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

Submitted by: **Eric C. Cosman (OIT Concepts LLC)**

Date: **September 22, 2015**

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1		Minor	P1, L8	*"…strategic objectives for pursuing the development and use of international standards…"* The objective is not entirely clear. Is pursuit the objective, or should it in fact be the establishment of these standards?	Clarify intent
2		Minor	P1, L17	Work not only with *"federal agencies*" but also specific SDO's and other relevant groups in the private sector.	
3		Minor	P2, L47	How is *"cost efficient"* measured? Is it the total cost (incurred by all parties), and if so, how can this be determined? Or is it cost to government?	Clarify
4		Minor	P2, L76	In addition to the goals mentioned it is also critical to ensure **consistency** across related standards that may overlap in scope to a degree that is short of total duplication. Asset owners should not get inconsistent direction on requirements and expectations.	Emphasize the need for consistency.
5		Minor	P3, L101	YES! Continue to emphasize that it is performance and outcome that is the basis for assessment of standards, and not the processes used for their development or the specific directions given.	
6		Minor	P3, L116	Are there requirements from specific organizations (e.g., ANSI) that can be referenced in this paragraph?	
7		Minor	P4, L195	*"…IT consortia developing standards…"*; It is also very important to be clear about where such standards are and are not suitable. For example, some of these standards may not be appropriate for industrial control systems in the critical infrastructure.	
8		Minor	P5, L205	Is it possible for government to identify areas where they may be a potential for competition between SDO's, without appearing to show preference?	
9		Major	P5, L220-222	Maintaining the commitment to a specific standards development effort is **critical**. For many SDO's the exclusive reliance on volunteer resources make it almost impossible to reliably plan efforts and predict availability of final standards. Any sort of consistent commitment would greatly help with this problem.	Add emphasis to this point.
10		Minor	P6, L242	Consider adding "system integrity and safe operation"	
11		Major	P7, Table	In the Industrial Control Systems column they are already several standards that have been published and are available. For example, of the thirteen elements of the ISA/IEC 62443 series at least six have been	Reconsider the characterizations in this column.

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

Submitted by: **Eric C. Cosman (OIT Concepts LLC)**

Date: **September 22, 2015**

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
				approved and published, with an additional four available as almost complete drafts. Several of those published are also under revision.	
12		Minor	P9, L328	In the case of ISA (individual membership) it is a requirement that committee membership be balanced between various constituencies, such as end user, vendors, etc.	Change "is not built in" to "may not be built in"
13		Minor	P9, L335	What are the criteria that would be used to determine which of these levels of engagement are appropriate for a given situation?	
14		Major	P10, L380	The current level of continuity of participation from USG is quite low, and seems to depend largely on budgets and the timing within the fiscal year. We have seen several examples where government funded contributions terminate suddenly and without warning.	
15		Minor	P10, L399	Recommend referencing the Department of Labor Cybersecurity Industry Model, which defines competencies for IT and OT cybersecurity professionals and as such would be a good resource to include in the participation/training/education resources. It may also be worth mentioning in the same reference that the Department of Labor Automation Competency Model and the Engineering Competency Models also contain cybersecurity competencies.	Include reference to Department of Labor Cybersecurity Industry Competency Model.
16		Minor	P11, L456	*"… coordinate on major issues…"* Exactly what does this mean? Is this coordination of <u>government</u> activity only?	
17		Major	P12, L473	As stated above, consistent commitment is critical.	
18		Minor	P12, L484	Given the large number of standards that are identified as being required, it might be worth prioritizing these and/or specifying deadlines.	Consider identifying deadlines or priorities for the standards to be developed.
19					
20					