New Law Mandates Improved Cybersecurity for Government Internet of Things (IoT) Devices

On December 4, 2020, the Internet of Things (IoT) Cybersecurity Improvement Act of 2020 (the "Act") was enacted, to establish minimum security standards for IoT devices owned or controlled by the federal government, among other things.

The Act defines IoT devices as those which have "at least one transducer (sensor or actuator) for interacting directly with the physical world," "have at least one network interface" and which "are not conventional Information Technology devices, such as smartphones and laptops" as well as "can function on their own and are not only able to function when acting as a component of another device, such as a processor." Despite widespread and increasing deployment, cybersecurity is seen by some manufacturers as an optional add-on. This creates a massive risk for any organization, including the federal government, which deploys numerous IoT devices.

The Act:

• Requires the National Institute of Standards and Technology (NIST) to publish standards and guidelines on the appropriate use and management of IoT devices by the federal government, including minimum information security requirements for managing cybersecurity risks associated with such devices.
• Directs the Office of Management and Budget (OMB) to review federal government information security policies and principles and make any necessary changes to ensure they are consistent with NIST's standards and guidelines.
• Requires that the NIST standards and guidelines be updated every five years.
• Requires NIST to publish guidelines regarding security vulnerability relating to (i) information systems owned or controlled by the federal government and (ii) contractors and subcontractors providing to the federal government an information system (including an IoT device) receiving information about a potential security vulnerability relating to the information system and disseminating information about the resolution of a security vulnerability relating to the information system. OMB will oversee the implementation of these NIST guidelines.
• Prohibits the federal government from procuring or obtaining, renewing a contract to procure or obtain, or using an IoT device that does not comply with the foregoing standards and guidelines, subject to a waiver process for national security, for research purposes or that is secured using alternative and effective methods appropriate to the function of such device.
• Requires not later than two years after the date of the enactment of the Act, OMB, in consultation with the Secretary of Homeland Security to develop and oversee the implementation of policies, principles, standards, or guidelines as may be necessary to address security vulnerabilities of information systems (including IoT devices).

An anticipated consequence of the Act is to eventually steer IoT manufacturers towards adopting the same standards more uniformly, whether or not they seek to contract with the federal government.