COVINGTON

NIST Seeks Comment on Security for IoT Sensor Networks

February 6, 2019

Internet of Things, Privacy

The National Institute of Standards and Technology ("NIST") is seeking comments on its draft project on securing sensor networks for the Internet of Things ("IoT"). Organizations and individuals concerned with the security of IoT sensor networks are invited to comment on the draft through March 18, 2019.

Sensor networks are integral parts of many modern industries and critical infrastructure, including the electric grid, healthcare system, environmental protection, and manufacturing. These networks of small devices can detect, analyze, and transmit data, such as by monitoring and reacting to the physical characteristics around them—including temperature, pollution, humidity, and electrical usage. In the electric grid, for example, sensor networks may monitor and control the power generation of distributed resources, such as solar cells owned by consumers. Connected and automated vehicles are increasingly reliant on sensors deployed inside vehicles, and in road infrastructure, which detect and communicate environmental features and hazards to the vehicle. Sensor networks are also increasingly used in medical devices, which can be programmed to monitor an individual's health condition. They may also monitor properties of critical water supplies, including to determine the presence of minerals or toxins. The accuracy, integrity, and availability of the data being reported and monitored by a sensor network can be critical.

While the NIST project focuses on sensor networks used for building management—for example, systems designed to open and close vents based on temperatures or to stop pulling air into a facility at a certain humidity threshold—NIST expects its work to be "applicable to multiple industry sectors." According to NIST, the wireless sensor network market was valued at $573 million in 2016 and is projected to increase to at least $1.2 billion by 2023.

The 29-page project on which NIST seeks public comment focuses on the requirements to ensure sensor networks function securely. It identifies threats relevant to each component and technologies that can be used to help improve security. The document also maps the characteristics of such commercial technologies to the NIST Cybersecurity Framework.

NIST has identified four goals for the project:

- Serve as a building block for sensor networks in general, future IoT projects, or specific sensor network use cases
- Establish a security architecture to protect a building management system sensor network by using standards and best practices, including the communications

channel/network used to transmit sensor data to the back-end building control systems (hosts) for processing

- Explore the cybersecurity controls to promote the reliability, integrity, and availability of building management system sensor networks
- Exercise/test the cybersecurity controls of the building management system sensor network to verify that they mitigate the identified cybersecurity concerns/risks, and understand the performance implications of adding these controls to the building management system sensor network

Comments are sought through March 18, 2019. Organizations and individuals are invited to submit their comments online or via email.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Internet practice:

Kate Goodloe	+1 202 662 5505	kgoodloe@cov.com
Zachary Mears	+1 202 662 5414	zmears@cov.com