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	CDC, Office of the Chief Information Officer	Editorial/Major	General	Many international standards are not free like NIST standards. Many smaller IT vendors, as well as Government agencies, do not have resources allocated for the significant cost of "proprietary" standards. For example, three of the five standards relevant to the USG promoted SWID standard for software asset management are priced as follows in the ANSI web store (licenses for a single user of these documents): ISO/IEC 19770-1:2012 Software asset management Part 1 $240.00 ISO/IEC 19770-2:2009 Software asset management Part 2 $265.00 ISO/IEC 19770-5:2015 IT asset management $149.00 Site licensing costs are not addressed. Similar licensing might be needed for all standards publishers. This cost will have a significant impact on the ability of producers and consumers to access and implement these standards. There are nearly 200 information security FIPS and SP standards documents on the NIST website, plus a number of NISTIRs. There appear to be hundreds or thousands of IT standards on the ISO website. The cumulative cost of international standards from all standards bodies could be significant. Likewise, paid organizational memberships may be required by some of these standards bodies for individuals or organizations to participate at various levels in the standards development/vetting process, which may exclude valuable input such as from non-profit privacy advocates who have contributed significantly to the development of NIST standards.	Provide recommendations to address managing the cost associated with using international standards. Potential options include: • Only using standards bodies which do not charge anyone for copies of their standards. • Approving a limited number of non-free standards bodies to manage the number of sources for which site licenses must be obtained. • Proving a mechanism for a US Government-wide site license to be obtained and perpetually renewed for all relevant standards bodies. • Addressing competitive disadvantages created for small businesses which would be burdened by the cost of obtaining all relevant security standards.

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)

August 10, 2015

Comment Template for NISTIR 8074 Volume 2, Supplemental Information for the 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	CDC, Information Technology Services Office	Clarification; better definition	9; 369; Table 2	“Reference Implementation” states only “is available”. The other maturity models provide specific facts of the model within the right hand column.	What is a reference implementation or what is it not? Is it less than an Approved Standard which is available to the public? Our guess is it’s implemented but yet has reached a maturity level of acceptance.