July 18, 2014

Mr. Jon Boyens
National Institute of Standards and Technology
ATTN: Computer Security Division, Information Technology Laboratory
100 Bureau Drive - Mail Stop 8930
Gaithersburg, MD 20899-8930

Re: ITSCC Comments on NIST Special Publication 800-161, Second Draft: Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Dear Mr. Boyens:

The Information Technology Sector Coordinating Council (IT SCC) respectfully submits the following response to the request for comments on the second draft for National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161 Supply Chain Risk Management Practices (SCRM) for Federal Information Systems and Organizations. Our membership represents a broad range of companies that are an integral part of the global Information Technology (IT) supply chain and we share the goals of NIST and the U.S. Government in protecting the security and integrity of IT hardware, software and networks. As with the previous draft of SP 800-161 and other IT SCRM-related publications issued by NIST, we appreciate the opportunity to contribute to the development process and provide input that reflects the experiences and perspectives related to the commercial operations of the IT industry and the markets we serve.

In reviewing the second draft of SP 800-161, we are pleased to see that NIST has incorporated a number of suggestions from the IT industry that have improved portions of the document. NIST is to be commended for including these changes. In particular, we are encouraged that the practical and cost implications related to the U.S. Government imposing new SCRM processes and controls for IT-related acquisitions now receive greater emphasis. This is a critical point as the vast majority of IT companies currently invest considerable amounts of money and resources to ensure that our products are secure and comply with a broad range of industry best practices, standards, quality assurance measures and government regulations. Should U.S. Government agencies seek to impose additional SCRM requirements, additional costs, limits on system and component availability and competition, as well as other challenges that will result for affected IT hardware, software, and networking products and services.

With regard to SP 800-161, Draft 2, the IT SCC recommends NIST consider the following points and address the issues raised in future drafts of the publication.

Focus on High Impact Systems and Improved Guidance to Agencies on the Impact of Applying SCRM Controls to Lower Impact Levels or Specific Components: The Draft explains the guidance and controls in the publication are "recommended for use with high-impact systems," as described by Federal Information Processing Standard (FIPS) 199 (Page 2, lines 404-406). This is an appropriate application of SP 800-161 given the considerable risks associated with FIPS 199 high impact systems; the additional expense and limitations that the U.S. Government will incur for the controls and guidance described in the publication are understandable. The Draft further states, however, that "because of interdependencies and individual needs, agencies may choose to apply the guidance to systems at a lower impact level or to specific system components" (lines 406-408). The IT SCC understands the need for agencies to have flexibility to make appropriate decisions based on specific circumstances and that those agencies that have designated certain systems as FIPS 199 moderate impact systems may have legitimate needs for additional risk management controls. We recommend, however, that NIST add additional guidance and explain the impact of such decisions on acquisitions, including the additional costs associated with agency assessment and acquisition processes, as well as the potential impact related to the cost, availability and competition to acquire and maintain systems and components for lower impact level acquisitions. The support structures, requirements and costs for high-impact systems are much more expensive and onerous for both agencies and suppliers than lower impact levels, and even limited application of SCRM controls for lower levels will result in significant cost and operational complexities for agencies. In short, agencies should be fully informed and carefully consider all implications of designating additional SCRM controls for an IT system or component.

Greater Emphasis on the Use of Industry Standard Practices and Certifications for Security Assessments and Compliance with Control Requirements: The IT SCC has consistently recommended that industry standards are an effective and efficient means for agencies to recognize effective practices that suppliers have implemented that help manage supply chain risks. We are encouraged that the Draft recommends that agencies may use external assessment authorities and certifications as part of the security assessment process and cites several leading industry standards (Pg. 66, CA-2 SECURITY ASSESSMENTS). Given the importance of recognizing supplier adherence to current industry standards and certifications to any security assessment, we believe greater emphasis throughout the publication on the use of recognized industry standards to meet SCRM control requirements is not only warranted, but necessary. Further, we recommend that the list of recognized industry standards should be expanded to provide greater awareness of those that are related to SCRM by implementing agencies. The IT SCC is prepared to assist with providing additional input regarding specific standards and standards bodies if it would be helpful to NIST.

Reduce Complexity and Length of SP 800-163 to Improve Clarity: The sheer amount and presentation of the information contained in the draft publication is daunting and presented with an unnecessary level of complexity. Reducing the length of the document to less than 100 pages through further consolidation and editing so that the wording is more concise would enhance the utility of the document considerably.

Significantly Revise the Impractical Guidance on the Control for Provenance: Many IT SCC members serve global markets and operate as part of the global ICT supply chain. As such, they currently maintain robust tracking and controls systems for their products and operations, including some that are required of U.S. companies to comply with U.S. customs and export requirements and other laws and programs. The IT SCC is concerned that the provenance-related control contained in DRAFT 800-161 may result in duplicative or impractical requirements from agencies, particularly if they are implemented differently by each agency. The IT SCC recommends that the provenance control besignificantly revised to provide guidance for agencies to recognize existing provenance management systems that companies have in place.

Agency Processes Should Include Formal Advisory Exchanges for the Development and Implementation of SCRM Policies and Controls: The current Draft recommends an ongoing dialogue between acquirers and ICT suppliers. Pages 8-9 suggest that acquirers "establish a dialogue with the ICT suppliers regarding the possibility of implementing ICT SCRM processes and controls in this publication," noting that "ICT suppliers might not be able to offer significant tailoring or choose not to modify their processes or products to support federal agency security and ICT SCRM requirements" (lines 546-553). The IT SCC is interested in working with NIST and agencies to develop an approach for the exchanges that is open, transparent, scalable and appropriately leverages the technical and operational expertise of industry."

Vendor Notice of Denial/Non-Compliance and Appeal: We understand that the controls described in SP 800-161 Draft 2, like any NIST SP controls, will not be placed directly on bidders and suppliers per se, but rather be translated by the department or agency that chooses to use them through purchase-related documents such as a "sources sought notification" or an RFP. Procedures for notification of whether a bidder meets the requirements and is chosen, as well as due process regarding bid results, are currently governed by existing regulation in the Federal Acquisition Regulation (FAR) and the various agency specific supplements to the FAR. For ongoing SCRM policy compliance issues, however, we suggest that the federal government establish a separate, clearly defined process requiring notification to any disqualified supplier, so that they can know why they are excluded from consideration, and a process to appeal or rectify any specific deficiencies, so that the supplier has a way to remedy the problem and re-establish eligibility for competition.

In conclusion, we note that we understand SP 800-161 is a work in progress and we are encouraged by the progress made to date and the commitment to industry inclusion. We welcome the opportunity to continue to work with NIST to refine the process and help ensure that recommendations, processes and controls contained in the publication are reasonable and effective. Please contact Angela McKay, Chairman of the IT SCC and Director of Cybersecurity Policy and Strategy for Microsoft Corporation, or Steven Kester, Director of North America Government Affairs for AMD, if you have any questions or would like additional information.

Sincerely,

Angela L. McKay

Angela McKay
Chairman, IT SCC
Director of Cybersecurity Policy and Strategy, Microsoft

Steven Kester
Co-Chair, Supply Chain Risk Management Working Group, IT SCC
Director, North America Government Affairs
AMD