August 10, 2015

Comment Template for NISTIR 8074 Volume 1, Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (Draft)

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1	The Open Group	Editorial	P1; 6	I believe this if the first instance of using NSC therefore should spell it out.	Include the full name first and then (NSC)
2	The Open Group	Major	P6; 258	The Open Group develops international standards – they are international standards in and of themselves, but several of their standards have also been approved and adopted by ISO (e.g. the Open Trusted Technology Provider Standard – Mitigating the Risk of Maliciously Tainted and Counterfeit Products (O-TTPS) was recently approved as ISO/IEC 20243 and is relevant to cybersecurity).	Please include the "The Open Group;" on this line. NOTE: Additional changes related to this request are in the Volume 2 comment sheet from The Open Group.
3	The Open Group	Major	P6; 264	It is important to acknowledge the innovative and dynamic nature of standards and to recognize the value SDOs and their communities bring to the evolution of standards.	Please consider adding a paragraph that says: Given the importance of SDOs and considering the number of relevant standards being developed by SDOs, it is important that in addition to recognizing NIST and ISO we also recognize the work of some of these other SDOs. The standards produced by SDOs actually represent a point in time snapshot with today's standards often representing yesterday's innovations. But they cannot remain static, they need to evolve and they need these active supporting communities of SDOs to revise them in a way that meets the challenges of the ever-changing threat landscape. Given that the dynamic nature of standards it is important not to be locked into policy that enforces the use of a static set of procedures or standards.
3	The Open Group	Major	P6; 273	There is another level that is not covered by your 3 listed categories of: Standards Mostly Available, Standards Being Developed, and New Standards Needed. The suggested new category is: "Some Standards Available". Not having this additional category provides an inaccurate picture of the landscape for the case where some standards do exist. Cyber challenges are complex and may require multiple standards to address a particular cybersecurity application. Additionally, one standard may not work for all cases and alternatives are needed. To provide a more accurate picture it is important to recognize existing work even though it may need to be evolved or where additional standards may also be needed.	Please add another category and sentence: "Some Standards Available" Some Standards Available indicates that some standards exist and have standards-based implementations, but there may be a need for additional standards and/or revisions to existing standards in this area.
4	The Open Group	Major	P7-8; Table 1	It is difficult to map all standards to these vertical applications – as some cybersecurity standards apply horizontally to ICT technology, which all IT applications use and depend on, including those applications listed in this table. The O-TTPS is one of those standards. And it specifically covers these areas: Network Security, Software Assurance, Supply Chain and Risk Management, System Security Engineering, and IT System Security Evaluations.	If you have agreed to add the category that was requested earlier per #3 (i.e. "Some Standards Available"), then please for the following rows: Network Security, Software Assurance, Supply Chain and Risk Management, System Security Engineering, and IT System Security Evaluations, change all areas in these rows that currently say "New Standards Needed" or "Standards Being Developed" to "Some Standards Available".

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
					If you have not agreed to add that category then please at least change "New Standards Needed" to "Standards being Developed" – in the mentioned rows, especially in the Supply Chain and Risk Management row.
5	The Open Group	Major	P7-8; Table 1	In Table 1, for the rows: IT System Security Evaluation, Network Security Software Assurance, Supply Chain Risk Management, Information Security Management Systems, Security Automation and Continuous Monitoring, and System Security Engineering, please include The Open Group to the column entitled: Examples of SDOs – as The Open Group has "Available Standards" in these areas (E.G. O-TTPS (ISO 20243) for IT System Security Evaluation, Network Security, Software Assurance, Supply Chain Risk Management and System Security Engineering; O-ISM3 for Information Security Management Systems, O-AECML for Security Automation and Continuous Monitoring)	Under the column entitled: "Examples of Relevant SDOs," please add "The Open Group" to each of these rows: IT System Security Evaluation, Network Security Software Assurance, Supply Chain Risk Management, and System Security Engineering, Information Security Management Systems, Security Automation and Continuous Monitoring.
6	The Open Group	Major	P6; 284	This categorization of standards into vertical application is a bit concerning - particularly when there are process standards for IT development and manufacturing that are horizontal and applicable to the development of all ICT, the same ICT that is used in all of these applications. Because this general horizontal concept is integral to mitigating the cybersecurity risks associated with the IT that most applications depend on and because a similar concept applies to the software applications as well – it is important to note that not all standards need to or should be specific to a vertical application – there are many requirements/standards that apply across the board from a cybersecurity hygiene perspective.	Please consider adding a note in the text: "Please note that while this table is structured by application there are some cybersecurity standards that apply across the applications to the development and manufacturing of ICT products (hardware and software), products that most if not all of these applications depend on.
7	The Open Group	Major	P12; 510	It would be helpful if federal agencies not only supported and coordinated the development of conformity to standards, but also showed preference for those organizations that conform to standards through conformance assurance programs.	Please consider adding a phrase to this bullet. The third bullet currently reads: "…accelerate the development and use of technically sound standards and standards-based products, processes and services (e.g., the Federal Risk and Authorization Management Program (FedRAMP))" Please add the following phrase to the end of the sentence: "and where appropriate show preference in procurement for those suppliers who demonstrate conformance to standards."