CLIENT ALERT

APEC Taking Lead on IoT Standards and Cybersecurity

Oct.07.2019

The rapid growth of the Internet of Things (IoT) is creating new risks, vulnerabilities, and leadership opportunities for the private sector on a global scale. It is estimated 20 billion connected devices will be in operation by 2020 and IoT spending will total nearly $1.4 trillion by 2021.[1] As IoT creates new, innovative opportunities for businesses worldwide, it also introduces new types of cybersecurity risks that will begin to evolve and grow. To continue the secure, innovative growth of the global IoT sector, the business community must find a sustainable solution that takes into account all connected IoT devices, the applications they run, and the networks they use to transmit information.

In the United States, the National Institute of Standards and Technology (NIST) released its guidance document on securing IoT products in August of 2019, which recommends the cybersecurity features to include in these network-capable devices whether designed for consumer or commercial use. The NIST guidance references many of the major European efforts to secure IoT devices, including the European Union Agency for Network and Information Security (ENISA) (2017) Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, and the European Telecommunications Standards Institute (ETSI) (2019) Cyber Security for Consumer Internet of Things. ETSI Technical Specification 103 645 V1.1.1. At bottom, all of these guidance documents share a common purpose proposing ways to communicate securely, ensure software integrity, and minimize vulnerabilities.

Important guidance on IoT security has also been created by the Asia-Pacific Economic Cooperation (APEC), a group comprised of 21 economies that border the Pacific Rim.[2] APEC has positioned itself to be a global leader on the development of IoT frameworks, standards, and norms. Historically, APEC has a strong track record for creating standards within the digital economy, including developing the Framework for Securing the Digital Economy and the APEC Internet and Digital Economy Roadmap. Now, with impetus from the U.S. government, the APEC Committee on Trade and Investment (CTI) has started a multi-year initiative to address cybersecurity standards in the APEC region.

The first APEC cybersecurity standards workshop took place in Puerto Varas, Chile during the 3rd Senior Officials' Meeting in August 2019. Next year, APEC Malaysia 2020 will continue driving the momentum on cybersecurity issues by hosting a CTI workshop focused exclusively on IoT standards. This is a chance to get governments, industry, and academia to collaboratively address IoT challenges and solutions in one of the most dynamic, high-growth regions in the world.

[1] "Demystifying IoT Cybersecurity: The Internet of Things introduces new vulnerabilities across the entire ecosystem. Here's what you need to know—and prepare for", IoT Cybersecurity Alliance, 2017.

[2] Australia; Brunei Darussalam; Canada; Chile; China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; The Republic of the Philippines; The Russian Federation; Singapore; Chinese Taipei; Thailand; the United States of America; and Viet Nam

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Robert Holleyman
Partner and C&M International President & CEO – Washington, D.C.
Phone: +1 202.624.2505
Email: rholleyman@crowell.com

Clark Jennings
C&M International Managing Director, Asia – Singapore
Phone: +65.9111.0610
Email: cjennings@crowell.com

Cheryl A. Falvey
Partner – Washington, D.C.
Phone: +1 202.624.2675
Email: cfalvey@crowell.com

Olivia Burzynska-Hernandez
C&M International Consultant – Washington, D.C.
Phone: +1 202.624.2909
Email: ohernandez@crowell.com