September 24, 2015

Department of Commerce
National Institute of Standards and Technology
100 Bureau Drive, Stop 1070
Gaithersburg, MD 20899

Submitted via electronic mail to nistir8074@nist.gov

Re: DRAFT Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (NISTIR 8074 Volumes I and II)

To whom it may concern:

Microsoft appreciates the opportunity to review and comment on the National Institute of Standards and Technology (NIST) Draft Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (NISTIR 8074 Volumes 1 and 2). As NISTIR 8074 Volume 1 highlights, the U.S. government's engagement in the development of international cybersecurity standards is critical to achieving long-term economic security and public safety. In addition, over time, investments in support of the development of international cybersecurity standards will drive economic growth, as advancing security increases the reliability of and trust in the global digital economy.

As a global technology company, Microsoft invests heavily in the development and adoption of cybersecurity standards and best practices.[1] In addition to developing and sharing widely the Security Development Lifecycle (SDL),[2] our software development security assurance process, and Operational Security Assurance (OSA),[3] which improves operational security across our cloud services, Microsoft is an industry leader in obtaining certifications and voluntarily conforming to standards that demonstrate our commitment to meeting the security needs of public and private organizations. For instance, numerous Microsoft services have achieved ISO 27001 and 27002 certifications,[4] and Microsoft was the first major cloud service provider to adopt ISO 27018, the world's first international standard for cloud privacy.[5] In addition, Microsoft has helped to adapt SDL into an international standard, ISO 27034-1,[6] and has helped to drive within the Trusted Computing Group the development of the Trusted Platform Module (TPM) 2.0 standard, which was adopted as ISO 11889 this year.[7]

While Microsoft and many of our customers invest significantly in security development, trustworthy platforms, and other best practices, technologies and practices continue to evolve, creating a need for stakeholders to

[1] This includes global consortia as well as international standards development organizations.

[2] Security Development Lifecycle, Microsoft, http://www.microsoft.com/en-us/sdl/.

[3] Operational Security for Online Services Overview, Microsoft, https://www.microsoft.com/en-us/download/confirmation.aspx?id=40872.

[4] ISO 27001/27002: 2013, Microsoft Azure, http://azure.microsoft.com/en-us/support/trust-center/compliance/iso27001/; Security, Audits, and Certifications, Microsoft Office 365 and Dynamics CRM Online, https://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Security_Audit.htm.

[5] *Microsoft adopts first international cloud privacy standard*, Microsoft on the Issues (Feb. 16, 2015), http://blogs.microsoft.com/on-the-issues/2015/02/16/microsoft-adopts-first-international-cloud-privacy-standard/.

[6] *Microsoft SDL Conforms to ISO/IEC 27034-1: 2011*, Microsoft Cyber Trust Blog (May 14, 2013), http://blogs.microsoft.com/cybertrust/2013/05/14/microsoft-sdl-conforms-to-isoiec-27034-12011/.

[7] Governments recognize the importance of TPM 2.0 through ISO adoption, Microsoft Cyber Trust Blog (June 29, 2015), http://blogs.microsoft.com/cybertrust/2015/06/29/governments-recognize-the-importance-of-tpm-2-0-through-iso-adoption/.

continue to collaborate in identifying and standardizing best practices in security. Having a robust and current set of cybersecurity standards enables all stakeholders, including both providers and users of technologies and services, to access and demonstrate meaningful conformance with security baselines across the global, interdependent cyber ecosystem.

NIST is already recognized for its technical competence and as an information and communications technology (ICT) standards setter globally; for instance, many governments' cloud computing strategies reference NIST's definitions for cloud computing as well as for cloud service and deployment models.[8] However, to have a meaningful impact in the deliberate and time-intensive process of standards development, especially in the constantly expanding cybersecurity space, NIST must be supported by long-term resourcing and dedicated technical engagement from stakeholders across the U.S. government. Ultimately, with the support of a well-resourced and synchronized U.S. government, NIST can effectively improve the coordinated development of international cybersecurity standards, enabling it to work not only towards the four strategic objectives outlined in NISTIR 8074 Volume 1 but also towards increasing the reliability of and trust in the global digital economy.

Microsoft is committed to working collectively with the U.S. government as well as with other government and industry partners to support the development of international cybersecurity standards. We offer the below overarching comments as well as more detailed comments in the attached Appendices A and B with the aim of opening an ongoing dialogue with NIST and other U.S. government stakeholders, both on NIST's draft report and on the U.S. government's broader plans to engage in standards development.

1) **The U.S. government should *prioritize* international cybersecurity standards development to raise the baseline of cybersecurity globally and to increase trust, transparency, and predictability for ICT providers and users, including governments.**

   We recognize that advancing cybersecurity is a vast undertaking and that many important cybersecurity initiatives and programs compete for U.S. government resources, including both expertise and funding. Indeed, even well-developed and regularly updated international cybersecurity standards do not represent an end unto themselves but instead are one element of many across numerous and varying strategies, all of which are necessary to advance cybersecurity. However, the U.S. government must recognize the long-term strategic importance of engaging in international cybersecurity standards development as a foundational investment that has far-reaching positive effects. In particular, we call for U.S. government executives to demonstrate their recognition of the strategic importance of engaging more intensely in international cybersecurity standards development than the U.S. government has engaged in recent years.

   As a user of ICT, the U.S. government will benefit, both directly and indirectly, from NIST's and broader U.S. government efforts to improve international cybersecurity standards. Directly, as highlighted by the NISTIR 8074 Volume 1 objectives, the U.S. government will be able to leverage for its own systems and software the technically sound cybersecurity standards that will be developed and updated. Indirectly,

[8] E.g., Australian Government Cloud Computing Policy, Department of Finance (2014), http://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf; Unleashing the Potential of Cloud Computing in Europe, European Commission (2012), http://ec.europa.eu/digital-agenda/en/european-cloud-initiative; Government of India's GI Cloud (Meghraj) Strategic Direction Paper, Department of Electronics and Information Technology (2013), http://deity.gov.in/content/gi-cloud-initiative-meghraj; Cloud Computing Strategy, Ireland Department of Public Expenditure and Reform (2012), ; Cloud Security Policy for Government Agencies, Qatar National Information Assurance (2014), http://www.ictqatar.qa/en/documents/document/cloud-security-policy-government-agencies; U.K. Government Cloud Strategy (2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf.

the U.S. government will also benefit from a more secure ecosystem with which it regularly interacts via systems and software managed by other governments and by industry. More specifically, if the networks in other countries and in private industry with which the U.S. government connects are more secure, then the U.S. government's own networks will also be more secure.

In addition, the U.S. government will, as detailed in the NISTIR 8074 Volume 1 objectives, facilitate international trade and promote innovation and competitiveness. International standards not only help providers to respond to the security needs of their users but also help to preserve the global nature of the Internet. Relatedly, in supporting a system of international cybersecurity standards and assessment schemes, the U.S. government will also help to create more trust, transparency, and predictability in the cyber ecosystem.[9] ICT users will have more confidence in using trusted standards to evaluate ICT providers, and ICT providers will have a clearer sense of what security measures are most important to their ICT users, including governments. The net result will be a global digital economy that continues to grow and empower users to do more.

Given such potential impacts that committed U.S. government engagement in international cybersecurity standards development could have, the U.S. government should make clear that such standards development is a priority, not only via direction provided by executive leadership as described above but also via appropriate attention to coordination and resourcing as described below.

2) **U.S. government engagement in international cybersecurity standards should be centrally *coordinated*, in accordance with its prioritized status, at the executive leadership and interagency levels.**

Because developing international cybersecurity standards in a prioritized way will require many U.S. government organizations to be synchronized, such development efforts must be centrally coordinated. As suggested by NISTIR 8074 Volume 1 Recommendation 1, Microsoft supports the institution of an Executive Office of the President (EOP) interagency policymaking body that would provide the proper level of authority to oversee such a coordination process. Additionally, this body would be tasked with periodic evaluation and reporting of the value derived from standards engagement efforts. Microsoft recommends that the existing Office of Science and Technology Policy (OSTP) perform this function.[10] The OSTP is already engaged in work with the researcher and developer communities, meaning that it could build from its existing functions and deepen its engagements with those communities. More specifically, researcher and developer communities are leading many efforts to form new technologies and processes, and through its engagement in these communities, OSTP can help to identify the potential need for and evaluate the impact of cybersecurity standards.

As also suggested by NISTIR 8074 Volume 1 Recommendation 1, in addition to creating or recognizing an EOP-level interagency policymaking body, a subordinate interagency working group should be established. An interagency working group would represent a forum in which Federal cybersecurity officials could regularly discuss and coordinate their approaches on important standards development issues. Microsoft supports the Department of Commerce's hosting of such a working group.

[9] This does not negate the value of security standards produced by industry consortia that may have more technology-specific implications.

[10] 42 USC 6613 (b)(4) and 42 USC 6614 describe OSTP's authority 1) to coordinate the research and development of science and technology programs for the Federal government; and 2) to serve as a source of analysis of federal policies, plans, and programs relating to science and technology.

However, we also urge NIST, the EOP-level interagency policymaking body, and the Commerce working group to work towards formalizing the EOP body's and working group's roles in facilitating the execution of many of NISTIR 8074 Volume 1's other recommendations. For instance, as highlighted by Recommendation 2, Federal agencies should support a long-term commitment to and value and reward staff participation in international cybersecurity standards development activities; ensuring such support and valuation should be the responsibility of OSTP or the EOP interagency policymaking body. EOP-level support for such a commitment is necessary because of the lengthy process of international standards setting; the commitment must be resilient to changes in administration as well as to shorter-term funding priorities. Likewise, as highlighted by Recommendation 3, Federal agencies should support and coordinate timely contributions to standards and assessment schemes; regularly reviewing Federal agency engagements to ensure that they are having the most significant, timely, and complementary impact should also be coordinated by and ultimately be the responsibility of OSTP or the EOP interagency policymaking body. In addition, as highlighted by Recommendation 4, continued collaboration between the U.S. government and the private sector will support the creation of prioritized, consensus-based, and technically sound international cybersecurity standards; ensuring such collaboration should be the responsibility of the Commerce working group, which should regularly interface with a FACA-exempt private sector committee.

3) U.S. government engagement in international cybersecurity standards should be sufficiently *resourced* in accordance with its prioritized status, and Federal agency funding should be tied to the developing and leveraging of international cybersecurity standards.

As highlighted in the above sections, the U.S. government's commitment to the development of international cybersecurity standards must be reflected as a priority across the U.S. government, with Federal agencies conveying to their cybersecurity officials the importance of and supporting long-term engagement in standards development organizations (SDOs). To be effective, such engagement will be resource-intensive. The development of international cybersecurity standards often takes years and necessarily involves globally distributed meetings and workshops where subject matter experts may collaborate, debate, and otherwise work to establish the required consensus. Moreover, not only technical leadership and participation but also diplomatic support and collaboration may be required as standards work their way through the consensus process. Ultimately, consistent in-person participation will be required to build trust with other working group stakeholders and to influence decisions. Moreover, as highlighted within NISTIR 8074 Volume 1 Recommendation 6, seeking leadership roles in SDOs will help the U.S. government to encourage and support the development of an efficient and balanced standards environment. To effectively lead a cybersecurity standard working group, Federal cybersecurity officials will require expanded standards training and an assurance of consistent budgetary support to properly fulfill obligations.

To ensure that Federal agencies have sufficient long-term funding to support their training and intensive engagement in SDOs over a period of many years, the Office of Management and Budget (OMB) has an important role to play. OMB must not only ensure that sufficient funding is allocated to OSTP and to Federal agencies so that their staff can support and pursue international cybersecurity standards development but also tie the developing and leveraging of international cybersecurity standards to Federal agency funding. Consistent with and driving implementation of NISTIR 8074 Volume 1 Recommendation 8, such an approach by OMB will both reinforce executive leadership's prioritizing of international cybersecurity standards development and strengthen Federal agency coordination. More specifically, the tying of funding to the coordinated developing and leveraging of international cybersecurity standards will solidify the importance of utilizing international SDO forums and standards development processes rather than engaging in one-off standards development efforts between Federal agencies and nationally-focused organizations.

4) **The U.S. government should *execute* on the development of international cybersecurity standards in coordination with the private sector, in collaboration with other governments, and in a prioritized manner.**

If the U.S. government's engagement in international cybersecurity standards development is prioritized, coordinated, and resourced, then Federal agencies will be empowered to execute on the U.S. government's strategy and will reap the benefit of global leadership in this space. However, to effectively execute on such standards development, the U.S. government must have regular mechanisms for coordinating with the private sector, collaborating with other governments, and prioritizing standards efforts.

Coordinating with the private sector will inform the U.S. government's international cybersecurity standards engagement efforts and help it to be agile. Many organizations within the private sector are already heavily engaged in international cybersecurity standards development and can provide OSTP, a Commerce working group, and Federal agencies feedback on which standards areas demonstrate greatest need for U.S. government engagement. In addition, because the ICT ecosystem is particularly dynamic, the U.S. government must be responsive and self-evaluative, continuously assessing whether it is engaging in the most appropriate SDOs on the most appropriate standards areas and achieving its desired impact. Regular private sector coordination can also help the U.S. government to stay informed on how technologies and the ICT ecosystem are constantly evolving and on how such evolution is having an impact on international cybersecurity standards gaps. As highlighted above, from Microsoft's perspective, the best forum for ongoing U.S. government and private sector engagement is regular coordination between a Commerce working group and a FACA-exempt private sector committee.

In addition to coordinating with the private sector, we encourage a synchronized U.S. government to collaborate with other governments as Federal agencies work towards developing and leveraging international cybersecurity standards. Around the world, many governments are facing cybersecurity challenges that are similar to those facing the U.S. government, and bringing like-minded governments together outside of an SDO process, at which there may be governments, industry, and other multi-stakeholder participants engaged, can help the U.S. government to gain traction and momentum towards its cybersecurity standards goals. Moreover, considering the significant resource investment required to participate effectively in this broad space of international cybersecurity standards, collaborating with other governments may help the U.S. government to extend its impact beyond those standards groups in which Federal agency officials are deeply engaged.

Thirdly, to execute effectively on international cybersecurity standards development, the U.S. government must prioritize among those standards areas in which it could engage. In the NISTIR 8074 Volumes 1 and 2, NIST deeply evaluated this prioritization, considering numerous core areas of cybersecurity standardization and key IT applications. However, from Microsoft's perspective, the key IT applications listed in Table 1 in NISTIR 8074 Volumes 1 and 2 should be narrowed, allowing the U.S. government to focus on priority areas. Specifically, cloud computing and health IT should be considered priorities, as much of the learnings achieved from those applications will be transferable to and impact the other applications listed. NIST should also note that not all cybersecurity standards must result in a certification scheme; the vast majority of international standards rely upon self-attestation and voluntary compliance, which have proven to be effective compliments to auditable standards.

Moreover, as noted above, as the ICT ecosystem rapidly changes, ongoing coordination with the private sector will help the U.S. government continue to prioritize the many cybersecurity standards areas in and attestation mechanisms toward which it could drive engagement and support.

We thank you for the opportunity to comment on NIST's Draft Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity. The U.S. government must make influencing the development of international cybersecurity standards a priority, committing to sustained coordination and funding and driving SDOs toward filling important cybersecurity standards gaps in coordination with the private sector. While driving consensus around international cybersecurity standards will require significant and ongoing financial investments, at least over the next five to ten years, the payout will ultimately be a trusted, interoperable global ICT ecosystem.

We look forward to our continued partnership with NIST as well as with other government and industry stakeholders as the development of international cybersecurity standards is effectively prioritized, coordinated, resourced, and executed by the U.S. government.

Sincerely,

J. Paul Nicholas
Senior Director, Global Security Strategy and Diplomacy
Trustworthy Computing, Microsoft Corporation

Jason Matusow
General Manager, International Standards
Microsoft

Attachments:
Appendix A: Microsoft Comment Matrix – nistir_8074_vol1_draft
Appendix B: Microsoft Comment Matrix – nistir_8074_vol2_draft

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	Vol. 1	Editorial	1; 33	Since the document is about engagement in international standardization for cybersecurity, NIST might consider aligning the definitions of key words with existing standards (e.g., ISO, ITU).	**ISO/IEC 27032** defines cybersecurity as follows: “Preservation of confidentiality, integrity and availability of information in the Cyberspace” with also NOTE1 “In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved”. **ITU-T** defines cybersecurity as follows: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.
2	Vol. 1	Editorial	2; 76	The phrase, “…avoid duplication…” should be reconsidered. There are many examples of standards that are considered duplicative (e.g. .gif, .jpg, .tiff image formats) that do not create any technology or marketplace problems. Success for standardization is not automatic harmonization. Rather, there is a more significant concern with standards that “conflict” with each other (in other words, one implementation will prevent another from functioning). A simple word change can address this concern.	…avoid conflicting standards…
3	Vol. 1	Major	3; 105	One goal should be to create trust in other countries’ networks so that we can have secure communications with them.	Possible addition of a #5: U.S. Government trusted communications with other governments. A secure means for data transfer for law enforcement exchanges, military partnerships and cooperation, customs document transfers, etc.
4	Vol. 1	Major	4; 150	The majority of cybersecurity standards do not have an assessment scheme nor a recognized certification process. Voluntary implementation and self-attestation are far more common and have proven to be a highly effective means for driving quality implementations. An important subset of standards does have conformity assessment schemes and certification processes, such as ISO/IEC 27001/2 that are widely accepted as a means of assurance. Please be cognizant of the fact that this document will be broadly read and interpreted by governments in other countries. It would not be helpful to the production or implementation of cybersecurity standards if it is perceived that this paper is advocating for more conformity assessment, testing, and certification.	We encourage NIST to be thoughtful about the manner of describing conformity assessment.

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)**
5	Vol. 1	Minor	5; 201	Speed of standardization is not always the most important factor. Having a cybersecurity standard be accurate and globally accepted may require a more process-heavy SDO. International standards for cybersecurity need to be trustworthy to a broader community of implementers, be they private or public sector.	This is a contextual comment for NIST's consideration.
6	Vol. 1	Minor	6; 263	Being able to influence cybersecurity standards development requires more than just liaisons, it requires active engagement as well.	This is a contextual comment for NIST's consideration.
7	Vol. 1	Editorial	9; 323	IEC is currently excluded from this paragraph.	NIST may consider including the IEC in this section.
8	Vol. 1	Minor	10; 371	It is worth noting that other countries are making sustained efforts to fund national participants in leadership positions which will ultimately put US industry at a disadvantage and/or limit the influence of the USG. It is in all of US industry's interest to have competent USG representatives in leadership roles.	This is a contextual comment for NIST's consideration.
9	Vol. 1	Major	12; 465	While the document makes clear that the private sector plays an important role in standardization, making it explicit how the US government will continue to coordinate with the private sector is important.	NIST may consider adding an explicit statement that coordination will happen not only at an inter-agency level but also with relevant private sector experts.
10	Vol. 1	Major	12; 468	Short-term priorities will always win-out over long-term investments and will continually threaten US engagement in SDOs.	Recommendation 2 is missing the idea of educating senior leadership of agencies regarding the value of standards work and the need for long-term consistency of investment.
11	Vol. 1	Major	13; 522	People in decision-making positions need to understand the role of standards in terms of national competitiveness, industrial policy, market dynamics, etc.	Leadership training should be included in this.
12	Vol. 1	Editorial	13; 540	While standards must continue to evolve with the ecosystem, it is important to recognize the quality standards that have already been developed to minimize privacy risks.	Recommendation 7 should include language that recognizes the existence of many foundational standards such as ISO/IEC 29100 or ISO/IEC 27018.
13	Vol. 1	Editorial	13; 540	Setting the bar as to "*minimize privacy risk*" might become controversial since what is understood as sufficiently minimal is always seen differently by different countries, let alone between private sectors and government in the same country.	Since this document is about engaging with international standards, we recommend replacing "minimize privacy risk" with "respect the privacy principles of international standards" as described in **ISO/IEC 29100**.

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	Vol. 2	Editorial	2; 91	"…interoperability among trade partners…" is missing the fact that they need interop for law enforcement and military purposes as well (i.e. NATO). Security standards are not just about trade with preferred partners.	"…interoperability among trade, law enforcement and military partners…" Possibly leave out military if it alters the meaning of the end of the sentence in terms of the global economy.
2	Vol. 2	Major	3; 122	We made a similar point in comment #4 for Volume 1. Conformity assessment and testing are not the norm when it comes to information technology standardization, be it for cybersecurity or general interoperability. Voluntary implementation and self-attestation are far more common than conformity assessment, testing or audited certification. In some cases, such in crypto, there is an excellent case for it conformity assessment just as there is an excellent case for audited certification when it comes to information systems security management practices. There should be a discussion in the paper of the fact that conformance testing raises costs for both vendors and consumers but may be worth it in some cases. In other cases, the norm of self-attestation and implications of truth-in-advertising is strong enough to achieve the desired result. Again, please be considerate of the fact that this paper will be broadly read and interpreted by many other governments. If this paper is perceived to be advocating for more conformity assessment, testing and audited certification, the results could be negative both for private industry, but in creating a disharmonized conformity assessment and testing landscape that could lead to marketplace confusion and ultimately less effective security.	We encourage NIST to be thoughtful about the manner of describing conformity assessment.
3	Vol. 2	Editorial	4; 167	These are other important core areas in cybersecurity standardization.	NIST may consider augmenting this list with the following: • Information sharing/exchange • Physical and environment security, • Operational security (although this is partially covered under "IT System Security Evaluation", and "security automation and continuous monitoring"). • Securing data at rest (i.e. storage security)
4	Vol. 2	Editorial	4; 178	"It allows…" This paragraph currently suggests that standards are the sole means for information sharing. There are additional methods and it would be worth being careful to express that fact.	"It suggests that standards are one method of many that enable jurisdictions…"

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
5	Vol. 2	Minor	4; 212	The Core area of "Security Automation and Continuous Monitoring (SACM)" is important for describing various aspects of how to support "Cyber Incident Management, ISMS, and Network security." It may be useful to discuss how it ties back to enabling these items.	This is a contextual comment for NIST's consideration.
6	Vol. 2	Editorial	5; 232	"…ensuring software is free from vulnerabilities…" is a significant overstatement of what a standard can do. A standard can provide methodologies and guidance that can assist in developing better software, but it will not "ensure" that it is secure. Poor implementation, bad testing, malicious intent, etc. are all factors that negate the assertion that security can be "ensured" by a standard.	"…for significantly decreasing the likelihood of software having vulnerabilities…"
7	Vol. 2	Editorial	5; 256	NIST may wish to consider if the concept of IoT/Cyber Physical Systems fit into this section or should it be included in a different section.	This is a contextual comment for NIST's consideration.
8	Vol. 2	Editorial	7; 331	The description of "New Standards Needed" states that "…many needed cybersecurity standards are at the beginning stages of development within various SDOs and therefore standards-based implementations are not yet available"—which is similar to the description of "Standards Being Developed," which states "SDO approved cybersecurity standards are still under development and that needed standards-based implementations are not yet available." Hence it is not clear that New Standards Needed is different from Standards Being Developed.	It may be useful to establish greater clarity between "Standards Being Developed" and "New Standards Needed" descriptions.
9	Vol. 2	Major	10; 378	Cloud computing discussion is currently framed that on premise IT is inherently more secure than cloud. "…[cloud] does not inherently provide for the same level of security, privacy and compliance…that were achieved in the traditional IT model…"	We encourage NIST to take a more balanced approach to the discussion of on premise vs. multi-tenant cloud relative to security. There are economies of scale that enable cloud providers to do much deeper security/privacy/compliance work than most small/medium orgs can do for themselves. Maintaining systems with up-to-date patches for example is something that is frequently overlooked in smaller organizations and the shift to a cloud solution enables them to have significantly improved security. We recognize that this is a topic of debate but would like to see a more balanced representation of the issues in this section.
10	Vol. 2	Major	10; 396	We realize that the list on this page is not comprehensive but think that it should highlight important standards and not mischaracterize the Cloud Security Assessment and Audit.	The activity on Cloud Security Assessment and Audit is only an Annex on a Technical Report (not a standard) and as such should not be included in this list of current cloud standards development. Additionally, we suggest that NIST include 27036-4, which deals with Supply Chain Security-Cloud Services and may be of value to this discussion.

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
					We also note that within this paragraph there is no reference made to either 27018 or 27017, both of which are completed and would be valuable additions.
11	Vol. 2	Minor	10; 408	Noting the use of the term "cloud brokers" which is in the NIST Cloud Reference Architecture, but if following the International Standard on Cloud Reference Architecture (ISO/IEC 17789) this term is not a high level role.	This is a contextual comment for NIST's consideration.
12	Vol. 2	Editorial	11; 439	This paragraph says that cloud standards are fostering the rapid growth of a cloud marketplace. This is an overstatement, particularly if referring to international standards. The rapid growth of cloud as a market is based upon industry innovation and solutions that customers find compelling (competitive differentiation of offerings). The relative compatibility is not a function of standards, though it may be that new standards could help with incompatibles. That said, NIST should not be advocating for a lack of market competition. Integration and interop are always a source of creative tension as innovation and competitive differentiation are a function of market dynamics. Current standards have limited impact on the pace of innovation, rather they are a reasonable brake on the pace of change due to the needs of interop, manageability, secure processes, etc. Moreover, something like SLA is not a standard first. Rather vendors and customers have extensive SLAs even though there is no existing international (or even national) standard for this topic. Customer agreements exist with no standards but are there because customers need those terms in order to be able to make a purchase decision. Security is just as much a function of market demand as it is a requirement of regulation and/or a standard.	This is a contextual comment for NIST's consideration.
13	Vol. 2	Editorial	14; 565	Some additional relevant standards that should be noted should be added.	ISO/IEC 29147 Information technology – Security techniques – Vulnerability disclosure ISO/IEC 30111 Information technology – Security techniques – Vulnerability handling process
14	Vol. 2	Editorial	14; 579-81	It should be noted what SDO is working on this activity.	These are both being worked in OASIS.

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
15	Vol. 2	Editorial	15; 622	This needs to be updated with the most current information.	27017 is currently in ballot for final approval (FDIS) and should be done by Oct 2015.
16	Vol. 2	Editorial	18; diagram	Some important SDOs are missing.	Missing: ISO TC 292 ITU-T SG 20 DMTF Open Group
17	Vol. 2	Editorial	24; 908-9 and 916	Very few standards start as a white page project in a committee just based on a topic choice. Some company, academic or institution makes a substantial contribution of a core set of ideas. Then the committee works to refine and drive consensus. This is important because it shows the need of healthy communities of experts and a willingness to make contributions to that community.	Add missing concept – information technology standards work is almost entirely contribution-based.
18	Vol. 2	Minor	25; 949	Contribution is an important step to highlight.	The graphic should have an insertion of “Contribution” in a box immediately below “Requirements”
19	Vol. 2	Editorial	26; 980-82	The reality of the small participation in most consortia of non-US participants means that their specs may have trouble being accepted in non-US countries. A lack of international participation is a limiting factor for most consortia. Thus the balance of the Big I players which may be slower, but ultimately more trusted and/or politically acceptable.	Add missing concept.
20	Vol. 2	Editorial	27; 1037	ISO Case Study Comments: The first paragraph should point out the advantages of the process-heavy approach that is slower rather than assume a negative only view. ISO Specs are harder to produce and the process protects the minority voice (think small countries). Because of this trust by government in ISO standards, those standards can have a positive harmonization effect on policies and regulatory rule making that is in all industry (not just the US) general interests. This is like legislation, you don’t want fast-moving legislation that ignored the minority voice and potentially is enacted without considering the consequences of the law.	This is a contextual comment for NIST’s consideration.
21	Vol. 2	Editorial	27; 1049	Factual error, “ISO Technical Committees may also…”	“Member national standards bodies may also…”

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
22	Vol. 2	Editorial	28; 1070	Text addition to the sentence.	"…such as speed, consensus, expense, and quality…"
23	Vol. 2	Minor	29; 1104	Difficulty examples are both focused on testing.	Possible alternate examples might be technical expertise of SMEs in terms of lack of knowledge limiting the capability to engage in a given project.
24	Vol. 2	Editorial	29; 1104	Even though this sentence already include the word "technical", it would be useful to also point out that the maturity of a technology area also can raise the difficulty of creating a standard.	This is a contextual comment for NIST's consideration.
25	Vol. 2	Minor	29; 1107	Product competition where different vendors are both pushing for standards, but different standards, is different from a vendor resisting commoditization. Also there is a reality of geopolitical challenges in terms of voting choices and/or collaboration work within committees. (i.e. Germany's recent concerns about the TPM 2.0 specification)	This is a contextual comment for NIST's consideration.
26	Vol. 2	Editorial	31; 1201	It is also commonly accepted that "open standards" enable participation and a clear process for work so as not to discriminate.	"The common definition of an open standard is that it is open to all participants, it has clearly defined processes and its specification is publically available."
27	Vol. 2	Editorial	32; 1243	Section on How to Effectively Engage in SDOs could use some additional concepts: - Contribution drafting - Review of contributions from others - Overall strategy for the SDO needs to be aligned with individual standards activities It may also be useful to give a sense of scale for what engagement will look like. SC27 has 260+ projects, 2x meetings per year, interim engagements prep on hundreds of contributions per meeting, interim drafting/commenting and outreach to other participants…	This is a contextual comment for NIST's consideration.
28	Vol. 2	Minor	32; 1274	It is also in the best interest of US industry for the USG to take leadership roles. But leadership roles come at a higher cost. Those individuals must act more neutrally and thus you may need to also have SME available to drive technical agenda. Is it worth mentioning that other countries are taking on as many leadership roles as possible and thus there is a long-term implication of the US losing its influence in key SDOs?	This is a contextual comment for NIST's consideration.

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)
29	Vol. 2	Editorial	39; 1490-92	Conformity assessment and testing are not the norm when it comes to information technology standardization, be it for cybersecurity or general interoperability. Voluntary implementation and self-attestation are far more common than conformity assessment, testing or audited certification.	Suggest adding point that conformity assessment is done on a minority of standards overall.
30	Vol. 2	Major	51; 1989	It is not clear what the differences are with cloud computing that would require changes to existing ISMS or risk management frameworks. This might be better to be listed as information security management systems with an understanding of how applied to a cloud services. The focus here seems to be on what the cloud customer needs to understand when deciding to move to cloud services. There may not be a need to re-invent standards for cloud, but a better clarification on how to use those standards in a cloud environment. Additionally, the concept of trust boundary is not clear and it is not clear how this is different from defining a methodology that allows for clear identification and delineation of security and privacy responsibilities.	This is a contextual comment for NIST's consideration.
31	Vol. 2	Editorial	51; 1996	It needs to be clear that this is a methodology and not a checklist. It needs to be kept in mind that different types of cloud services (IaaS, PaaS, SaaS, etc) will have different delineations.	Suggest mentioning that responsibilities will differ according to cloud service model.
32	Vol. 2	Editorial	52; 2048	This needs to be updated with the most current information.	Update with current level that standards are at (i.e.27017 is now beyond DIS). Additionally, the SC 27 investigations have moved forward and also include Use cases for cloud security and potential standardization gaps.
33	Vol. 2	Editorial	55; 2139	This bullet should have more standards-relevant information.	There should possibly be a note to ISO/IEC 28000 family on standards that relates to Supply Chain Security.
34	Vol. 2	Editorial	60; 2333	Add for completeness	Additionally ISO TC 215 which included ISO 27799 (ISMS for Health)
35	Vol. 2	Editorial	63; 2395	Add for completeness	Work happening in ISO/IEC JTC 1 on 27019 (ISMS for Smart Grid)
36	Vol. 2	Editorial	Annex E	Add for clarity	Either inclusion of another column that identifies the Core Areas of Cybersecurity Standardization or change cyber security scope to align with Core areas of Cybersecurity standardization for clarity.