From: **Birgit Smeltzer - QT3JB** <birgit.smeltzer@gsa.gov>
Date: Tue, Apr 11, 2017 at 8:31 AM
Subject: GSA/FAS/ITC/IT Security Subcategory Comments to NIST Framework
To: cyberframework@nist.gov
Cc: Shon Lyublanovits - QTGBA <shondrea.lyublanovits@gsa.gov>, Terence Rountree - QTGBAC <terence.rountree@gsa.gov>

Good Morning,

Please see the comments for the Cybersecurity Framework.

Regards,

Birgit Smeltzer | Phone: 202.412.7801
Program Manager | IT Security Category Managment Operations/Office of IT Security Services
Office of Information Technology Category (ITC)
Federal Acquisition Service (FAS)
U.S. General Services Administration (GSA)

ACQUISITION GATEWAY

[Attachment Below]

Organization: GSA/FAS
Name: Office of Information Technology Category (ITC) IT Security Subcategory
Document Name: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

Comment Number	Comment Type (C, S or A)	Page #	Line #	Document Paragraph #	Comment	Rationale
1	A	Cover			Update the date when issued (here and the header).	For consistency
2	A	1	63		Regarding “critical infrastructure” - What is considered critical infrastructure? Suggest defining this term and maybe have a few examples. Would ISPs / Telco (communication) providers for the Federal government be considered critical infrastructure?	For better readability/understanding
3	A	1	64		Consider listing the 16 critical infrastructure sectors identified in PPD-21 Critical Infrastructure Security and Resilience, either here, or as a footnote, or with the “Critical Infrastructure” definition in the Glossary.	For better readability/understanding
4	A	3	121		Suggest this document reference PPD 21 Critical Infrastructure Security and Resilience as it appears to work hand in hand with EO 13636.	For better readability/understanding
5	A	3	121		Suggest adding the year “2013” to the date of February 12 for completeness.	For completeness
6	A	5	200		Suggest to include this text to show a benefit of the Core: “The Framework Core enables communication of cyber risk across an organization.” Source: Framework for Improving Critical Infrastructure Cybersecurity – NIST, January 2016.	For better readability/understanding
7	A	5	207		Suggest to specify text to show each Tier builds on the previous: “…with each Tier building on the previous Tier.” Source: Framework for Improving Critical Infrastructure Cybersecurity – NIST, January 2016.	For better readability/understanding
8	A	5	217		Suggest to specify text to show a benefit of the Profile is to assist prioritize and measure, as the opportunities for improving cybersecurity postpose are identified: “The Profile supports prioritization and measurement while factoring in business needs.” Source: Framework for Improving Critical Infrastructure Cybersecurity – NIST, January 2016.	For better readability/understanding
9	A	6	251		Suggest to provide document hyperlink to Section 4 as was done for the other sections in the Document Overview	For consistency
10	A	6	256		Suggest to provide document hyperlink to Appendix D as was done for the other sections in the Document Overview	For consistency
11	A	7	273		Suggest creating a table where the four elements are placed on top in a heading format.	For ease of readability/understanding

12	A	9	356		Suggest different word choice, such as "provide" instead of "inform."	For better readability/understanding
13	A	10	358		Suggest adding a table/graphic of Tiers and descriptions.	For better readability/understanding
14	A	14	502		This paragraph goes on to give examples of outcomes design, build/buy, and deploy lifecycle phases, but not operate and commission. Suggest adding those examples as well.	For better readability/understanding
15	A	15	547		Regarding "sources" suggest to specify the types of sources	For better readability/understanding
16	S	16	602		"Manager" should be "Manage"	Incorrect word used
17	A	17	609		Delete the extra period at the end of the sentence in the quote.	Extra period was used
18	A	17	626		The sentence starts with "Suppliers encompass" - Suggest using singular - "Supplier refers to..." and be consistent as in the previous sentence for ease of readability.	For better readability/understanding and consistency
19	A	18	637		Suggest referencing Table 2, Framework Core, and adding a hyperlink.	For ease of readability/understanding
20	A	18	642		Not quite sure what the "(Section 3.3)" reference is meaning - clarify - as was discussed in Section 3.3 of this document?	For clarity
21	A	20	737		For the last bullet, suggest referencing Section 3.2, Establishing or Improving a Cybersecurity Program.	For ease of readability/understanding
22	A	21	745		Regarding "measuring state" Suggest updating "state" to "cybersecurity state."	For better readability/understanding
23	A	22	804		Suggest changing to: "enabling cybersecurity to be factored into enterprise risk management."	For better readability/understanding
24	A	23	814		Consider adding an Operational measurement to Table 1.	For better readability/understanding
25	A	23	814		Suggest adding Policy to the Table 1 list. Policy is the driving force behind Practices and Processes.	For better readability/understanding
26	S	24	854		SP-28 should be SC-28	Incorrect reference/NIST SP 800-53 security control
27	A	27		ID.AM-5	Suggest rename to Hardware/Software Resources to differentiate from human/personnel resources	For better readability/understanding
28	A	31		ID.SC-5	Under "Subcategory" Suggest to include SCRM consideration text: "…including SCRM incident response." Organizations should integrate ICT SCRM considerations into incident response policy and procedures.	For better readability/understanding
29	A	31		ID.SC-5	Under "Informative Resources" Suggest to add IR-1 (Incident Response Policy and Procedures).	For better readability/understanding
30	A	33		PR.AC-6	Under "Subcategory" validate "asserted" is the correct word choice versus "inserted."	For better readability/understanding
31	A	35		PR.DS-6	Under "Subcategory" Suggest to add text to also reference SCRM: "…including ICT SCRM considerations." (SI-7)	For better readability/understanding

Organization: GSA/FAS
Name: Office of Information Technology Category (ITC) IT Security Subcategory
Document Name: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

32	A	35		PR.DS-8	Under “Subcategory” Suggest to add text to also reference SCRM: “…including ICT SCRM considerations.” (SI-7)	For better readability/understanding
33	A	35		PR.IP-1	Under “Subcategory” Suggest “privilege” versus “functionality”	For better readability/understanding
34	A	37		PR.IP-9	Under “Subcategory” Suggest to include SCRM consideration text: “…including SCRM incident response.” Organizations should integrate ICT SCRM considerations into incident response policy and procedures.	For better readability/understanding
35	A	37		PR.IP-9	Under “Informative Resources” Suggest to add IR-1 (Incident Response Policy and Procedures).	For better readability/understanding
36	A	38		PR.PT-3	Under “Subcategory” Suggest “privilege” versus “functionality”	For better readability/understanding
37	A	48		Appendix B – Leading Measurement	Correct typo “achieve” to “achieved”	Correct typo
38	A	48		Appendix B – Non-IT/OT Partner	Suggest changing “providers” to singular: “Product or service provider that does not ….”	For better readability/understanding
39	A	48		Appendix B – Risk	Because this Framework document now includes SCRM, suggest to also include the NIST SP800-161 Appendix F Glossary definition of ICT Supply Chain Risk in this Glossary: ICT Supply Chain Risk - Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.	For better readability/understanding
40	A	49		Appendix B – Supplier	Suggest changing “providers” to singular.	For better readability/understanding
41	A	49		Appendix B	Suggest to include the NIST SP800-161 Appendix F Glossary definition of ICT SCRM in this Glossary: ICT Supply Chain Risk Management - The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains.	For better readability/understanding
42	A	51		Appendix D – Second change listed	Typo found – it states Table of Contents was modified to reflect “the all” – change to “all the”	Correct typo