Trump signs IoT Cybersecurity Improvement Act into law

Sarah A. Sargent
414.287.9450
ssargent@gklaw.com

Justin P. Webb
414.287.9527
jwebb@gklaw.com

Zachary R. Willenbrink
414.287.9463
zwillenbrink@gklaw.com

On Dec. 4, 2020, President Donald Trump signed into law the bipartisan-backed Internet of Things Cybersecurity Improvement Act of 2020. By its terms, the new law applies solely to federal government agencies, but its downstream consequences are likely to reach further, impacting devices procured by the federal government and—likely, eventually—consumer devices.

Internet of Things (IoT) devices are in widespread use, most visibly by consumers of new smart home devices. The new law defines IoT devices as those devices that:

1. Interact with the physical world
2. Have a network interface for transmitting or receiving information via the internet
3. *Are not* conventional information technology devices such as smartphones or laptops and cannot function as a component of another device such as a processor

Despite having a highly technical definition, IoT devices are common and becoming increasingly so. You probably even have several in your home or office, with many wireless devices—like refrigerators, smart speakers, networked printers, security systems and locks—satisfying this definition of an IoT device.

Though perhaps less visible than consumer adoption of IoT devices, the federal government's use of IoT devices is increasing and, given the federal government's significant size and buying power, impacting the market in meaningful ways. For instance, the Environmental Protection Agency (EPA) uses sensors that transmit data regarding weather conditions. Customs and Border Protection (CBP) uses autonomous surveillance towers that detect and identify items of interest at the border. NASA even uses spacesuits that monitor and transmit data regarding astronauts' vital signs. Although these items often serve more sophisticated functions than IoT devices purchased and used by consumers, many of the underlying technologies are similar or even identical.

Despite, or perhaps *because of*, their growing adoption, IoT devices are generally viewed as being more vulnerable to cyberattacks and subject to abuse as part of distributed denial of service (DDoS) attacks.

The IoT Cybersecurity Improvement Act seeks to reduce those risks, at least among IoT devices procured by the federal government. To achieve this goal, the new law:

1. Tasks the National Institute of Standards and Technology (NIST) with developing, publishing and updating security standards for IoT devices

2. Requires the Office of Management and Budget (OMB) to review each federal agency's information security policies to ensure they comply with the standards NIST promulgates for IoT devices

3. Prohibits federal agencies from procuring any devices that fail to comply with NIST's standards

Although NIST's standards are not yet drafted and, even when they are, will not impose any direct requirements on the private sector, it is important for all device manufacturers and sellers to pay close attention to developments. The sheer size and scope of the federal government's buying power may result in private sector businesses adopting the eventual NIST standards to ensure they can sell devices to the government. Similarly, the eventual NIST standards may provide a possible baseline for private sector businesses to satisfy and bring themselves into compliance with state IoT security laws that require "reasonable security features."

Godfrey & Kahn's Data Privacy & Cybersecurity Practice Group will continue monitoring developments stemming from this law, including NIST's eventual promulgation of security standards.

If you need any assistance in preparing for the implementation of NIST's standards, planning for the future of your IoT business, or any other data privacy and security matters, contact our Data Privacy & Cybersecurity Practice Group.