Information Technology
Industry Council

SIA SEMICONDUCTOR
INDUSTRY
ASSOCIATION

November 1, 2013

Mr. Jon Boyens
Senior Advisor, Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 893
Gaithersburg, MD 20819

Via e-mail to: scrm-nist@nist.gov

RE: Response to NIST SP 800-161, "DRAFT Supply Chain Risk Management Practices for Federal Information Systems and Organizations"

Dear Mr. Boyens:

The Information Technology Industry Council (ITI) and Semiconductor Industry Association (SIA) appreciate the opportunity to comment on NIST SP 800-161, DRAFT Supply Chain Risk Management Practices for Federal Information Systems and Organizations. We are submitting our comments both in this letter and the comments template provided.

ITI is the premier voice, advocate, and thought leader for the information and communications technology (ICT) industry. ITI's members comprise the world's leading hardware, software, and services companies with extensive ICT supply chains. As both producers and consumers of ICT products and services, our members have extensive experience working with the U.S. Government—as well as governments around the world—on the critical issues of cybersecurity policy and government procurement.

SIA is the voice of the U.S. semiconductor industry, one of America's top export industries and a bellwether of the U.S. economy. Semiconductor innovations form the foundation for America's $1.1 trillion technology industry affecting a U.S. workforce of nearly six million people. SIA seeks to strengthen U.S. leadership of semiconductor design and manufacturing by working with Congress, the Administration, and other key industry groups. SIA encourages policies and regulations that fuel innovation, propel business, and drive international competition to maintain a thriving semiconductor industry in the United States.

As you are aware, industry shares the government's interest in security of ICT supply chains. We understand federal departments and agencies are increasingly asking NIST which current controls should be used for SCRM (for example, which SP 800-53 controls would be appropriate), and we understand NIST is trying to answer that need with SP-161. ITI and SIA appreciate NIST's strong commitment to outreach and engagement with stakeholders regarding ICT supply chain issues in an attempt to come to effective policy guidance for federal departments and agencies. We also appreciate your continued efforts to refine this document, which has been under development for the last few years.

SP-161 has some important improvements over its predecessor, NISTIR 7622, including removal of the reference to acquisition and procurement (which is the purview of GSA). The addition of language making clear to those to whom this document is targeted—the federal departments and agencies that acquire ICT products and services—that implementing SCRM practices will have "cost and scheduling constraints" (p. 7) is a very welcome addition, although we do think that fact must be made earlier and more explicitly, as we describe below. We also appreciate the efforts to more explicitly map this document to existing NIST guidance.

At the same time, we have some concerns about this document. We continue to believe that in some places the document mistakenly implies that a federal agency has "management oversight" over the entire product life cycle, much of which is and must remain the responsibility of vendors—at least when the government chooses to purchase commercial-off-the-shelf (COTS) technologies. ICT COTS companies conduct a range of activities to manage global supply chain security risks, including counterfeits, throughout their product lifecycles. The attached appendix details activities that both ITI and SIA member companies undertake. Further, some of the suggested practices in SP 800-161, such as anti-counterfeiting measures, are already being addressed via DoD through anti-counterfeit product marking, multinational customs enforcement efforts, and the like, and therefore we question the value of including them here and worry that doing so could create redundant or conflicting efforts within the federal government.

We will not make specific suggestions to improve the areas mentioned above, however, as we have raised these concerns to NIST on past versions. We will focus our input on three other areas: 1) suggestions for the abstract and introduction; 2) some specific line-item suggestions (see attached matrix); and 3) suggestions regarding due process and contracting. The due process and contracting items may not be appropriate to include in SP 800-161 but we suggest be addressed elsewhere in federal guidance or documents.

Suggested Improvements: Abstract and Introduction

We find this document difficult to understand due to its length and density. Although we realize it is aimed at technical people accustomed to following NIST guidance, we believe the abstract and introduction could benefit from substantial reorganization and tightening so that the document's purpose is clearer and it can be better understood from the policy perspective. This can help reduce confusion among some readers. We also suggest that some key concepts, facts, and definitions be highlighted much more strongly, such as in text boxes. Our specific recommendations for improvements to the abstract and introduction along these lines are below and we hope they are constructive criticism for consideration. Aside from the abstract, we did not propose revised text, but would be happy to provide more detailed wording suggestions if that is of interest.

Bring key facts about SP 800-161 into abstract. The abstract currently lacks key facts about the document. The two paragraphs about supply chains and government visibility into them should be shortened to 1-2 sentences and other key facts added.

A suggested revised abstract is below.
Federal government information systems have been rapidly expanding in terms of capability and number, with an increased reliance on outsourcing and commercially available (commercial-off-the-shelf, or COTS) products. To create leading-edge, affordable COTS products, COTS suppliers use increasingly complex, globally diverse, and scaled information and communications technology (ICT) supply chains. Federal acquirers are concerned about procuring counterfeit ICT products or those with unwanted functionality, and fear that the increasingly complex supply chains decreases their visibility into, and understanding of, how the technology they are acquiring is developed, integrated and deployed, as well as the processes, procedures, and practices used by suppliers to assure the integrity, security, resilience, and quality of the products and services. Currently, federal departments and agencies use varied and nonstandard practices to select and implement processes and controls, which makes it difficult to consistently manage and measure ICT supply chain risks across different organizations.

NIST Special Publication (SP) 800-161 provides guidance to federal departments and agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels in their organizations. SP 800-161integrates ICT supply chain risk management (SCRM) into federal agency enterprise risk management activities by applying a multi-tiered SCRM-specific approach, including supply chain risk assessments and supply chain risk mitigation activities and guidance. NIST SP 800-161 is based on existing NIST publications, with additional SCRM guidance provided when necessary.

Bring key facts about SP 800-161 into beginning of the introduction. The first few paragraphs of the introduction should clearly include the following points, most of which are buried in various places in the introduction's nine pages.

- Why the document exists (the government is concerned about procuring counterfeit products or those with unwanted functionality) (p. iii)
- How the document is expected to help to improve the security of federal information systems
- That the government seeks to establish a consistent, government-wide approach to ICT SCRM practices
- The audience for this document (federal agency personnel involved in engineering/developing, testing, deploying, acquiring, maintaining, and retiring a variety of ICT components and systems) (p. 6)
- That implementing SCRM requires departments and agencies to establish a coordinated team-based approach to assess and manage risk (p. 6)
- That the document is recommended for use when procuring high-impact systems (p. 6)
- That the document is a set of unified information security guidance based on existing sets of controls, specifically SP 800-53 REV 4 and others (pp. 5-6)
- That agencies and departments should take an incremental approach and ensure that they first reach a base level of maturity in these organizational practices prior to specifically focusing on more advanced ICT SCRM practices (pp. 7-8)
- That, because the government relies heavily on COTs products, implementing ICT SCRM practices will have cost and scheduling constraints (p. 7)

Insert text boxes or otherwise flesh out the following points. There are some key definitions, facts, and explanations that are not clear and would benefit from additional information early in the document.

- Key definitions of entities, including of organization, supplier, and acquirer.
- Description of the complexity of ICT supply chains. There currently is a description in the first two paragraphs of appendix, and p. 1. A text-box description should make clear that ICT supply chains are extremely globalized and use multiple tiers of distribution channels.
- Description of the ICT supply chain risks that are of concern/related to government information systems. Page 2 has a narrative and figure, but it would be helpful to put these together in a text box. The text box should include a sentence reminding the reader that there are helpful threat scenarios later in the document.
    - In this section, it would be appropriate to add a few sentences affirming that industry has its own processes to manage ICT supply chain security.[1]
- Explanation of why the federal government purchases COTS products, and that any non-standard practices the government requests suppliers to take related to ICT SCRM will raise costs to the government.

General tightening. Overall, many descriptions in the introduction are unnecessarily long. Tightening many of these sections will make the document much more accessible and quickly understandable. For example, the three paragraphs describing the target audience (1.2, p. 6) could easily be condensed.

Specific Line-Item Suggestions

Our specific line-item suggestions are not extensive and are in the attached matrix. We assume NIST will receive much more detailed line-item feedback from individual companies.

Other Suggestions

Due process: We understand that these controls, 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. 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), Defense Federal Acquisition Regulation Supplement (DFARS), and General Services Administration Acquisition Regulation (GSAR) and are under the clear purview of GSA, DOD, and the FAR Council. However, particularly for ongoing SCRM policy compliance issues, we suggest another mechanism be put in place to ensure that a disqualified supplier can know why they are excluded from consideration and has a process to appeal.

[1] Our attached appendix details examples of activities that companies undertake to manage ICT supply chain security risks.

Contracting language: Previous NIST SCRM guidance, such as SP 800-53, was addressed to agencies and departments for management of their internal operations, and did not define specific procurement requirements. SP 800-161 departs from this practice by making specific recommendations for actions of suppliers. Thus, it might be helpful for the Administration to create consistent, government-wide contracting language. We understand NIST's distinct role to develop technical security guidance, whereas the General Services Administration (GSA) and Office of Management and Budget (OMB) develop acquisition and contract guidance—and therefore contracting language is not appropriate for this document. However, consistent contracting language through which these ICT SCRM controls are translated by agencies/departments would provide predictability for suppliers. ITI would appreciate conversations with the appropriate GSA and OMB offices to determine if and how to develop any accompanying contracting language. In particular, any non-commercially used, government-unique requirements will need to be addressed by negotiating modification of contract terms or via the FAR that provide opportunities for public comment. If the contract requirements depart too grossly from common commercial practices, commercial suppliers may choose not to do business with the government.

Conclusion

Thank you very much for your consideration. Please do not hesitate to contact us with any questions at dkriz@itic.org or dtodd@semiconductors.org. We look forward to continuing to work with you on this very important topic.

Sincerely,

Dustin J Todd

Danielle Kriz
Director, Global Cybersecurity Policy
Information Technology Industry Council

Dustin Todd
Director, Government Affairs
Semiconductor Industry Association

Attachments:

- Appendix of Industry Practices to Manage ICT Supply Chain Security Risks
- Comment Matrix

APPENDIX: INDUSTRY PRACTICES TO MANAGE ICT SUPPLY CHAIN SECURITY RISKS

SUPPLIED BY ITI AND SIA

Information Technology Industry Council

ICT Industry Activities to Manage Global Supply-Chain Security Risks

Within any supply chain, as with any activity, there are risks. Risks exist during product development, manufacturing and shipment. Because these risks threaten the core of ICT businesses (our products) our sector is highly motivated to combat these risks with the same innovative focus we apply to our own product development. For ICT companies, the primary focus is the integrity, reliability and functionality of the product at hand. To advance these goals, companies assess a range of risks, including evaluating the security properties of inbound components and products as well processes and testing throughout the products lifecycle. These processes help guard against the risks of both malicious and unintentional vulnerabilities that may be inserted during the product development process.

The ICT industry manages supply-chain security risks in numerous ways. It is important to note that due to the various types of risk and their impact on such a wide variety of products in the communications sector, there is no single activity that protects all global ICT products. Instead, ICT companies utilize many different practices in concert based on an assessment of risk, which can be unique to each company's situation.

Company-specific activities: Individual ICT companies have been managing supply-chain security risks for years, and as a result, they have deep expertise on the practices that are best suited to mitigate their particular risks. Our companies undertake a number of activities to secure their supply chains.

- <u>Product development practices.</u> These practices span from product concept to completion. They include providing security training for product developers, defining security requirements at the outset of product development, identifying and addressing potential threats in the early design phases (e.g., threat modeling and mitigation planning), teaching and instilling secure coding practices, teaching and instilling secure code handling practices, conducting product testing to validate that security practices have been met, and security documentation.
- <u>Purchasing from authorized suppliers, using contracts as enforcement.</u> One way in which the technology industry seeks to ensure supply chain integrity is through the use of authorized distributors and/or resellers. In an authorized relationship, each supplier identifies and qualifies their authorized distributors and/or resellers using a broad set of criteria, which includes legal and regulatory compliance, long-term business viability, quality systems, order placement and fulfillment processes, customer support policies, and other contractual requirements. Contracts provide enforcement mechanisms and a range of potential actions, from remediation, to termination, to legal action. In addition, suppliers periodically audit their distributors to ensure product management and

contractual provisions are properly executed. Similarly, purchasing only from authorized distributors and resellers is one simple way that the U.S. government can gain higher levels of assurance than if it chooses to purchase from unauthorized sources.

Industry-wide standards activities: More recently, industry has been working together in multiple forums to develop common best practices, controls, and standards for supply-chain risk management. Several industry-wide standards and best practices address ICT supply-chain risks. Our companies contribute to developing such standards on a global, voluntary, and consensus basis through a range of organizations. Examples of supply-chain security standards include a variety of International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards, including:

- ISO/IEC 15408, which serves as the basis for the Common Criteria, the global IT security certification arrangement. A pilot is underway to incorporate supply-chain risks in the Common Criteria evaluations of IT products. It is important to note that the Common Criteria is an agreement among the governments of 26 mostly developed nations. The U.S. is represented in the Common Criteria by the National Information Assurance Partnership, which is led by the National Security Agency; and
- The ISO/IEC 27000 risk management framework, which will include a component under development to address supply-chain security (27036, information security for supplier security).
- SAE-AS5553, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition" is an industry best practice.

In addition, other activities include:

- The Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services.
- The Open Group Trusted Technology Forum (OTTF) is an industry-led global standards initiative that aims to shape global procurement strategies and best practices that help to reduce threats and vulnerabilities in the global supply chain. The U.S. Department of Defense is a member of the OTTF.

The standards efforts above are global, with participation and contributions from companies from all over the world. In addition, many of them include government participation—not as dominant players, but as distinct stakeholders with interests in the outcome.

Again, it is important to stress there is no one-size-fits-all "supply-chain security standard" or set of practices applicable across the board. The security practices a particular company chooses depend on its products, services, markets, and business methods. In addition, industry continually updates existing standards or establishes new standardization efforts addressing emerging cybersecurity risk concerns. Thus, the government should recognize and support these activities, but not mandate any one standard, approach, or activity. Such an inflexible approach would likely divert resources away from addressing emerging risks and challenges, thereby decreasing security. Given the substantial time and resources the government would need to devote to identifying standards and writing them into contracts, the reality is that any government –required standards will be static, rather than evolving to address changing threats. Security standards evolve as new threats and vulnerabilities emerge, and new products and technologies emerge as well. *Today's best practice can be outdated tomorrow.*

SIA SEMICONDUCTOR
INDUSTRY
ASSOCIATION

Introduction to industry efforts to combat counterfeits

The semiconductor industry is inherently security-sensitive in terms of the design, sourcing, manufacture, and distribution of our products. U.S. semiconductor companies operate under robust and mature security practices and protocols, and the industry has long been subject to strict export control regulations and other legal and regulatory regimes designed to assess, monitor, and control access to semiconductor-related technologies and products. Semiconductor products increasingly have built-in security features that are used to protect system hardware from a cyber-attack, as well enhance the operation of other hardware and software based security features and end-use products. In many cases, the government can advance its security interests by improving upon existing practices, without the need for new requirements or mandates. While the semiconductor industry believes that counterfeit risks can best be mitigated by procuring semiconductors from authorized channels, the industry is taking many other steps to ensure the flow of secure, reliable, and authentic semiconductors into the supply chain. A few examples of industry action include the following:

- Incorporation of security features into semiconductors – semiconductor companies incorporate risk appropriate technologies into their products to help promote security and authentication.
- Secure personnel policies – semiconductor companies implement rigorous personnel practices to safeguard product design, manufacturing, and distribution operations.
- Developing a research agenda – SIA and members companies have a long history of working in close partnership with the government and universities on research, including efforts to promote product and systems trust and assurance. The Semiconductor Research Corporation (SRC), the industry's collaborative research consortium, is leading an industry initiative to identify and address research priorities aimed at strengthening security and trustworthiness throughout the design and manufacture process.
- Cooperation with law enforcement – SIA and member companies have cooperated with the arrest and prosecution of people who have made, imported, and sold semiconductor counterfeits. These counterfeits were destined for critical applications such as a high speed train braking system, radiation detection instruments used by first responders, and a Navy vessel Friend-or-Foe identification system.
- Partnerships with government – SIA and member companies work closely with governments to promote product security and authenticity. For example, for semiconductors that are used in special military or space applications, the government

and industry have established a “trusted supplier” program. The industry also works with government to address the challenge of counterfeit products.

Buying from Authorized Sources to Mitigate Counterfeit Risks

Improper purchasing practices are the primary reason that counterfeit semiconductor products have proliferated. Counterfeit components reported to semiconductor companies and reported through the Government-Industry Data Exchange Program (“GIDEP”) invariably involve purchases from sources that are not authorized by the original component manufacturers (“OCMs”) to sell their company’s semiconductor products. The OCMs sell their products directly through their own network of authorized distributors and authorized resellers. The OCMs authorize and manage their networks to meet stringent handling, storage, and transportation requirements to protect the semiconductors from damage; this allows the products to be covered by the OCMs’ full warranties.

Fortunately, contractors and subcontractors are able to easily avoid counterfeits by always buying semiconductor components either directly from OCMs or directly from OCMs’ authorized distributors and authorized resellers. With regard to older, out-of-production semiconductors (“legacy products”) that are not available from OCMs directly or through OCMs’ authorized distributors and authorized resellers, purchasers can avoid buying counterfeits because these products are still generally available through aftermarket distributors and manufacturers that are authorized by OCMs to buy end-of-production products and/or obtain licensing to manufacture the original products. These authorized aftermarket distributors and manufacturers literally have billions of older products that meet all of the OCM’s storage, handling, transportation, performance and reliability requirements. In many cases, these products are available for immediate delivery.

The only way to ensure that semiconductor components are authentic, and meet the manufacturer’s quality and reliability specifications, is to buy them exclusively through OMs or their authorized sources. No other sellers are approved or authorized by the OCMs. These non-authorized (“open market”) sources include independent distributors, brokers, on-line component exchanges, and other companies and individuals that obtain products from a wide range of suppliers. Some suppliers either intentionally or unknowingly introduce counterfeits into the non-authorized supply chain. Even if components purchased from non-authorized sources are authentic, they may not have been properly handled and stored and may therefore risk future performance and reliability problems. Therefore, non-authorized components may not be authentic, may not be reliable, and are not covered by the OCM’s warranty.

More information on using authorized sources to mitigate the risks of procuring counterfeits can be found at http://www.semiconductors.org/document_library_sia/anti_counterfeiting/sia_whitepaper_winning_the_battle_against_counterfeit_semiconductor_products/?query=category.eq.Anti-Counterfeiting&back=DocumentSIA

DRAFT NIST SP 161 COMMENT MATRIX

Date: 2013-08-16

1	2	3	4	5	6	7	8
Comment #	**Organization** **Name**	**Chapter/ Subsection Appendix** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change)**	**Proposed change**	**Resolution on comment**
1.	ITI /SIA		Table 2-8	ed	In Tier 3, a mitigation is to "initiate engineering change."	Confirm the engineering change would be in agency's own system, not a requirement for a supplier to engineer change.	
2.	ITI/SIA	Chapter 3, p. 85		te	The requirements in 800-53 SA-12 (14) as referenced in this section stipulate that "Identification methods [such as labelling or tagging] are sufficient to support the provenance in the event of a supply chain issue or adverse supply chain event." The use of serial number labels and shipment tagging is currently common commercial practices. However, SP 161 stipulates that: "Acquirers, system integrators, suppliers, and external service providers should maintain the provenance of systems and components under their control to **understand where the systems and components have been, the change history, and who might have had an opportunity to change them**." This is not a common commercial practice by COTS suppliers or external service providers (e.g. cloud). This recommendation goes much further than the use of labeling of product containers or tagging of	**SP-161 - Provenance** is a new control family, developed specifically to address ICT supply chain concerns. All systems and components originate somewhere and may be changed throughout their existence. The record of system and component origin along with the history of, the changes to, and the record of who made those changes is called "provenance." Acquirers and their system integrators, should maintain the provenance of systems and components under their control to understand where the systems and components originated, their change history while under government control, and who might have had an opportunity to change them. Provenance allows for all changes from the baselines of systems and components to be reported to specific stakeholders. Creating and maintaining provenance within the ICT supply chain helps government	

1 **Type of comment:** **ge** = general; **te** = technical; **ed** = editorial

DRAFT NIST SP 161 COMMENT MATRIX

Date: 2013-08-16

1	2	3	4	5	6	7	8
Comment #	**Organization** **Name**	**Chapter/ Subsection Appendix** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change)**	**Proposed change**	**Resolution on comment**
					shipments. Maintaining the change history of an individual products, or requiring service providers to report all routine maintenance, software updates or other changes to their systems, would be a significant burden that would drive up costs. Further, if SP-161 is intended to require suppliers to provide a complete Bill-Of-Material breakdown for all the components in a product and/or information about the manufacturer's sub-component suppliers, it would create a huge information burden that would significantly increase the cost of doing business with the Federal government.	agencies achieve greater traceability in case of an adverse event and is critical for understanding and mitigating risks. COTS suppliers (e.g. OEMs or authorized distributors) and external service providers may use pprovenance to demonstrate that the source of goods (e.g. computer hardware or software) are genuine and not counterfeit.	
3.	ITI/SIA	Abstract		Ed	See attached letter	See attached letter	
4.	ITI/SIA	Introduction		Ed	See attached letter	See attached letter	
5.	ITI/SIA	Lines 1081-1084, Page 28-29: CRITICALITY ANALYSIS:		Ed	The Supplemental Guidance section on Criticality Analysis states as follows: "When identifying critical functions and associated systems/components and assigning them criticality levels, consider the following: • Logic-bearing components are especially susceptible to malicious alteration	We ask that NIST strike the specific reference to logic-bearing components.	

1 **Type of comment:** **ge** = general; **te** = technical; **ed** = editorial

1	2	3	4	5	6	7	8
Comment #	**Organization** **Name**	**Chapter/ Subsection Appendix** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change)**	**Proposed change**	**Resolution on comment**
					throughout the program life cycle;" ITI and SIA object to this statement, which is inaccurate, unjustified, and creates bias by treating this specific class of products differently than other key system components and elements. There are many components that comprise a system and multiple potential vulnerabilities at multiple levels and layers of systems and networks. Treating logic-bearing components as a special class is not only unwarranted, it also de-emphasizes other potential vulnerabilities and threats..		
6.	ITI/SIA	Page 80 – Control Information System Architecture/Supplier Diversity		Ed	ITI and SIA recommend that NIST include language that recommends that acquiring agencies only purchase directly from qualified original equipment manufacturers (OEMs) and original equipment manufacturers (OCMs,) or their authorized distributors and resellers. Lines 6-9 show where this language should be added.		
7.	ITI/SIA	Page 85 – Provenance		Ed	See above		
8.	ITI/SIA	Page 88 – Risk Assessment		Ed	See above		

1 **Type of comment:** **ge** = general; **te** = technical; **ed** = editorial

DRAFT NIST SP 161 COMMENT MATRIX

Date: 2013-08-16

1	2	3	4	5	6	7	8
Comment #	**Organization** **Name**	**Chapter/ Subsection Appendix** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change)**	**Proposed change**	**Resolution on comment**
9.	ITI/SIA	Pages 89-90 – SCRM_SA-4 Acquisition Process		Ed	See above		

1 **Type of comment: ge** = general; **te** = technical; **ed** = editorial