crowell moring

CLIENT ALERT

On the Cyber Frontier of IoT Security

Apr.11.2018

In the Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT), the National Institute of Standards and Technology (NIST) performed an extensive survey of current cybersecurity standards applicable or potentially applicable to IoT devices. Among the many key findings and discussions, some of the more notable are: (1) NIST elected not to define IoT due to the many varying definitions already in the field (see Annex A); (2) NIST used several functional IoT applications (connected vehicles, consumer devices, health/medical devices, smart buildings and smart manufacturing) to assess current cyber standards and gaps; (3) NIST recognized that no one-size-fits-all standards exist, as specific sectors will have differing risk scenarios and security objectives, thus requiring cyber standards to be tailored; and (4) IoT security should be built around eleven core areas of cybersecurity standardization. Also, NIST is looking for your comments on draft NISTIR 8200 by April 18. To learn more, join us at the IoT National Institute on May 9-10 in Washington, D.C.

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

Jodi G. Daniel
Partner – Washington, D.C.
Phone: +1 202.624.2908
Email: jdaniel@crowell.com

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

Laura Foggan
Partner – Washington, D.C.
Phone: +1 202.624.2774
Email: lfoggan@crowell.com