Client Alert: NIST Guidelines Expanded to Include 'Internet of Things' Devices and Systems in the Private Sector

Related Professionals

John L. Landolfi

Christopher L. Ingram

Christopher A. LaRocco

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 8.25.2017

The National Institute of Standards and Technology (NIST) recently released an updated draft of its Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations* that sets forth cybersecurity guidance for securing devices and software commonly referred to as the "internet of things." The draft represents NIST's latest attempt to produce a unified information security framework for the federal government that is now also bleeding into the private sector.

While previous versions of the draft targeted only federal agencies, NIST's latest update targets privacy protections for the private sector. For the first time, the draft sets forth security controls intended to help private sector companies in securing the "internet of things." The list of security controls includes both technical and procedural safeguards that are designed to protect systems, organizations, and individuals. NIST's latest guidance gives private sector companies a framework for securely using these types of devices. For instance, the guidelines set forth procedures and technical information necessary in protecting "smart" medical devices.

The draft also fully integrates privacy controls across all systems aimed at limiting unnecessary exposure to various types of personal information. For instance, one particular privacy control addresses the data captured by sensors, such as those used in traffic monitoring cameras or parking garages. The control establishes protocols that companies can use to configure these sensors to avoid unnecessary collection of personal information. Another privacy control, which is particularly useful to retailers, details the process for developing or purchasing "consent tools" used in gathering customer consent. The control sets forth several key recommendations such as: using active voice and conversational style; logical sequencing of main points; consistent use of the same word (rather than synonyms to avoid confusion) and; the use of bullets, numbers, and formatting where appropriate to aid readability; and legibility of text such as font style, size, color and contrast.

Companies considering employing interconnected devices or “internet of things” devices should review the new draft, available here. For questions on SP 800-53, cybersecurity programs, or data privacy, please contact John Landolfi, Chris Ingram, Chris LaRocco, or your Vorys attorney.