Comments of the
Information Technology Industry Council

Regarding the NIST Draft Report

"Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity"

NISTIR 8074 Volume 1 (Draft)

The Information Technology Industry Council, ITI, welcomes the opportunity to provide comments regarding the draft "Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity" [NISTIR 8074 Volume 1 (Draft), hereafter "Report"]. ITI applauds the sustained interest of the National Institute on Standards and Technology (NIST) and its staff in cybersecurity standards issues, and their appreciation of industry perspectives. We support the recommendations outlined in the Report.

ITI is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry. ITI's members comprise the world's leading innovation companies, with headquarters worldwide. Cybersecurity is rightly a priority for governments and our industry, and we share a common goal of improving cybersecurity.

As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. Further, our members are global companies doing business in countries around the world. Most service the global market via complex supply chains in which products are developed, made, and assembled in multiple countries across the world. As a result, we acutely understand the impact of governments' policies on security innovation and the need for U.S. policies to be compatible with – and drive – global norms.

ITI commends NIST's work in leading the development of this Report, and we believe implementation of the Recommendations will help improve global cybersecurity. In particular, ITI strongly supports Recommendations 1 and 4.

1101 K Street, NW Suite 610
Washington, D.C. 20005
(202) 737 - 8888 | www.itic.org

Recommendation 1 espouses the creation of a new "high-level interagency coordination process for cybersecurity standardization," with interagency coordination driven and overseen by an Executive Office of the President policymaking body, and including the creation of a subordinate interagency working group hosted by the Department of Commerce. ITI has increasingly advocated for tighter coordination across the USG on cybersecurity policy and standards, and we believe this recommendation provides both sufficient authority and an effective structure to drive interagency coordination, as well as a mechanism for providing industry input though a familiar partner. In addition, we believe that the U.S. government must commit sufficient resources to support coordinated agency engagement in cybersecurity standards development over a period of five to ten years. Cybersecurity officials must be confident of long-term support to take on valuable leadership roles in standards development organizations.

Additionally, ITI strongly supports Recommendation 4: "Federal agencies should regularly promote close collaboration with the private sector in standards development for cybersecurity." Cyber-related challenges are ever expanding and evolving. Industry and governments share a common goal of better securing and facilitating cyber-based transactions and activities. Accordingly, we believe it is essential for governments to partner with the private sector, including information technology companies, to develop international standards that effectively respond to the complex challenges presented by cybersecurity issues.

Furthermore, ITI recognizes that cybersecurity standards issues are global in scope and, thus, that proposed solutions must be tailored to a global audience. We fully agree that the U.S. government "should ensure dialogue and information exchange takes place between senior Federal cybersecurity officials and their counterparts in key partner countries on cybersecurity standards development activities" (Recommendation 5).

Regarding the section "Background on conformity assessment" beginning at line 148, ITI requests that NIST augment the discussion of conformance testing and certifications. While there are a few select standards where third-party conformity assessment may be appropriate, a large majority of successful cybersecurity standards are implemented on a voluntary basis where self-attestation is an effective means of assurance. We believe this should receive greater emphasis in the Report.

Finally, ITI is appreciative that NIST points out in the Report the strong preference under U.S. law and policy that "Federal agencies are required to use voluntary consensus standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical." (See lines 116-177, n. 6 references to NTTA and OMB Circular A-119). However, given the overarching thrust of the Report is to set out strategic objectives for pursuing the development and use of international standards and a coordinated USG strategy to support this endeavor, we believe the Report can even more forcefully reiterate that U.S. federal agencies use voluntary and open standards, and connect this to the strong preference in favor of developing and using international cybersecurity standards, as stated numerous times elsewhere in the Report.

Again, thank you for the opportunity to provide feedback. We welcome any questions and comments regarding ITI views.