

NIST Seeks Input on Managing IoT Privacy, Cybersecurity Risk

The Commerce Department is seeking comment on managing the privacy and cybersecurity risks of connected devices.

A [draft internal report](#) from Commerce's National Institute of Standards and Technology lays out high-level ideas and recommendations for how organizations can mitigate the risks related to devices that connect to the internet and can interact with each other. Commonly known as the internet of things, these devices can include smart thermometers, cars, and coffee makers. The comment period closes Oct. 24.

The IoT market has raised concerns about the vast amount of personal and corporate data that could be exposed if a hacker exploited a vulnerability in a single device. A 2017 Gartner Inc. report estimated there will be 20 billion internet-connected devices deployed by 2020.

“Many organizations are not necessarily aware of the large number of IoT devices they are already using and how IoT devices may affect cybersecurity and privacy risks differently than conventional information technology (IT) devices do,” the agency said in the draft report.

Each sector has its own types of IoT devices, which carry different risks from each other and from traditional devices. IoT devices interact with the “physical world” differently than conventional devices, and can also be accessed and monitored in different ways, NIST said.

The agency suggests adjusting policies to address changing risk mitigation challenges throughout device lifecycles, such as figuring out what capabilities the device has, assessing the risk of a device in its environment rather than in isolation, and knowing which devices are in use.

Other voluntary considerations include updating risk mitigation practices, which may need to be done for hundreds or thousands of IoT device types per organization. Each type of device carries its own privacy and cybersecurity risks, NIST said in the report.

The draft internal report provides baseline privacy and cybersecurity risk mitigation strategies for IoT devices. NIST plans a series of publications to address more specific recommendations for particular types of devices, the agency said.