Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change	
Andy Purdy	ed.	p. i	14	Note to reviewers	It would be helpful if the release of v. 1.0 of the Framework in February 2014 is accompanied by a clear message to companies who perform key functions as part of the Critical Infrastructure, specifically to Company Boards of Directors and C-level officers, that it is requested that they do several things to ensure their organization is appropriately addressing cybersecurity risk to improve the security and resilience of the critical infrastructure; more specifically: Be sure that you have an enterprise risk program that includes cyber/information risk, and that the program is owned by a committee of the Board of Directors. Huawei has found that it is essential to provide the Board of Directors with visibility and responsibility for end-to-end cyber security is essential to an effective program. At Huawei, the Vice Chairman of the Board chairs the Global Cyber Security Committee that includes not only company-wide cybersecurity leadership, but also senior officials of the company including the business	Include strengthened message to Boards of Directors and C-level Officers.	

					units themselves. This helps to ensure that cyber security is imbedded into the organizational design, with governance of the risk management strategy and the internal control framework being the starting point for the design, development, and delivery of good cyber security. The message to boards of directors should include the following: that they conduct an enterprise risk assessment, at least focused on cyber/information risk. Then, considering the spirit and substance of the NIST Framework: 1) Determine which categories of the Framework are applicable to their organization, and if any are not applicable, determine why not. 2) For each category determine which standard(s) or best practice(s) does, or will, their organization choose to follow. 3) Determine the current state of the organization's risk posture relative to the framework, and the target state that the organization should strive for, and develop and begin to implement a plan with resources to achieve that target state. 4) Determine the metrics and milestones that will be tracked and reported to the C-level along the path to the target state, and the metrics that will be tracked		

					and reported to the C-level regarding the organization's risk posture going forward. 5) Determine whether the organization has an internal compliance program that adequately takes into account the cyber issues covered by the Framework. 6) Recommend that such organizations consider getting independent, input -- at least from outside the business unit(s) being evaluated -- regarding each of these determinations at the start of this process – for the same reasons that there are independent financial audits – and, going forward, get independent, input (at least from outside the business units if not externally) periodically or on an ongoing basis, regarding the risk posture, in general, and progress toward the target state and the risk status going forward, in particular.		

Andy Purdy	ed.	p. 9	332-385	2.4	Although the idea of having tiers that represent progressions along a path an organization follows toward a target state is appealing, the description of the tiers – specifically the distinctions between the tiers -- are not sufficiently substantial or clear enough to be applied consistently and with meaningful effect (for example, the distinction between tier 1 and tier 2). If the tiers mapped as needed, one should be able to provide a graphic illustration of how the categories and subcategories map to the tiers. I don't think that is possible at present.	Request comment regarding the rationale for the use of tiers, and whether and how to develop tiers.	

Andy Purdy	ed.	p. 37	549-566	App. C2 Conformity Assessment	I hope NIST will encourage key stakeholders to launch an effort(s) to stand up a conformity assessment program for ICT products, perhaps beginning at the sector level. Huawei has found in the evaluations we have done of our products – and the evaluations others have done of our products – that it is essential to provide vendors with objective information about their products to provide feedback to their internal development and manufacturing process, as well as to provide those who buy ICT products with objective information about the security/assurance status of the products. Mechanisms to help make buyers more informed will enable them to be more discriminating about what they buy. It is demonstrable that very insecure products are being deployed unnecessarily into the nation's	Suggest adding a call to action to the private sector to lead on engaging about conformity assessment to inform Framework version 2.0.	

					networks (as well as globally). The process of independent evaluation -- both internally (separation of duties) and externally by independent third parties , has helped us, and will no doubt help others, raise the bar on the products that we/they offer and release to customers and will raise the bar on the purchasing/using side for RFPs and the ability of customers to make much more informed decisions about what to purchase and ask/require of vendors. The value of a Consumer Reports or Underwriters Laboratory kind of a model for ICT products will be an important contributor to making our nation's (and global) networks and systems more secure. Huawei recently published a security white paper that goes into some detail about Huawei's global assurance program.		

					Huawei invites constructive feedback about our approach and suggestions about how to facilitate greater global collaboration hopefully leading to the use of common standards, best practices, and norms of conduct to help reduce global ICT risk while raising the security/assurance characteristics of ICT products and services. The paper can be found at the following link: http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-310548.htm. Information about product evaluation can be found in the paper at p. 24 (Section 7.6 Verification: Assume nothing, believe no one, check everything). It would be helpful if NIST could consider convening or encouraging others in government and in the private sector, perhaps at the sector level (e.g., IT SCCs (and ISACs)), to consider		

					convening a work stream(s) leading to some ideas, options, and perhaps straw men for a conformity assessment program. At the sectoral level, companies should find that they have a common interest in the quality/assurance characteristics of what they buy, and that together they could come up with a set of baseline requirements that they would all like their products to have, and encourage vendors/suppliers to test their products/services to those standards.		

Andy Purdy	ed.	p. 39	633-645	c. 8 - Supply Chain Risk Management	As indicated in NIST SP 800-161, several GAO reports, and the White House Cyberspace Policy Review (2009), supply chain risk is an important part of the risk landscape that an organization needs to include in its risk management program. Accordingly, for the NIST Cybersecurity Framework to contribute to achieving the purpose of the Executive Order on Cybersecurity, to promote the security and resilience of the critical infrastructure, supply chain risk must be addressed. Those who purchase ICT products and services -- whether government, critical infrastructure, or other private organizations -- should include supply chain risk requirements in their procurement and purchasing decisions. Huawei has provided a detailed overview of its approach to global	Suggest adding a call to action to the private sector to lead on engaging about supply chain risk to inform Framework version 2.0.	

					assurance -- including supply chain/procurement risk -- in it security white paper referenced earlier (http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-310548.htm). Information about supply chain and procurment assurance efforts can be found at pages 27-31 (7.7 Third-party supplier management - subsections on supply chain and procurement security). We hope that supply chain will be addressed and incorporated into the Cybersecurity Framework in Version 1.0 or, more likely, in Version 2.0 that will hopefully be released later in 2014. We hope that the Open Group Trusted Technology Forum Supply Chain Standard and Accreditation Process will be explicitly referenced in the Framework when supply chain risk is addressed		

					more comprehensively.		