GIBSON DUNN

February 17, 2021

NEW FEDERAL LAW FOR IOT CYBERSECURITY REQUIRES THE DEVELOPMENT OF STANDARDS AND GUIDELINES THROUGHOUT 2021

To Our Clients and Friends:

I. Introduction

At the end of the Trump Administration, the bipartisan Internet of Things (IoT) Cybersecurity Improvement Act of 2020 ("the Act") was enacted after passing the House of Representatives on a suspension of the rules and the Senate by unanimous consent. The Act requires agencies to increase cybersecurity for IoT devices owned or controlled by the federal government. Despite its seemingly limited scope, the Act is anticipated to have a significant, wide-ranging impact on the general development and manufacturing of IoT devices.

The Internet of Things is the "extension of internet connectivity into physical devices and everyday objects."[1] It covers devices — often labeled as "smart devices" — that have a network interface, function independently, and interact directly with the physical world."[2] While the Act's definition of IoT devices expressly excludes conventional information technology devices (for example, computers, laptops, tablets, and smartphones),[3] it extends to a variety of sensors, actuators, and processors used by the federal government.[4] Agencies have reported using IoT devices for controlling or monitoring equipment, tracking physical assets, providing surveillance, collecting environmental data, monitoring health and biometrics, and many other purposes.[5] This usage is likely to expand as over 85% of federal agencies either are currently employing IoT devices or plan to do so in the next five years, further elevating the significance of the Act.[6]

Although the Act is focused on federal government IoT devices, it has significant implications for the widespread and growing corporate and private consumer use of these devices. The North American market for IoT devices has been valued around $95 billion in 2018 and forecasted to be $340 billion by 2024.[7] This has been driven by about 2.3 billion IoT device connections in 2018, which are expected to reach almost 6 billion by 2025.[8] The global market for these devices is similarly expected to grow substantially, with an approximately 37% increase from 2017 to over $1.5 trillion by 2025.[9] This global number of active IoT devices is projected to rise from 9.9 billion in 2019 to 21.5 billion in 2025.[10] As federal standards are often a baseline or guide for industries, such as for product manufacturers seeking uniformity and efficiency, the measures set pursuant to the IoT Cybersecurity Improvement Act should be closely monitored by all industry stakeholders.

II. Provisions of the Act

The Act has a few primary components for strengthening IoT cybersecurity and the government's critical technology infrastructure. First, the National Institute of Standards and Technology (NIST) is tasked with developing security standards and guidelines for the appropriate use and management of all IoT devices owned or controlled by the federal government and connected to its information systems.[11] This includes establishing minimum information security requirements for managing cybersecurity risks associated with these devices. In formulating these guidelines, NIST must consider its current efforts regarding the security of IoT devices, as well as the "relevant standards, guidelines, and best practices developed by the private sector, agencies, and public-private partnerships."[12] Within 90 days, NIST will promulgate the standards and guidelines for the Office of Management and Budget (OMB) to implement, under consultation with the Department of Homeland Security (DHS) as necessary, by reviewing agency information security policies and principles for consistency.[13] Devices that are a part of a national security system, however, are exempt from review by OMB.[14]

A second set of the Act's provisions govern the disclosure process among federal agencies and contractors regarding information security vulnerabilities. Again, NIST is tasked with creating guidelines, within 180 days, to advise agencies and contractors on measures for receiving, reporting, and disseminating information about security vulnerabilities and their resolution.[15] These guidelines will also be formulated by considering non-governmental sources in order to better align them with industry best practices, international standards, and "any other appropriate, relevant, and widely-used standard."[16] Similarly, these measures will be implemented by OMB in consultation with DHS, who will also provide operational and technical assistance to agencies.[17]

While the previous components will set the baseline for federal IoT cybersecurity standards, the real bite of the Act comes from its prohibition on agencies from procuring, obtaining, or using any IoT devices that would render an agency non-compliant with NIST's standards and guidelines.[18] These determinations will be made by an agency's Chief Information Officer (CIO) upon reviewing its government contracts involving IoT devices.[19] Agency heads have some flexibility to waive this prohibition, however, if the agency CIO determines that the device is necessary for either national security interests or research purposes, or if it is secured using alternative and effective methods based on the function of the device.[20] IoT device manufacturers currently supplying or vying for government contracts should ensure cybersecurity compliance by the time that the prohibition takes effect in December 2022.[21] All other IoT device manufacturers, including those that focus entirely on private consumers, would also be well-advised to carefully consider the requirements established pursuant to the Act, as the U.S. government is the single largest consumer in the world and creates standards that are likely to have trickle-down effects on the industry as a whole.

Lastly, a few of the Act's remaining provisions require the Government Accountability Office (GAO) to submit reports to Congress on the processes established by the Act and broader IoT efforts.[22]

III. Draft Guidance by NIST

Since the Act was passed, NIST has already started carrying out its mandate by releasing four new public drafts of its guidance on IoT cybersecurity. The first document — Draft NIST SP 800-213 — is a part of the Special Publication 800-series developed to address and support the security and privacy needs of U.S. government information systems.[23] This draft provides guidance for federal agencies to establish and evaluate the security capabilities required in their IoT devices.[24] It includes background information on the security challenges posed by IoT devices, as well as various considerations for managing risks and vulnerabilities.

The remaining three draft documents — NIST Interagency Reports (NISTIRs) 8259B, 8259C, and 8259D — build upon a series directed at establishing baselines for IoT device manufacturers to identify and meet the security requirements expected by customers.[25] This 8259-series currently contains a total of five documents that together discuss foundational cybersecurity activities, baselines for cybersecurity and non-technical capabilities, and a process for developing customized cybersecurity profiles to meet the needs of specific IoT device customers or applications.[26] The series contains an example of the process applied to create a profile on the federal government customer, which can also serve as a guide for manufacturers to profile other customers and markets. On January 7, 2021, NIST also published a report — NISTIR 8322 — summarizing the feedback received from its July 2020 workshop on the creation of the federal profile of IoT device cybersecurity requirements.[27]

Since releasing the drafts, NIST has opened a public comment period for soliciting community input. This comment period was recently extended to February 26, 2021. Any IoT stakeholders should consider reviewing the documents and providing feedback to NIST. The Act directs NIST to release finalized standards and guidelines by March 4, 2021, for the appropriate use and management of government IoT devices by federal agencies.[28] NIST must also establish its guidelines for receiving, reporting, and disseminating information about security vulnerabilities and their resolution by June 2, 2021.[29]

IV. Context and Effect

The IoT Cybersecurity Improvement Act of 2020 will undoubtedly help strengthen critical technology infrastructure, although how effective it will be at preventing attacks remains to be seen. The Act comes at a time when addressing information security vulnerabilities in the government's contractor supply chain is as pressing as ever.

Some IoT devices released into consumer markets have turned out to have insufficient cybersecurity protections, as cyber criminals have found ways to exploit the trade-offs between cost, expediency, and security made by manufacturers to meet rapidly evolving consumer demands. Cyber criminals have taken advantage of IoT vulnerabilities to access systems and data, as well as to commit denial-of-service or ransomware attacks. For example, the infamous Mirai botnet used insecure IoT devices to conduct a massive distributed denial-of-service attack in 2016 that took down the websites of multiple major U.S. companies.[30] This issue has only intensified as the global coronavirus pandemic has driven further reliance on IoT devices. A recent report indicated that the share of IoT devices being infected has doubled in 2020 compared to other similarly connected devices.[31]

Very few states have enacted legislation requiring IoT device manufacturers to meet certain cybersecurity standards. These states include California and Oregon, both of which mandate manufacturers to equip devices with "reasonable security feature[s]."[32] Beyond the U.S., Europe has a baseline cybersecurity standard for consumer IoT devices, which was released by the European Telecommunications Standards Institute in June 2020,[33] as well as guidelines by the European Union Agency for Cybersecurity (ENISA) for securing supply chain processes used to develop IoT products.[34] The U.K. has also taken recent regulatory steps to directly address IoT device cybersecurity.[35] As the first federal legislation in the U.S. targeting IoT security, the IoT Cybersecurity Improvement Act is a welcome addition to the country's historically sectored and disparate legal landscape for information security and data privacy.

The Act's improvements for federal IoT device security are anticipated to similarly strengthen and push forward protections in the private sector. The cybersecurity standards for federal IoT devices and contractors are likely to both reflect and shift what security features are deemed "reasonable" — the legal standard adopted by California and Oregon for evaluating IoT device security.[36] The concept of reasonableness is also used to assert civil liability against product manufacturers by claiming that the lack of certain features or measures is unreasonable and a failure of the duty of care. As NIST is required to consider private sector best practices in developing its standards and guidelines, the public-private relationship can create a positive feedback loop that will propel IoT cybersecurity protections towards continuous improvement. Some manufacturers could maintain and highlight distinctions between public and private consumer security needs to attempt to avoid having the federal standards used against them in civil liability. Others manufacturers of IoT devices may simply find it easier to have uniform security mechanisms in both their government and private consumer products. Nonetheless, the developing standards and guidelines being established pursuant to the IoT Cybersecurity Improvement Act will have significant implications for the IoT device industry as a whole and should be carefully considered.

* * *

The legal issues and obligations related to the IoT Cybersecurity Improvement Act of 2020 are likely to shift as federal agencies implement its provisions. We will continue to monitor and advise on developments, and we are available to guide companies through these and related issues. Please do not hesitate to contact us with any questions.

---

[1] Cong. Rsch. Serv., *H.R.1668 — IoT Cybersecurity Improvement Act of 2020: Summary*, Congress.Gov, https://www.congress.gov/bill/116th-congress/house-bill/1668 (last visited Dec. 29, 2020).

[2] Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, § 2(4), 134 Stat. 1001, 1001 (2020).

[3] *See id.*

[4] U.S. Gov't Accountability Off., GAO-20-577, Internet of Things: Information on Use by Federal Agencies 5 (2020).

[5] *Id.* at 7–11.

[6] *Id.* at 11–12.

[7] Shanhong Liu, *Internet of Things in the U.S. — Statistics & Facts*, Statista (May 29, 2020), https://www.statista.com/topics/5236/internet-of-things-iot-in-the-us.

[8] *Id.*

[9] Patricia Moloney Figliola, Cong. Rsch. Serv., IF11239, The Internet of Things (IoT): An Overview 2 (2020), https://crsreports.congress.gov/product/pdf/IF/IF11239 (citing the predictions by IoT Analytics).

[10] *Id.* at 1.

[11] IoT Cybersecurity Improvement Act § 4(a)(1).

[12] *Id.* § 4(a)(2)–(3).

[13] *Id.* § 4(b)(1)–(2). OMB shall conduct this review no later than 180 days after NIST completes the development of the relevant standards and guidelines. *Id.* § 4(b)(1).

[14] *Id.* § 4(b)(3).

[15] *See id.* § 5(a).

[16] *Id.* § 5(b)(1).

[17] IoT Cybersecurity Improvement Act §§ 5(d)–(e), 6(a)–(c). OMB shall develop and oversee this implementation no later than two years after the Act is enacted. *Id.* § 6(a).

[18] *Id.* § 7(a)(1).

[19] *Id.* § 7(a)(1).

[20] *Id.* § 7(b).

[21] *Id.* § 7(d).

[22] *Id.* §§ 7(c), 8.

[23] *NIST Special Publication 800-Series General Information*, Nat'l Inst. Standards & Tech. (May 21, 2018), https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information.

[24] Michael Fagan et al., *SP 800-213 (Draft) — IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, Nat'l Inst. Standards & Tech. (Dec. 2020), https://csrc.nist.gov/publications/detail/sp/800-213/draft.

[25] *Defining IoT Cybersecurity Requirements: Draft Guidance for Federal Agencies and IoT Device Manufacturers (SP 800-213, NISTIRs 8259B/C/D)*, Nat'l Inst. Standards & Tech. (Dec. 15, 2020), https://www.nist.gov/news-events/news/2020/12/defining-iot-cybersecurity-requirements-draft-guidance-federal-agencies-and.

[26] Michael Fagan et al., *NISTIR 8259 — Foundational Cybersecurity Activities for IoT Device Manufacturers*, Nat'l Inst. Standards & Tech. (May 2020), https://csrc.nist.gov/publications/detail/nistir/8259/final; Michael Fagan et al., *NISTIR 8259A — IoT Device Cybersecurity Capability Core Baseline*, Nat'l Inst. Standards & Tech. (May 2020), https://csrc.nist.gov/publications/detail/nistir/8259a/final; Michael Fagan et al., *NISTIR 8259B (Draft) — IoT Non-Technical Supporting Capability Core Baseline*, Nat'l Inst. Standards & Tech. (Dec. 2020), https://csrc.nist.gov/publications/detail/nistir/8259b/draft; Michael Fagan et al., *NISTIR 8259C (Draft) — Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline*, Nat'l Inst. Standards & Tech. (Dec. 2020), https://csrc.nist.gov/publications/detail/nistir/8259c/draft; Michael Fagan et al., *NISTIR 8259D (Draft) — Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government*, Nat'l Inst. Standards & Tech. (Dec. 2020), https://csrc.nist.gov/publications/detail/nistir/8259d/draft.

[27] Katerina Megas et al., *NISTIR 8322 — Workshop Summary Report for "Building the Federal Profile For IoT Device Cybersecurity" Virtual Workshop*, Nat'l Inst. Standards & Tech. (Jan. 2021), https://csrc.nist.gov/publications/detail/nistir/8322/final.

[28] *See* IoT Cybersecurity Improvement Act § 4(a)(1).

[29] *See id.* § 5(a).

[30] *See* Nicole Perlroth, *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, N.Y. Times (Oct. 21, 2016), https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html.

[31] Nokia, Threat Intelligence Report 2020 9 (2020), https://onestore.nokia.com/asset/210088.

[32] *See* Cal. Civ. Code § 1798.91.04(a) (2018); Or. Rev. Stat. § 646A.813(2) (2019). Some states have proposed similar legislation. *See, e.g.*, H.B. 3391, 101st Gen. Assemb., Reg. Sess. (Ill. 2019); A.B. 2229, Gen. Assemb., Reg. Sess. (N.Y. 2019); H.B. 888, 441st Gen. Assemb., Reg. Sess. (M.D. 2020).

[33] Sophia Antipolis, *ETSI Releases World-Leading Consumer IoT Security Standard*, ETSI (June 30, 2020), https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard.

[34] *IoT Security: ENISA Publishes Guidelines on Securing the IoT Supply Chain*, ENISA (Nov. 9, 2020), https://www.enisa.europa.eu/news/enisa-news/iot-security-enisa-publishes-guidelines-on-securing-the-iot-supply-chain.

[35] Dep't for Digital, Culture, Media & Sport, *Secure by Design*, Gov.UK (July 16, 2020), https://www.gov.uk/government/collections/secure-by-design#history.

[36] *See* Cal. Civ. Code § 1798.91.04(a) (2018); Or. Rev. Stat. § 646A.813(2) (2019).

This article was prepared by Alexander H. Southwell, a partner in Gibson Dunn's New York office, and Terry Y. Wong, a recent law graduate working in the Firm's New York office who is not yet admitted to practice law.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any of the following members of the firm's Privacy, Cybersecurity and Data Innovation practice group:

United States

Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen – Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)

GIBSON DUNN

Europe

Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com)
Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Bernard Grinspan – Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic – Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen – London (+44 (0) 20 7071 4203, swazen@gibsondunn.com)

Asia

Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)