September 24, 2015

National Institute of Standards and Technology
Attn: Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930
Email: nistir8074@nist.gov

On behalf of Intel, we respectfully submit the attached comments in response to the request for comments. This submission is being filed electronically.

Sincerely,

Philip Wennblom
Director of Standards
Intel Corporation
philip.c.wennblom@intel.com

**Intel Corporation**
2200 Mission College Blvd.
P.O. Box 58119
Santa Clara, CA 95052-8119
408-765-8080 direct
www.intel.com

Intel appreciates the opportunity to provide comments on NIST IR 8074, "Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity."

Intel is the world's largest semiconductor manufacturer and a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world's computing devices and equipment. Intel invests substantially in development of cybersecurity technologies and international cybersecurity standards.

Intel supports the recommendations in IR 8074.

Because international standards are critically important in the area of cybersecurity, a coordinated USG process for engaging in cybersecurity standards development is essential. We agree with the report that, "USG should institute a high-level interagency coordination process for cybersecurity standardization."

We would like to emphasize the importance of public/private collaboration in cybersecurity standards development. As the report says in Recommendation 4, "Federal agencies should regularly promote close collaboration with the private sector in standards development for cybersecurity." Because collaboration and effective participation requires a long-term commitment of resources, we agree with the report that, "Federal agencies should support a long-term commitment of resources and participations with specialized knowledge, skills and abilities for international cybersecurity standardization." We encourage USG to continually improve collaboration models with industry to increase ability to respond quickly to the standardization needs of the dynamic environment today.

International coordination is increasingly important in cybersecurity standards development. We agree with Recommendation 5 and suggest that special attention be paid to the use of structured mechanisms for dialogue and information exchange with international stakeholders. International coordination also benefits pre-standardization activities; collaborative mechanisms for pre-standardization activities should be further improved and used to a greater degree.

Recalling our comments on the first draft of NIST IR 7977, Intel would like to highlight the importance of planning for global acceptance of cybersecurity technologies when NIST is involved in their development. As we said in our comments submitted in April 2014, "NIST should develop a global acceptance strategy for each standard it is involved with developing that it anticipates having a commercial impact. A key element of those strategies should be a stronger and more consistent preference for participating and contributing to security standards developed by open and fair international standards development organizations and then adopting the resulting standards for use by the U.S. Government." As the USG further strengthens its participation in international cybersecurity standards, it should continue to consider how that engagement can be utilized for gaining global acceptance of NIST developed technologies. In addition, we recommend that NIST strive to reference international standards wherever possible in NIST deliverables, especially when a referenced NIST specification has been further progressed to become an international standard.

Finally, we recommend that USG invest in promoting positive awareness of the benefits of adopting international cybersecurity standards. Not all countries recognize these benefits. International cybersecurity standards undergo extensive reviews by diverse groups of

**Intel Corporation**
2200 Mission College Blvd.
P.O. Box 58119
Santa Clara, CA 95052-8119
408-765-8080 direct
www.intel.com

cybersecurity experts, helping to achieve higher levels of security than is often provided in other standards.

Thank you for the opportunity to provide these comments.

**Intel Corporation**
2200 Mission College Blvd.
P.O. Box 58119
Santa Clara, CA 95052-8119
408-765-8080 direct
www.intel.com