop the necessary capabilities to support efforts internally and in support of the federal government as federal contractors.

***

Again, ECC thanks NIST for the opportunity to provide feedback on SP 800-161 and contributing to NIST's important work in improving the security of our nation's supply chains, whether the software supply chain itself or those that depend on the use of software. We welcome questions on our feedback and look forward to continuing to be a part of this discussion as it develops.

Most sincerely,

Omid Ghaffari-Tabrizi
Enterprise Cloud Coalition
oghaffari@enterprisecloudcoalition.org
https://www.EnterpriseCloudCoalition.org/