CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

April 18, 2018

Via NISTIR-8200@nist.gov

Michael Hogan
Ben Piccarreta
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Subject: Draft NIST Interagency Report (NISTIR) 8200, *Status of International Cybersecurity Standardization for Internet of Things (IoT)*

Dear Messrs. Hogan and Piccarreta:

The U.S. Chamber of Commerce appreciates your efforts in developing the draft National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) 8200, *Status of International Cybersecurity Standardization for Internet of Things (IoT)*, referred to as NISTIR 8200 or the report.[1] This document is proceeding on the right track.

IoT Cybersecurity Needs to Be Rooted in Global, Industry-Driven Standards and Practices

In 2015, the Chamber supported NISTIR 8074, *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, which served as a precursor to NISTIR 8200. We believe that IoT cyber efforts are optimal when they reflect global standards and industry-driven practices. Initiatives to improve the cybersecurity of the public and private sectors should reflect the borderless and interconnected nature of our digital environment, including consumer and industrial devices.

Standards, guidance, and best practices relevant to cybersecurity are typically led by the private sector and adopted on a voluntary basis; they are most effective when developed and recognized globally. Such approaches avoid burdening multinational enterprises with the requirements of multiple, and often conflicting, jurisdictions.

The Chamber believes that NIST realizes how government-directed or centrally coordinated standards, procurement, and regulatory regimes—which are common in other countries—are poor architectures for cybersecurity and would spread companies' information-security budgets too thinly to meet the dictates of local magistrates.

[1] https://csrc.nist.gov/publications/detail/nistir/8200/draft

Any cybersecurity standardization processes that industry assumes would favor compliance and bureaucracy over creativity, speed, and innovation would almost certainly discourage buy-in from the private sector, which is crucial to the success or failure of most standards. The Chamber thinks that businesses need minimal structure and maximum autonomy to counter, in partnership with government, rapidly changing cyber threats.[2] NISTIR 8200 shows that multiple IoT cyber standards exist today that are applicable to connected vehicles, consumer IoT, smart manufacturing, and more, which is significant to industry.

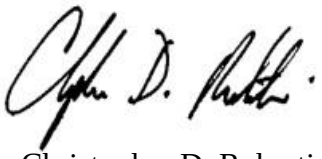
***

The Chamber welcomes the opportunity to provide feedback on NISTIR 8200. At a time when governments are developing either flexible plans or top-down directives to structure public-private approaches to IoT cybersecurity, NIST's positive role in assessing the status of international standards for IoT is significant to America's engagement strategy and U.S. business interests at home and abroad.

Setting standards needs to be a collaboration between industry and government, and the Chamber urges NIST to involve us as standards are created, revised, and implemented. We believe that the agency needs to be a champion for the American business community during its discussions with international standards bodies and regulators. Further, the smart and effective development of international standards for IoT cyber promotes U.S. commercial priorities by facilitating constructive outcomes like improved interoperability, higher confidence and trust in online and offline transactions, and strengthened competitiveness of American products and services.

If you have any questions or need more information, please do not hesitate to contact Christopher Roberti (croberti@uschamber.com, 202-463-3100) or Matthew Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,



Christopher D. Roberti
Chief of Staff
Senior Vice President, Cyber, Intelligence, and Security

Matthew J. Eggers
Vice President, Cybersecurity Policy

[2] www.nist.gov/itl/comments-draft-nistir-8074-volumes-1-and-2