Information Technology Industry Council

IT Alliance for Public Sector

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

Dear Mr. Boyens:

On behalf of the Information Technology Alliance for Public Sector (ITAPS)[1] and the Information Technology Industry Council (ITI),[2] we are responding to the request for comments on the second draft of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161, *Supply Chain Risk Management Practices (SCRM) for Federal Information Systems and Organizations*. This SP seeks to provide guidance to federal agencies on identifying, assessing, and mitigating information and communications technology (ICT) supply chain risks at all levels of their organizations by showing agencies how to incorporate SCRM into their organization's risk management activities. ITAPS and ITI commend NIST for engaging industry over the past six years to develop guidance for ICT SCRM. We appreciate this opportunity to share our perspectives and comment on the latest SP 800-161draft.

NIST incorporated several changes in the recent update to reflect comments from stakeholders. In particular, we would like to thank NIST for incorporating many of the changes ITI suggested to the first draft of the SP.[3] By reorganizing, tightening, and bringing key facts about SP 800-161 into the introduction, NIST has made clearer the publication's purpose, thereby lessening confusion and making the SP more understandable from a policy perspective. Importantly, the second draft makes more apparent to agencies that the benefits that may result from implementing the ICT SCRM processes and controls should be weighed against likely accompanying costs. These include costs to the agency directly (e.g., financial and human resource requirements, as described in the text box on p. 14) as well as indirect costs (e.g., non-standard practices the government might request suppliers take related to ICT SCRM that could raise costs of the products or services in questions and therefore likely increasing prices to the government acquirer as described in text boxes on p. 9 and 14 and in the narrative, lines 537-541 and 553-555). Finally, we also thank NIST for incorporating some of our line-item suggested edits to specific controls.

[1] The IT Alliance for the Public Sector (IT Alliance, ITAPS), a division of ITI, is an alliance of leading technology companies (including ICT companies and the defense industrial base (DIB)) offering the latest innovations and solutions to public sector markets. With a focus on the federal, state and local levels of government, as well as on educational institutions, the IT Alliance team advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants. Visit itaps.itic.org to learn more.

[2] The Information Technology Industry Council (ITI) is the premier advocacy and policy organization for the world's leading information and communications technology (ICT companies). ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world. Visit www.itic.org to learn more.

[3] ITI's Response to NIST SP 800-161 (November 2013)

ITAPS and ITI share the government's interest in the security of ICT supply chains. Our members have complex supply chains spanning multiple countries where products and services are developed, made, assembled, and distributed across the world. Supply-chain security practices are critical to our members' success. The protection of our customers, our brands, and our intellectual property (IP) are essential components of our business and our ability to grow and innovate in the future. Entities within the supply chain ecosystem depend on each other to develop, integrate, and use ICT products and services. We seek to maintain the highest levels of integrity in our products and services, regardless of whether they are sold to commercial or government markets. Moreover, as both providers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity and supply chain policies, and we are committed to working with the U.S. federal government to improve cybersecurity in its acquisition of goods and services.

Our input below is focused on suggestions in the following key areas: 1) the SP's introduction; 2) some specific line-items/controls (see attached matrix); 3) reducing the size of the SP; 4) using industry SCRM practices; 5) segregating SCRM from other controls; 6) vendor notice of denial/non-compliance and appeal; and 7) training guidance to be issued by the General Services Administration (GSA) when this SP is finalized. For the last two items, we understand the SP itself cannot include due process requirements or training guidance. Our suggestions here are for consideration by relevant agencies during the next stage of this process.

Suggested Improvements: Abstract and Introduction

Better explain to agencies the need to focus SCRM on high-impact systems. Page 2, lines 404-406, explains the guidance and controls in the publication are "recommended for use with high-impact systems," as characterized by Federal Information Processing Standard (FIPS) 199. However, the text goes on to say 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). We understand NIST wants to provide agencies flexibility to make appropriate decisions in circumstances when a particular system or component may require more extensive risk management controls than the overall system (and that in fact in certain cases agencies already use a mix of controls when using FIPS 199, such as by classifying a system as moderate impact, but using high controls for certain parts of that system).

Nonetheless, this section of SP 800-161 should include additional wording to guide agencies through a thoughtful and informed consideration of whether they should indeed apply these ICT SCRM controls outside of high-impact systems. Given the growing focus on ICT supply chain security (in industry, the Administration, the Congress, among other governments, the media, and the like –a focus which in some cases is not well-informed, such as provisions in legislation that equate country of origin with security),[4] agencies may feel pressure to look like they are "doing something" related to ICT supply chain security. Thus, they may feel compelled to apply these SCRM controls broadly throughout their IT procurements, whether truly warranted or not. We understand federal departments and agencies need to work to protect

[4] A case in point is Section 515 of the January 2014 Omnibus Appropriations bill (P.L. 113-76), which imposes risk assessment requirements on the Commerce, Justice, and Science agencies' IT procurements, with a specific (and unnecessary) reference to goods and services connected to China.

the entire enterprise from malware, counterfeit products, unauthorized access, IP theft, and poor manufacturing and development practices in the ICT supply chain. But, as NIST is aware, there are inherent risks in all IT systems (just as there is inherent risk in all aspects of business overall) and prioritization of security resources among these systems—including SCRM activities—is essential.[5] The goal should be to focus government and private-sector cybersecurity resources, which are not infinite, where they offer the most benefit for mitigating risk by lowering vulnerabilities, deterring threats, and minimizing the consequences of incidents.

Thus, this section of SP 800-161 should add a sentence or two highlighting the potential costs of applying SCRM controls to IT systems at lower impact levels or to specific system components. NIST could easily pull from the other portions of the document (pp. 9 and 14) where it stresses the costs that can accompany SCRM controls generally. SP 800-161 acknowledges that each organization has a different mission and risk environment, and we suggest NIST should amend this section with something like the bold text below to stress the need to look at missions and risk environments:

> *The guidance and controls in this publication are recommended for use with high-impact systems according to Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. However, 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.* ***Agencies should carefully consider the potential costs of applying SCRM controls beyond high-impact IT systems because, as described on pages 9 and 14 of this publication, implementing these controls will require financial and human resources, not just from the agencies directly but also potentially from their systems integrators, suppliers, and external service providers, that would also result in increased costs to the acquirer. SCRM controls are a form of risk management, and should be considered in the context of the agency's or organization's mission and risk environments. Agencies should carefully consider if the IT system or component in question truly rises to the level of risk deemed necessary to apply these additional risk management tools.***

Expand narrative promoting a "dialogue" between acquirers and ICT suppliers. Pages 8-9 suggest 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).

This section needs explicit and prominent clarification and additional elaboration on the extent to which conversations between acquirers and suppliers are critical—throughout the procurement process, including well before requests for proposals (RFPs) are issued as well as after the RFP is awarded. Ongoing discussions are essential to increase the chances of successful procurements where suppliers can meet agency needs at an appropriate cost (and where agency needs are realistic). Acquirers need to

[5] The Administration has demonstrated this understanding of prioritization in some recent policy initiatives, including in the February 2013 Executive Order (EO) on Cybersecurity in Critical Infrastructure. Section 9 of the EO creates a new category, "Critical Infrastructure at Greatest Risk," that seeks to focus on a narrow subset of CI with significant dependencies upon cyber systems.

clearly understand suppliers' capabilities, constraints, and costs related to particular SCRM controls an agency might be interested in implementing; acquirers would also benefit from the perspective of the prospective bidders on each specific supply chain risk identified by the acquirers. At the same time, suppliers need to clearly understand acquirers' needs in terms of mission, system performance goals, and other factors determining the context in which the acquirer believes it must deploy particular SCRM controls. An ongoing discussion can likely reduce any misunderstandings and also allow both agency and supplier to determine if there is a better way to achieve the desired result than may have been originally considered or proposed by the agency.

Importantly, such a dialogue must supplement—but cannot replace—a robust risk assessment process inside the acquiring agency. Agencies must develop a realistic picture of the risks they want to mitigate. If the agency has done that risk assessment seriously and thoroughly, it can then initiate and maintain a potentially much more productive dialogue with its vendors.

Specific Line-Item Suggestions

Our specific line-item suggestions are in the attached matrix. We assume NIST will receive much more detailed line-item feedback from individual companies.

Other Suggestions

Reduce the size of the SP: In general, the volume of information is still arduous and presented with an unnecessary level of complexity. NIST should seek to solve the solvable and this document is far too expansive in its attempt to treat the subject. The entire document needs to be consolidated further to help agencies understand how to apply the proposed practices. Supplemental documents, providing more details and examples, could be used instead of keeping all the content in this SP.

Use industry SCRM practices: We remain concerned the agencies' acquirers and program managers do not and will not have the necessary expertise in how suppliers manage and secure their supply chains to know which SCRM controls are and are not effective, feasible, and/or cost-prohibitive. To prevent this problem, NIST should review every SCRM control it recommends in this SP against common SCRM practices of the commercial off the shelf (COTS) technology industry. Based on this review, this SP should explicitly identify every proposed control that departs from common practice, and for every such discrepancy the SP should provide agencies with guidance on how to determine when the cost and feasibility might warrant use. Importantly, NIST should seriously consider not including in this SP those controls whose cost-and-feasibility/benefit ratios are high, or at least explicitly calling out those controls with extreme ratios.
The suggestions we made above regarding promoting an expanded dialogue between acquirers and suppliers should help facilitate the understanding by acquirers about the feasibility and benefits of specific controls.

Segregate SCRM from other controls: The SP should explicitly and prominently direct agencies' acquirers and program managers to segregate their desired SCRM controls from the other acquisition requirements in their RFPs, whether or not the controls depart from common industry practice. This would enable bidders to meet the core functional requirements of the RFP and distinguish themselves on

the basis of their ability to satisfy the additional SCRM requirements, explain why these requirements are not feasible, or explain potential cost impact.

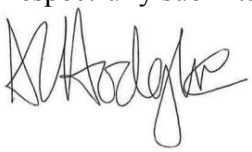
Vendor notice of denial/non-compliance and appeal: We understand that these controls, like any NIST SP controls, will not be placed directly on bidders and suppliers per se, but rather be translated by the department or agency that chooses to use them through purchase-related documents such as a "sources 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.

GSA training: We understand that once this SP is finalized, GSA will need to train contracting officers on how to use it. Given industry's extensive experience training our own employees on SCRM within our own supply chains, we believe we have unique expertise and lessons learned to contribute to GSA's efforts. As you move into the implementation stage of this SCRM work—namely the development of training materials and processes— ITAPS and ITI suggest that GSA approach the development of its training in a similarly transparent manner that welcomes stakeholder input. ITAPS and ITI companies would be pleased to contribute our knowledge and lessons learned to the government's efforts so that we can all benefit from ICT SCRM.

Conclusion

Thank you again for the opportunity to respond and share our viewpoints. We look forward to working with NIST as you continue to refine this publication. We are available at any time to elaborate on our response. Should you have any questions regarding these comments, please feel free to contact Pamela Walker, Senior Director of Homeland Security at (202) 626-5725 or pwalker@itic.org.

Respectfully submitted,



A.R. "Trey" Hodgkins, III
Senior Vice President, Public Sector

Danielle Kriz
Director, Global Cybersecurity Policy

Attachment: Comment matrix

ITAPS-ITI 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**
1.		***Abstract, page iii***			**"…or are vulnerable due to poor manufacturing and development practices within the ICT supply chain. These risks are associated with the federal agencies decreased visibility into, understanding of, and control over how the technology that they acquire is developed, integrated and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services."** We have two concerns with this section. Vulnerabilities due to "poor manufacturing and development practices" are not "supply chain risks" but are properly covered under "assurance." Further, because a plethora of assurance standards exists, it is confusing and potentially a duplication of resources to file assurance requirements under "supply chain risk." Additionally, the risk of buying a poor-quality product is a business risk--not a result of using or having a supply chain per se. It is not realistic to expect businesses to "over share" their business processes to buyers because of the expense of doing so and because those processes themselves often involve trade secrets. Further, the US Government has moved heavily to COTS by choice, and the nature of COTS is that the buyers cannot dictate or attempt to "control" exactly how products are built.	Remove the reference to suppliers' "poor manufacturing and development practices" and clarify that lack of visibility into processes might be justified. In particular, the phrase "…control over how the technology they acquire is developed…" should be stricken.	

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**
					Realistically, the customer can buy it or not buy it, and ask for "reasonable" amount of transparency into e.g. development practices.		
2.		***Introduction, page 1***			**"Similarly, the rapid adoption of open source software, most commonly in binary form, extends these risk scenarios to the libraries, frameworks, and toolkits on which so much of modern software relies."** Comment: the statement that open source is commonly incorporated in binary form is not accurate. On the contrary, many suppliers incorporate source code and compile the libraries into their code.	Phrase more accurately.	
3.		***Introduction page 1 and Footnote page 1***			**"It should be noted that, ICT products or services manufactured anywhere (domestically or abroad) may contain vulnerabilities that can present opportunities for ICT supply chain-related compromises," with Footnote 1 reference as follows:** **This document defines an ICT Supply Chain Compromise as:** **An occurrence within the ICT supply chain whereby an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits. An ICT supply chain compromise can occur anywhere within the system development life cycle of the product or service."**	This SP must distinguish correctly between 1) unintentional coding defects, 2) deliberate insertion of an exploitable defects (the latter is inherently an insolvable problem, as noted by [among others] the Defense Science Board task force report on Mission Impact of Foreign Influence on DoD Software (http://www.acq.osd.mil/dsb/reports/ADA486949.pdf), and 3) configuration weakness (sometimes also called incorrectly "vulnerability").	

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**
					Comment: This is a poor definition that conflates "vulnerability" with a supply chain *compromise*. They are entirely different. Correctly understanding the threat provides a better chance of determining the correct remedy.		
4.		**Introduction page 1**			**"…as well as poor manufacturing and development practices in the ICT supply chain."** Comment: unintentional defects that can be exploited are properly addressed under "assurance" and are not per se a supply chain risk. All quality problems are not "supply chain compromises." Also note that all software has undiscovered defects due to the extraordinary complexity of systems and huge code bases, and despite efforts to find the defects (through manual code reviews, QA, and static and dynamic analysis).	Clarify that defects are not necessarily supply chain risks/compromises, and that 100% defect-free products are not possible.	
5.		***Introduction, page 2***			"**Currently, federal agencies, and many private sector integrators and suppliers use varied and nonstandard practices, which makes it difficult to consistently measure and manage ICT supply chain risks across different organizations."**	Clarify that this sentence does not imply that standard practices among suppliers are possible or desired per se (given the heterogeneity of products and production processes, etc).	
6.		***Section 1.4 page 3***			**"Integrity is focused on ensuring that the ICT products or services in the ICT supply chain are genuine and authentic and do not contain any unwanted (and potentially dangerous) functionality, as**	Clarify who does not want the functionality or that unwanted functionality is not bad in all cases.	

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**
					well as that the ICT products and services will perform according to expectations; …" Comment: "Unwanted" is vague because it begs the question, "unwanted *by whom*?" Many COTS products are highly configurable and thus typically install multiple modules that may be separately licensed. A customer could argue they don't want things installed they didn't actually ask for or intend to pay for (which would require installation tool modification a vendor is unlikely to want to make). Furthermore, COTS may have and often does have undocumented functionality (functionality not intended to be accessed by end users but that is not malicious in design (e.g., code that is only compiled under certain circumstances that enables better testing, for example, or diagnostic ability)).		
7.					**"Resiliency is focused on ensuring that ICT supply chain will provide required ICT products and services under stress"** Comment: Resiliency of the supply chain is extremely vague in this context. The fact that "supply chain" is so broadly defined is a mistake and conflates all risks of purchasing a product or service with targeted attacks on the supply chain.	More narrowly define both "supply chain" and "resilience."	
8.		***Section 1.4.2 Page 7***			**"In addition, it may be difficult to determine whether an event was the direct result of a supply chain vulnerability."**	This document should not conflate vulnerability in a component (e.g., coding error) with a weakness in the supply chain itself, lest a considerable	

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**
					Comment: "supply chain vulnerability" is an incredibly vague term.	portion of a supplier's business operations fall under the purview of a customer's "supply chain risk management."	
9.		***Section 1.4.3 page 8***			**"However, ICT products created by suppliers are created for general purposes for a global market and typically are not tailored to any individual customer's specific requirements."** Comment: very true.	Additionally this section should state that COTS are often not designed for all threat environments, so products may not necessarily suffice in the actual environments into which they are deployed.	
10.		***Chapter Two page 15***			**"(iv) Monitor risk on an on-going basis, including changes to an information system or ICT supply chain infrastructure, using effective organizational communications and a feedback loop for continuous improvement."** Comment: This is unrealistic, since suppliers' cannot/ will not provide detailed insight into every change of their suppliers or every change to their supply chain practices. In some cases these are trade secrets and in others the overhead to do so would be considerable.	Delete "changes to an information system or ICT supply chain infrastructure"	
11.		***Section 2.2.1 page 26***			**"For ICT SCRM, threat sources include: (...) human errors"** Comment: "Human error" is not a threat – it is a risk of any activity.	Delete "human error"	
12.			***Table 2.2***		"**Disgruntled insiders sell or transfer**	Delete this as a threat agent/example.	

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**
			page26		**intellectual property to competitors or foreign intelligence agencies for a variety of reasons including monetary gain. Intellectual property includes software code, blueprints, or documentation.**" Comment: This is a supplier's, not government's, business risk.		
13.			***Table 2.2 page26***		**"Foreign intelligence services seek to penetrate ICT supply chain and implant unwanted functionality (by inserting new or modifying existing functionality) to be used when the system is operational to gather information or subvert system or mission operations."** Comment: there is no solution to the trusted insider problem (a conclusion reached by the Defense Science Board in their report on mission impact of foreign influence on DoD Software http://www.acq.osd.mil/dsb/reports/ADA486949.pdf: that is, a person with legitimate access to source code, can add "unwanted functionality" in a way that is undetectable).	Add footnote that it is impossible to address this 100%.	
14.		***Section 2.2.1 page 28***			**"A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Within the ICT SCRM context, it is any weakness in the system/component design, development, manufacturing,**	Narrow the definition.	

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**
					production, shipping and receiving, delivery, operation, and component end-of life that can be exploited by a threat agent to significantly degrade performance of a system that supports the mission." Comment: This definition is so broad that using would gravely hinder a wise allocation of resources. There is a considerable difference between an inadvertent coding error that introduces a security weakness, a design weakness (e.g., badly implemented or non-existent access control) and a configuration weakness (not changing default passwords). Furthermore, this definition can turn any "problems" into "vulnerabilities."		
15.		***Section 2.2.2 page 34***	Lines 1359-1360		**"The likelihood of exploitability is a key step to understanding impact."** Comment: NIST must be careful not to suggest that – if "vulnerability" encompasses product or component vulnerabilities-- COTS providers should provide details of exploitabilities of extant security vulnerabilities in advance of fixing them. Doing so would significantly weaken security.	Clarify that information on likelihood of exploitabilities should not be required to be divulged.	
16.		***SCRM_AC*-5 p. 57**			**"The organization should ensure that appropriate separation of duties is established for decisions requiring the acquisition of both information system and ICT supply chain infrastructure**	Delete the examples, or clarify they may not always be appropriate.	

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**
					components. Separation of duties helps to ensure that adequate protections are in place for components entering organizations supply chain." Comment: This is not always possible or desirable. For example, there may be limited suppliers of a particular component. Further, the "technical experts" may be keenly involved in procurement decisions for life cycle cost and maintenance reasons, among others. There are cases where a two-person rule may be warranted but there are many cases where it is not. Again, this is a matter of business practice.		
17.		***Family Audit and Accounta bility p. 62***			**"Organizations should ensure that they designate ICT supply chain-relevant events and audit for those events within their own system boundaries using appropriate audit mechanisms (e.g., system logs, Intrusion Detection System (IDS) logs, and firewall logs)."** Comment: typically logs are not kept for long and the media used to store them is written over periodically (e.g., just as backup tapes are cycled). Therefore, it's unlikely that audit records will exist long enough to be able to determine "what happened" unless it is within the timeframe of media cycling.	Clarify that acquirers should set realistic time bounds.	
18.		***SCRM_A U-2 AUDIT***			**"Such events should be identified as ICT supply chain auditable events and captured by appropriate audit**	Change to ask if a supplier has reasonable auditing on access to source code. Remove any suggestions	

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**
		EVENTS AU-2 p. 62			**mechanisms including: event occurrence, length and frequency of event occurrence. … An example of such an auditable event can include tracking change, frequency of change, as well as event of handing off of software source code to ensure that it is authorized, traceable, and verifiable."** Comment: This requirement regarding how to audit is inappropriate for COTS providers.	of mandates regarding how that auditing is done.	
19.		***SCRM_AU-7 . p. 64*** **(1) CROSS-ORGANIZATIONAL AUDITING I SHARING OF AUDIT INFORMATION AU-16(2)**			**"Supplemental ICT SCRM Guidance: Whether managing a distributed audit environment or an audit data sharing environment between organizations and its system integrators or external services providers, organizations should establish a set of requirements for the process of sharing audit information. In the case of the system integrator and external service provider and the organization, a service-level agreement of the type of audit data required vs. what can be provided must be agreed to in advance to ensure that the organization obtains the relevant audit information needed for ensuring that appropriate protections are in place to meet its mission operation protection needs. Ensure that coverage of both information systems and ICT supply chain infrastructure are addressed for the collection and sharing of audit information."**	Remove requirement for sharing audit information.	

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**
					Comment: Suppliers should not be required to share audit records with the US government. In addition, service providers face multi-tenancy issues that may preclude them from sharing audit logs (e.g. no other customer will agree to let audit logs that may record who accesses their hosted data be shared with another customer of the hosted service – in particular, if that customer is a government).		
20.		***SCRM_CA-6 CONTINUOUS MONITORING p. 67***			**"Supplemental ICT SCRM Guidance: Information gathered during continuous monitoring serves as inputs into ICT SCRM decisions including criticality analysis, vulnerability and threat analysis, and risk assessment. It also provides information that can be used in incident response and potentially can identify ICT supply chain compromise."** Comment: This is written too broadly and could put requirements on suppliers to continuously monitor everything pertaining to "supply chain," Including non-critical systems (e.g. order entry systems).	Clarify that continuous monitoring should be undertaken judiciously.	
21.		***FAMILY: CONFIGURATION MANAGEMENT p. 68***			**"Configuration Management helps track systems, components, and documentation throughout the ICT supply chain. This is important for knowing what changes were made to those systems, components, and documentation, who made the changes, and who authorized the changes. Basically, configuration management provides the tools to establish the chain**	Remove.	

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**
					of custody for systems, components, and documentation." Comment: Configuration management is in many cases not related to chain of custody. It is particularly not useful for documentation since in many cases documentation is not placed in source code management systems (there is no real business case for that, and "approval" may apply to code check ins but is unlikely to be applied to documentation changes). At any rate, acquirers will not get access to suppliers' configuration management systems or in many cases their practices in detail.		
22.		***SCRM_CM-6 p. 70*** **(1) CONFIGURATION SETTINGS I AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION CM-6(1)**			**"Supplemental ICT SCRM Guidance: The organization should employ automated mechanisms to centrally manage, apply, and verify configuration settings for ICT supply chain infrastructure and components."** Comment: this is not realistic. Under the SP's broad definition of "supply chain compromise," a multitude of systems could conceptually be covered as "supply chain-relevant." Further, a malicious actor would otherwise target and attempt to corrupt the configuration settings for the entirety of supply chain-relevant systems.	Delete	
23.		***SCRM_CM-10 SOFTWARE***			**"Evaluate and periodically audit the Open source ICT supply chain infrastructure as provided by the open source organization. This evaluation can**	Add text regarding the constraints in the open source arena.	

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**
		USAGE RESTRICTIONS p. 73			**be done reasonably easily by the organization through obtaining a number of existing documents as well as experience based on software update and download processes in which the organization may have participated."** Comment: In particular, any analysis of the use of open source software should look at the length of time a library is supported (meaning, the open source organization publishing the libraries will create patches for it) and the frequency of patches. A component that is unpatchable (because the open source group puts out new versions every 6 months and only supports the last 2 versions) is unlikely to work for, say, a system expected to have a useful life of 10-plus years. The integrator or acquirer will have to plan on and budget for creating their own patches to the libraries.		
24.		***SCRM_CP-2 CONTIGENCY PLAN p. 76 CONTINGENCY PLAN* | IDENTIFY CRITICAL ASSETS CP-2 (8)**			**"Supplemental ICT SCRM Guidance: Ensure that critical assets are identified to ensure that appropriate requirements are defined for contingency planning and administered to ensure continuity of operation. A key step in this process is to complete a criticality analysis on components, functions, and processes to identify all critical assets. See Chapter 2, Criticality Analysis."** Comment: In particular, the acquirer needs to regularly upgrade to new/supported versions and regularly apply critical security	Add text about upgrading.	

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**
					patches. Many vendors only fix security issues in newer versions (because not all patches can be backported) so newer versions are often more secure. Running on an out-of-date, unpatchable critical component is an avoidable and preventable risk if the acquirer plans for and budgets for regular upgrades and regular patching.		
25.		***INCIDENT RESPONSE p. 79***			**"FIPS 200 specifies the Incident Response minimum security requirement as follows: Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities."** Comment: Because "supply chain compromise" is defined so broadly, and "incident" is vague, this section should be corrected to ensure that supplier vulnerability handling is excluded from "incident."	This section should be corrected to ensure that supplier vulnerability handling is excluded from "incident." If addressed at all, product or component vulnerability disclosure by suppliers should be limited to a) ensuring the supplier has a reasonable process for logging, triaging and fixing security bugs (and notifying customers of the issue and/or patch availability) and b) SIs or acquirers analyse security fixes and apply them rapidly.	
26.		***SCRM_MA-7 MAINTENANCE MONITORING AND INFORMATION SHARING***			**"Control: The organization monitors the status of systems and components and communicates out of bounds and out of spec performance to [Assignment: organization-defined system integrators, suppliers, or external service providers]."** Comment: This section should apply to	Clarify that this applies to actual parts' failure rate.	

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**
		p. 83			actual parts' failure rate, but it is vague. It should not apply to keeping track of reported vulnerabilities in products (which is not a meaningful statistic).		
27.		***FAMILY: PERSONNEL SECURITY p. 91***			**"Personnel that have access to federal agency ICT supply chain should be covered by federal agency personnel security controls. These personnel include acquisition and contracting professionals, program managers, supply chain and logistics professionals, shipping and receiving staff, information technology professionals, quality professionals, mission and business owners, system owners, and information security engineers. Organizations should also work with system integrators and external service providers to ensure that they apply appropriate personnel security controls to their personnel that interact with the federal agency ICT supply chain, as appropriate."** Comment: this is not workable. Inherent in the decision to use a third party is that the personnel of that third party will not be subject to the same personnel policies as the customer's. That is particularly the case when the third-party is a global COTS provider.	Delete	
28.		***SCRM_PS-3 THIRD-PARTY PERSONNEL SECURIT***			**"Supplemental ICT SCRM Guidance: Third-party personnel, as soon as they are engaged, become part of the ICT supply chain infrastructure and as such, must meet the same personnel security requirements as those participating in**	Delete	

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**
		Y p. 92			**supply chain as organizational personnel. Examples of such third-party personnel can include the system integrator, supplier or external service provider personnel used for delivery, or supplier maintenance personnel brought in to address component technical issues that were not solvable by the organization or system integrator."** Comment: same comment as above.		
29.		***SCRM_PV -2 p. 94***		Possible typo	**"Ensures that the provenance information and the provenance change records including to whom, when, and what, is non-reputable."** Comment: This is confusing. Should this read "non-refutable" (someone cannot deny he or she did X to change a configuration, for example)? Or "non-reputable" (there is no attribution at all, e.g. action X cannot be reputed to be by person Y)?	Clarify	
30.		***SCRM_SA -1 p. 97***			**"Organizations should make sure that their system and services acquisition policy addresses ICT SCRM including changes of location, ownership, and control, and requirements to be communicated to the ICT supply chain."** Comment: the word "location" is vague and the security-relevance of location-related information is debatable at best.	Delete "location."	
31.		***SCRM_SA -4***			"**Define requirements for an established system integrator, supplier, external**	Change to ask "what" a supplier does in this area (change from telling the	

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**
		ACQUISITION PROCESS p. 98			**service provider vulnerability response process and their capability to collect inputs on vulnerabilities from acquirers and other organizations"** Comment: The government should not be defining this. Suppliers – especially large COTS providers – typically already have processes for a) looking for security vulnerabilities b) remediating them – typically on a fixed schedule and c) the amount of information they disclose. They should not give the US government earlier, more frequent, or more information than they provide any other customer. "Inputs from acquirers" is similarly vague. Any reasonably-sized vendor has customer support mechanisms by which customers can log bugs.	supplier what to do).	
32.		***SCRM_SA-4 ACQUISITION PROCESS p. 98*** j.			**"Monitor system integrators, suppliers, and external service providers' information systems where applicable. Monitor and evaluate the acquired work processes and work products where applicable"** Comment: The US government should not expect to monitor a COTS vendor's internal networks and systems (and "where applicable" will not effectively limit the overreach of this ask).	Delete reference to monitoring information systems.	
33.		***SCRM_SA-9 DEVELOPER SECURIT***			**"Supplemental ICT SCRM Guidance: Depending on the origins of components, this control may be implemented differently. For OTS (off-the-shelf) components, the acquirer**	It should be clarified that this is proof of testing, not test results, and that testing need not happen for all cases.	

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**
		***Y TESTING AND EVALUATION SA-11* p. 100**			**should request proof that the supplier (OEM) has performed such testing as part of their quality/security processes."** Comment: It should be clarified that this is proof of testing, not test results, and that testing need not happen for all cases. Testing for counterfeits is expensive, impractical, and essentially impossible, as it must be done for each and every single instance. Suggesting that it should be common practice is not realistic. In addition, it is unclear what is means to test the origin of a component, and what benefit that will provide.		
34.		***SCRM_SA-12 (2) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / THREATMODELING / VULNERABILITY ANALYSIS SA-15 (4) 4315 p. 104***			**"Supplemental ICT SCRM Guidance: This enhancement provides threat modeling/vulnerability analysis for the information system. This provides further detail and clarity to shape the ICT supply chain activities that need to be implemented for those critical components. This analysis provides useful inputs into the ICT SCRM threat and vulnerability analysis described in Chapter 2."** Comment: This is not feasible for large bodies of code that have been around for some time. A piece of COTS software that has millions of lines of code and hundreds of modules is not going to have "threat analysis" for every feature ever developed. Nor is it feasible in all development projects to do threat modelling for every "new feature."	Clarify that discretion should be made as to if/when this is applicable.	

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**
35.		***SCRM_SA-16 COMPONENT AUTHENTICITY SA-19 p. 106***			**"Supplemental ICT SCRM Guidance: Organizations can use tamper-resistance techniques to reduce counterfeit and tampering software and hardware in the ICT supply chain. Examples of tamper-resistance techniques include retarring of chips to avoid rebranding of discarded chips, or digital signatures to help non-repudiation of software."** Comment: Digital signatures for software will not work unless the acquirer wants to create (and pay for) signature on modified code. It is unclear how patch applications or upgrades are handled with regard to digital signatures. Digital signatures are useful in only one case of software authenticity assurance: ensuring that what someone downloads is what was supposed to be downloaded.	Remove digital signatures/software reference.	
36.		***SCRM_SC-12 CONCEALMENT AND MISDIRECTION p. 110***			**"Supplemental ICT SCRM Guidance… concealment and misdirection techniques include…"** This section/control is not actionable or relevant to acquisition. COTS suppliers change their origin of development quite frequently. These practices are not an attempt at concealment or misdirection but rather just normal business practices.	Delete.	
37.		***SCRM_SC-12 CONCEALMENT AND MISDIREC***			**"Supplemental ICT SCRM Guidance: Supply chain processes are necessarily structured with predictable, measurable, and repeatable processes for the purpose of efficiency and cost reduction. This opens up the opportunity for**	Delete reference to randomness.	

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**
		TION / CONCEALMENT AND MISDIRECTION - RANDOMNESS p. 110			**potential breach. In order to protect against compromise, employ techniques to introduce randomness into organizational operations and assets into the organization's information systems or ICT supply chain infrastructure (e.g. randomly switching among several delivery organizations or routes, or changing the time and date of receiving supplier software updates if previously predictably scheduled)."** Comment: This SP acknowledges the difficulty of consistency in defending against supply chain threats. To do so in an effective and cost-effective fashion (given that their resources are constrained), suppliers seek to run well-honed supply chain practices with "locked down" security for those repeatable processes. It is puzzling to expect suppliers to use scarce resources to deploy random processes that they are nonetheless asked to secure.		
38.		***Glossary Page A-4***			Definition of **ICT Supply Chain Risk** Comment: This is an unacceptably broad definition. It conflates any and all risk of buying from a third party with "supply chain risk."	Change definition.	
39.		***Glossary page A-6***			Definition of Provenance Comment: The notion of reporting "all changes" to "actors" is unreasonable because it assumes a level of information sharing that will not become general	Change definition.	

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

ITAPS-ITI 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**
					business practice. .		
40.							
41.							
42.							
43.							
44.							
45.							

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