ADVANCING GLOBAL COMMUNICATIONS

TELECOMMUNICATIONS
INDUSTRY ASSOCIATION

1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org

Tel: +1.703.907.7700
Fax: +1.703.907.7727

Submitted via email (nistir8074@nist.gov)

September 24, 2015

Willie May
Under Secretary of Commerce for Standards
and Technology and Director
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Director May:

The Telecommunications Industry Association (TIA), representing global manufacturers, vendors, and suppliers of information and communications technology (ICT), writes to express its input to the National Institutte of Standards and Technology (NIST) on its draft *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*.[1] TIA supported the Cybersecurity Enhancement Act of 2014,[2] and commends NIST in working transparently to meet Section 502's requirement that the Director of NIST work with relevant Federal agencies to ensure interagency coordination "in the development of international technical standards related to information system security," and to develop and transmit to Congress a plan for ensuring such coordination.

TIA represents approximately 300 ICT manufacturer, vendor, and supplier companies in government affairs and standards development. Numerous TIA members are companies producing ICT products and systems, creating information security-related technologies, and providing ICT services information systems, or components of information systems. These products and services innovatively serve many of the the public sector and are impacted by NIST's draft strategy. Representing our membership's commitments in this area, we also hold membership and are actively engaged in key public-private efforts that contribute to secure information systems, including the Communications Sector and Information Technology Coordinating Councils and the Federal Communications Commission's

[1] http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-8074

[2] P.L. 113-274.

Communications Security, Reliability and Interoperability Council (CSRIC), among other successful public-private partnerships.

TIA and our member companies are committed to enhancing the national security in both the public and private sectors, and generally urges that governments and regulators be guided by the following principles:

- The global nature of the ICT industry necessarily requires a global, consensus-driven standards-based approach to address cybersecurity concerns;
- Successful efforts to improve cybersecurity will leverage public-private partnerships to effectively collaborate on addressing current and emerging threats;
- The U.S. government should enable and stimulate greater cyber threat information sharing between the public and private sector;
- Policymakers and regulators should ensure that they address economic barriers for owners and operators of critical infrastructure in efforts to secure cyberspace; and
- A global supply chain can only be secured through an industry-driven voluntary adoption of best practices and global standards.

TIA believes that international standards, and organizations that develop international standards, should serve as a cornerstone in cybersecurity and cybersecurity conformity assessments. As the Draft Strategy demonstrates, standard developers and related organizations are already active in developing cybersecurity standards and related conformity assessments, and these organizations should continue to play a key role. While the majority of ICT security standards are predicated on voluntary implementation and self-attestation, TIA members specifically are heavily invested in several of the international standards cybersecurity conformity assessment regimes that the Draft Strategy includes, such as SAFEcode, the Trusted Technology Forum, and the Common Criteria, among others. Others are still being developed, such as the security assurance methodology for mobile networks now addressed by 3GPP Systems Aspects (SA) 3. These form part of the landscape of global standards and best practices that will continue to evolve in the future. We applaud NIST’s comprehensive Draft Strategy in this respect, and believe that it will help ensure that U.S. Government actions impacting international cybersecurity standards will neither stifle innovation nor constrain such industry-driven evolution.[3] We also continue to endorse the broader landscape of international security standards development that will

[3] Unfortunately, there are other parts of the globe where “foreign” input is disregarded, and the standardization system is effectively used as a way to give preference to parties physically located within a country. We believe that NIST is in alignment with other standardization stakeholders that such policies stifle innovation and investment.

rely on voluntary implementation and self-attestation as an essential complement to those that require conformity assessment.

Further, TIA believes that it is crucial that NIST and other USG representatives interact with and participate in the development of voluntary, consensus-based standards, and encourages such engagement as soon as possible, as widely as possible. We have long encouraged the participation of Federal agencies in industry technical standards development processes (including TIA's), and greatly appreciate the value of the public-private partnership that exists in the United States with regards to standards.

TIA member company technologies' continued success in the global marketplace has been enabled through the development of internationally-used standards and best practices. We support NIST's Draft Strategy's proposed approach which recognizes that that the global nature of the ICT industry necessarily requires a global approach to address cybersecurity concerns. TIA agrees that, in accordance with the WTO TBT committee decision, international standards are developed by a variety of standards setting organizations, not only by national-member based organizations.

Finally, we also commend NIST in addressing the need to ensure that cybersecurity standards are fully appreciated and understood within the U.S. Government workforce. The Draft Strategy reflects the importance of education, and that adequate workforce training across the Federal government will be required. TIA strongly supports NIST carrying this concept forward into the final version of its strategy and its related Congressional report.

Based on the views noted above, we append to this letter requested line edits to the Draft Strategy. Thank you for your continuing hard work on this important national and economic security issue, and TIA remains committed to working with NIST and other Federal entities to enhance the cybersecurity of the United States through international standardization and other means.

Sincerely,

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	TIA	Major	Page 2; Line # 67-#81	TIA urges NIST to address reasonable availability of the underlying specifications as a necessity to implement the standard as a factor for selection of standards. This would be consistent with the Administration's views on reasonable access to standards used in Federal regulations (*e.g.*, Office of the Federal Register's 2014 clarified views on reasonable availability of standards – see https://www.federalregister.gov/articles/2014/11/07/2014-26445/incorporation-by-reference).	Add in the following bolded text on line # 73: "…developing technically sound and fit for purpose **reasonably available** standards, in open…"
2	TIA	Major	Page 4; Line # 159-164	While the majority of ICT security standards are predicated on voluntary implementation and self-attestation, TIA members specifically are heavily invested in several of the international standards cybersecurity conformity assessment regimes that the Draft Strategy includes, such as SAFEcode, the Trusted Technology Forum, and the Common Criteria, among others. Others are still being developed, such as the security assurance methodology for mobile networks now addressed by 3GPP Systems Aspects (SA) 3. These form part of the landscape of global standards and best practices that will continue to evolve in the future. We applaud NIST's comprehensive Draft Strategy in this respect, and believe that it will help ensure that U.S. Government actions impacting international cybersecurity standards will neither stifle innovation nor constrain such industry-driven evolution. However, it is important that NIST recognize in its Strategy that the broader landscape of international security standards development that largely relies on voluntary implementation and self-attestation as an essential complement to those that require conformity assessment.	Add in the following bolded text, and delete the following struck-through text, on line # 159: "**While the broader landscape of international security standards development largely relies on voluntary implementation and self-attestation as an essential complement to those that require conformity assessment,** ~~T~~testing and attestation of products, processes, and services"
3	TIA	Major	Page 9; Line # 327-330	TIA agrees with NIST that treaty-based International agreements should have a mechanism for private sector advice and input given that on occasion the USG is blocked from expressing a view based on disagreements by affected industries. It is important that the USG fully understand the industry viewpoints on an issue that it may engage on within a standardization body, even if there is not unanimity amongst the industry.	Add the following bolded text on line # 329: "…from enhanced focus **through transparent and open consultations and mechanisms with the private sector** by the…"
4	TIA	Major	Page 10; Line # 385-392	TIA strongly encourages the USG to convene, participate, and advise international cybersecurity standardization efforts, but does not necessarily believe that the USG should "lead" these standardization efforts.	Delete the following struck-through text on line # 391: "In addition to effective participation ~~and leadership~~ by Federal agency…"

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	TIA	Major	Page 11; Line # 452-458	TIA strongly urges Federal interagency bodies determining policy decisions and areas of significant disagreement to utilize a mechanism for private sector advice and input given that on occasion the USG is blocked from expressing a view based on disagreements by affected industries. It is important that the USG fully understand the industry viewpoints on an issue that it may engage on within a standardization body, even if there is not unanimity amongst the industry.	Add the following bolded text on line # 457: "arise **through transparent and open consultations and mechanisms with the private sector**."
6	TIA	Major	Page 13; Line # 551-564	TIA believes that it is very important for NIST to specifically raise the need for Federal agencies to be mindful of their NTTAA and OMB Circular A-119 obligations, including the requirement to leverage voluntary consensus standards where available.	At the end of the sentence on line # 555, add the following new sentence: "Agencies should ensure adherence to requirements in the NTTAA and OMB Circular A-119, particularly the requirement to leverage voluntary consensus standards where available."