EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

December 15, 2023

The Honorable Mark R. Warner
United States Senate
Washington, DC 20510

Dear Senator Warner:

This responds to your letter dated September 26, 2023, regarding the implementation of the Internet of Things Cybersecurity Improvement Act of 2020[1] (the Act) to update you on the steps the Office of Management and Budget (OMB) has taken to implement the Act and to strengthen the Federal Government's approach to securing Internet of Things (IoT) devices. We agree that IoT cybersecurity is of critical importance to our national security. OMB's chief goal at this time is to ensure that agency IT leaders have visibility into the IoT devices in their enterprise environment, and have assessed risks so that they can impose appropriate security requirements and take other mitigating actions.

As you note in your letter, the Act directs OMB to review agency information security policies for consistency with the IoT standards and guidelines of the National Institute of Standards and Technology (NIST) and to "issue such policies and principles as may be necessary to ensure" that consistency.[2] NIST's standards and guidelines, found in NIST Special Publication 800-213, advise organizations to select cybersecurity requirements for IoT devices and provide high-level, general background and considerations intended to aid in that task.

Beginning in early 2023, OMB assessed agency policies for consistency with NIST's standards and guidelines by conducting a time- and labor-intensive series of meetings with a diverse set of agencies to better understand how they are deploying, managing, and securing IoT assets. Based on those engagements, OMB concluded that relatively few formal agency policies address the selection of cybersecurity requirements specifically for IoT devices.

Consistent with its obligations under the Act, OMB has acted to fill that gap. Because an enormous array of disparate devices may be considered part of the IoT, OMB determined that a governmentwide policy on establishing security requirements for IoT devices should first clarify which devices should be prioritized for urgent agency attention, and then require agencies to identify and document any of those devices connected to their information systems. Accordingly, OMB Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and*

[1] Pub. L. No. 116-207.
[2] 15 U.S.C. § 278g-3b(b)(1).

Privacy Management Requirements, released on December 4, 2023, requires agencies to prepare an enterprise-wide inventory of "covered IoT assets"—IoT devices, including operational technology (OT), that are embedded with programmable controllers, integrated circuits, sensors, and other technologies for the purpose of collecting and exchanging data with other devices and/or systems over a network in order to facilitate enhanced connectivity, automation, and data-driven insights across devices and systems.[3]

In complying with that requirement, agencies will document critical functions of their IoT devices and evaluate potential attack or disruption pathways adversaries could leverage to compromise those devices and the IT systems to which they connect. Taking these important actions will help agencies account for sector-specific threats and vulnerabilities. These steps will also allow agencies to take the appropriate actions to mitigate IoT cybersecurity risks by better enabling them to identify and patch vulnerabilities, respond to cyber incidents, and implement actions required by the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency's binding operational directives and emergency directives.

All of those efforts, of course, represent only one stage in the drive to secure agency IoT devices in a consistent manner. As agencies gain a comprehensive understanding of the range of those devices present across the Government and their role in Federal information systems, the Chief Information Security Officers' Council will be working with agencies to develop playbooks documenting security best practices for the IoT devices most commonly used in sectors such as healthcare, industrial control, and aerospace. OMB anticipates that these playbooks and the governmentwide IoT inventory mandated by M-24-04 will lay the groundwork for further developments in IoT security policy.

In addition to its review of agency policies and issuance of M-24-04, OMB has also implemented the Act by establishing a standardized process for the issuance of waivers pursuant to section 7(b) of the Act.[4] OMB tracks the waivers that agencies grant. During Fiscal Year 2023, four systems across the entire Federal enterprise overseen by OMB had IoT devices with waivers for not complying with NIST's IoT standards and guidelines; no agency had more than one system with a waiver. This accounts for less than two percent of the total number of systems with IoT devices that agencies have reported to OMB.

OMB has also worked with the Federal Acquisition Regulatory (FAR) Council to strengthen the procurement rules around IoT devices. On October 3, 2023, the FAR Council published a proposed rule in the *Federal Register* that would require contracts for the management of a Federal information system to specify any cybersecurity requirements necessary for IoT devices in accordance with NIST SP 800-213. The proposed rule would also implement the Act's prohibition on agencies' acquisition of an IoT device determined to be non-compliant with NIST standards and guidelines, absent a waiver by the agency head.[5]

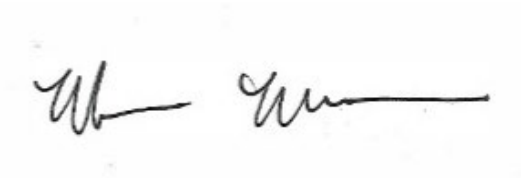
---

[3] M-24-04, at p. 5-8.
[4] 15 U.S.C. § 278g-3e(b).
[5] FAR Case 2021-019, Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems.

Finally, OMB serves as a key stakeholder in the development of the "U.S. Cyber Trust Mark" through the Federal Communications Commission's Cybersecurity Labeling Program for internet-enabled devices.[6] This voluntary labeling program would provide information to consumers about the relative security of internet-enabled devices. Such devices or products bearing the Commission's proposed cybersecurity label would be recognized as adhering to certain cybersecurity practices. If implemented as proposed, the program would simplify procurement decisions and reduce security risks for these technologies, both within and outside the Federal Government.

The Administration shares your view that cybersecurity of IoT devices is a critical priority, and I look forward to continuing to work with you on this important issue. If you have any questions, please contact the Office of Legislative Affairs at OMBLegislativeAffairs@omb.eop.gov.

Sincerely,



Wintta M. Woldemariam
Associate Director
Office of Legislative Affairs

[6] FCC Proposes Cybersecurity Labeling Program for Smart Devices | Federal Communications Commission.