ITI Promoting Innovation Worldwide

December 10, 2021

Jon M. Boyens
Information Technology Specialist, Computer Security Division
National Institute of Standards and Technology (NIST)
United States Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20889

Dear Mr. Boyens,

The Information Technology Industry Council (ITI) appreciates the opportunity to provide input into the second draft of the first revision of NIST Special Publication (SP) 800-161, *Cybersecurity Supply Chain Risk Management for Systems and Organizations.* ITI is the premier advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers with the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

ITI's members, who have expansive knowledge of the challenging and evolving nature of cyber threats, recognize that IT supply chain risk management (SCRM) is a crucial component of organization-wide risk management. Many of our members participate in ongoing efforts to promote sound SCRM policy, such as the U.S. Department of Homeland Security Cyber and Infrastructure Security Agency's (CISA) ICT Supply Chain Risk Management Task Force. We staunchly recognize the importance of the SP 800-161 guidance in the broader federal cybersecurity landscape, and have substantially contributed to the revision process. ITI previously submitted comments in response to both NIST's February 2020 pre-draft call for comments and the first draft of the revision published in April 2021.

General Comments:
We commend NIST for putting together a comprehensive and relevant second draft that, for the most part, reflects industry best practices. We appreciate that NIST has adopted multiple ITI suggestions from our input into the first draft document, including additional discussion of the multi-level risk management approach to SCRM, the clarification that the efficacy of a formal SCRM Program Management Office (PMO) will depend on an organization's size and mission, and the addition of new guidance on using qualified bidders lists and qualified manufacturers lists and vendor questionnaires to assess SCRM capability in the acquisition process.

Though we believe the second draft document made many positive changes from the first iteration published in April 2021, we would like to reiterate several points raised in our earlier comments submitted in June 2021. First, while the inclusion of Audience Profiles helps streamline the document's content for differing audiences who may read the new draft, we believe shortening the introductory text entirely would prove more helpful. At 323 pages, the guidance may be daunting for a new reader who is not yet familiar with cyber-supply chain risk management (C-SCRM). Moreover, while the introductory text generally conveys useful information, we feel that much of its language is duplicative and unnecessary. Thus, we recommend that NIST shorten the entire document to 100 total pages, and any additional information NIST feels is necessary to include should be divided into separate annexes. The use of appendices in the current document has made it more challenging to determine the specific practices that are being promoted. Clearly dividing the 800-161 guidance into high-level processes, specific practices, and then references (such as mappings to other publications like SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*) would significantly improve the document.

Missing from the document is a discussion of the importance of a secure development lifecycle in bolstering an organization's C-SCRM. The current draft does not reference in the Background section additional NIST or SAFECode practices on secure software development (such as NIST SP 800-218, *Secure Software Development Framework (SSDF*) *Version 1.1.: Recommendations for Mitigating the Risk of Software Vulnerabilities),* nor the ongoing work by NIST to update these. NIST should use the ongoing SP NIST 800-161 revision as an opportunity to articulate the importance of NIST's secure software development practices.

Control Additions:
ITI disagrees with NIST's addition of a net new control to SP 800-161 that was not included in the September 2020 NIST SP 800-53 Rev. 5. Rather, NIST should incorporate the new SR-13 "Supplier Inventory" control, which already refers to RA-9 as a related control, and the new MA-8 "Maintenance Monitoring and Information Sharing" control into the next revision of SP 800-53. If the drafters feel that these are important enough controls, they should include both within the pre-existing document's best practices guidance for a more mature organization.

Relationship Between the C-SCRM PMO and the Federal Acquisition Security Council (FASC):
While we appreciate the clarity added to the document's section on multi-level risk management, we feel this section would be strengthened by a discussion on the relationship between an agency's C-SCRM PMO and the Federal Acquisition Security Council (FASC), which was designed to perform an interagency C-SCRM coordination role parallel to that of the proposed C-SCRM PMO. We suggest that the final NIST SP 800-161 Rev. 1 include this consideration. Additionally, for the seven executive branch agencies that are represented on the FASC, NIST should recommend that the agency's C-SCRM PMO be led by (or at least include among its key participants) the agency's FASC liaison.

C-SCRM in Acquisition:
The IT acquisition process is a key driver of an organization's C-SCRM posture, and ITI applauds NIST for including a separate section on this topic. However, with the current phrasing, we are concerned that if a contracting officer requires adherence to NIST SP 800-161 for a specific procurement, then the inclusion of this new section may be interpreted as formal acquisition law, potentially in direct conflict with the Federal Acquisition Regulation (FAR). We recommend that NIST retain this section

but caveat it with a statement that agencies should follow the acquisition security guidance "to the greatest extent practicable."

While the document's language on optimizing C-SCRM through the acquisition process has improved significantly from the previous draft, we feel that there are several key elements missing that would have a considerable impact on a Federal agency's C-SCRM posture. First, NIST should explicitly discourage federal IT acquisition personnel from using lowest price technically acceptable (LPTA) source selection criteria for IT procurements, in line with current federal acquisition guidance. While LPTA is one of the most common source selection procedures used by Federal contracting personnel, there is a growing understanding that LPTA cannot assess the potential risk posed by a source and cannot reliably ensure the selection of the highest-performing ICT product. Additionally, because LPTA does not account for other risk mitigating actions outside of the scope of the procurement, it cannot accurately measure the total cost of an ICT product.

A FAR final rule issued in January 2021 instructs agencies to "avoid, to the maximum extent practicable," the use of LPTA for the acquisition of IT and cybersecurity services. Future iterations of the revised NIST SP 800-161 Rev. 1 should include similar language discouraging the use of LPTA for high-risk procurements. The document could address this issue by including the secure development lifecycle tie-in and best practices as a more integral part of NIST SP 800-161 Rev. 1. Moreover, NIST should assert in this section that price should be considered by contracting officers only after the technical evaluation process, when the pool has been narrowed to bidders who have "cleared the bar" in terms of C-SCRM maturity.

Second, NIST should recommend that agencies consider organizational resources when deciding whether or not to dedicate funding to C-SCRM. Agencies should be encouraged to leverage all existing IT funds to improve their C-SCRM posture. Additionally, to align with directives from Section 3 of the recent *Executive Order on Improving the Nation's Cybersecurity* for Federal civilian agencies to revise their digital transformation roadmaps and strategies to migrate to the cloud, we recommend that future drafts of NIST SP 800-161 Rev. 1 include elements on how agencies can manage C-SCRM by outsourcing their IT assets and migrating to cloud services.

Finally, ITI encourages NIST to leverage and incorporate existing standards and certifications, to the greatest extent possible, rather than create new requirements that do not add anything to what already can be achieved through existing requirements. For example, rather than requiring new attestations in the form of point-in-time scan reports, NIST should instead encourage software developers to leverage existing standards and certifications to demonstrate adequate cyber risk management. Committing to a comprehensive and dynamic cybercecurity risk management program that includes elements like scan reports is more meaningful than providing static scan reports.

New Appendices:

In general, Appendix E offers useful guidance to Federal agencies in conducting the risk assessments required by the Federal Acquisition Supply Chain Security Act. We particularly appreciate the comprehensive list of supply chain-related risk factors spelled out in the document, especially the note that no organization should use any one factor as the sole basis for making a risk decision. However, we recommend that NIST add language to this section clarifying that these risk factors should not be weighed equally, and that the decision to prioritize one risk factor over another depends heavily on the organization's mission and scope.

Additionally, we believe the content included in Appendix F provides helpful insight into how the requirements from the May 2021 *Executive Order on Improving the Nation's Cybersecurity* intersect with NIST SP 800-161. However, while it is useful to have all of the Executive Order's directives in a single appendix, this leads to unnecessary duplication of content and further reduces cohesion. For example, the content related to secure development should be included in SSDF 1.1, and the content related to EO-critical security measures should be incorporated into the appropriate C-SCRM security controls elsewhere in the document. We also recommend that NIST include in its introductory guidance language detailing the requirements from the U.S. Department of Defense's updated Cybersecurity Maturity Model Certification (CMMC) and showing where the program's underlying controls are similar to that of NIST SP 800-161.

ITI encourages NIST to streamline this document with other NIST documents and frameworks that address cybersecurity risks to ensure consistency and simplify requirements. For example, the discussion on software bills of materials (SBOMs) should refer back to the SSDF document, rather than add new requirements[1]. Additionally , ITI encourages NIST to recognize the limitations of what SBOMs can and should be used for—for instance, SBOMs should not be used as a risk or quality assessment tool during the procurement process. Furthermore, in implementing these requirements, NIST must ensure that software providers have enough agility and responsiveness to deliver timely security and functional updates. Maybe well-maintained software components have update cycles that range from days to weeks, and it's important that whatever set of SBOM requirements and tooling put in place can be incorporated into these rapid release cycles. We encourage NIST to balance these elements when providing guidance on the appropriate role and place for SBOMs.

ITI also encourages NIST to avoid creating conflicting or duplicative requirements and to consider whether there are ways to achieve the same result of addressing risk without unintentionally raising additional risk. For example, Appendix F suggests preferencing or mandating that suppliers provide a new "software security label or data sheet … that include[s] information about the software itself, the tools and technologies used to build the software, security tools and processes governing the software, and the people involved in building the software…" These requirements already are reflected in some of the proposed SBOM elements as well as SSDF practices. Requiring a new label or data sheet is duplicative of existing standards and practices and may raise additional risks by making this information readily available to cyber criminals. A better way to address this risk is to require compliance with existing standards, such as those in the SSDF that require participation in vulnerability disclosure programs and using industry standard secure development tools, rather than requiring a new label or data sheet for suppliers. The inclusion of the reference to "people" also is a new concept that may be difficult for suppliers to implement and may raise additional concerns.

[1] For additional thoughts on SBOMs, see https://www.ntia.doc.gov/files/ntia/publications/information_technology_industry_council_-_2021.06.17.pdf

Thank you for your consideration of our comments. We hope that ITI can serve as a resource to NIST as it continues the important work of revising the NIST SP 800-161 guidance. If you have any questions or would like to discuss our comments in greater depth, please don’t hesitate to reach out to Kelsey Kober, Senior Manager of Policy, Public Sector, at kkober@itic.org or 202-570-1177.

Respectfully submitted,

Gordon Bitko
Senior Vice President of Policy, Public Sector
Information Technology Industry Council (ITI)