U.S. Chamber of Commerce
Preliminary Feedback
IoT Cybersecurity Improvement Act of 2019 (S. 734 and H.R. 1668)
July 2, 2019

In June 2019, the Senate Homeland Security and Governmental Affairs Committee (HSGAC) and the House Oversight and Reform Committee (O&R) passed their respective versions of the IoT Cybersecurity Improvement Act of 2019 (S. 734 and H.R. 1668). The committees reported amendments in the nature of a substitute (ANS or substitute amendments) to the underlying legislation. The substitute amendments are different both from one another and the original legislation that was introduced last spring.

Bill writers are commended for capturing in the legislation that industry and the National Institute of Standards and Technology (NIST) are developing a core cybersecurity capabilities baseline for Internet of Things (IoT) devices. This recognition is a key change from the last Congress. Indeed, a top U.S. Chamber of Commerce priority for industry is to achieve consensus on the technical criteria that support the IoT cyber baseline. The Chamber wants device makers, service providers, and buyers to gain from the development of state-of-the-art IoT components and sound risk management practices.[1]

FURTHER DISCUSSIONS NEEDED

The Chamber urges additional dialogue on whether to define IoT in legislation and the specifics of the coordinated vulnerability disclosure (CVD) program, which are covered on pages 2 and 3. Meanwhile, it needs to be stressed that lawmakers' work remains incomplete. First, Congress should consider a national, more sustainable way to bolster IoT cybersecurity, rather than regulating the federal market for IoT devices. Such an approach would be critical to reducing the expanding policy and regulatory fragmentation that is taking place domestically and overseas.[2]

The Chamber urges Congress to develop legislation that would both spur device makers to build to the cyber baseline and grant legal liability and regulatory protections to the makers and sellers of strong IoT equipment. Legislation of this kind would be a win-win for government and industry.

Second, S. 734 and H.R. 1688 presuppose devices being hacked illegally, but they do not put pressure on malicious actors that threaten connected devices and their underlying networks. Policymakers should not place new mandates on businesses while leaving cyberattackers untouched. The Chamber made this argument to bill writers in 2017, and yet it has gone unaddressed. The legislation needs to elevate the government's portion of the security burden to make the mantra that cybersecurity is a shared public-private responsibility meaningful. As they are currently written, S. 734 and H.R. 1688 put the defense of IoT devices, particularly against nation-states hackers or their surrogates, on the shoulders of the private sector. Businesses should not have to contend with top cyber threats (e.g., Russia, China, Iran, and North Korea) single-handedly.[3]

IOT DEFINITION

The Senate ANS does not contain a specific definition of an IoT, or a "covered," device. This bill, alternatively, would defer decision making to NIST on the scope of IoT. Sec. 3(a) of the ANS requires NIST to develop "standards and guidelines . . . including minimum security requirements" on federal agencies' use and management of IoT devices.

The Chamber has generally not supported writing an IoT definition into law.[4] Among other things, IoT devices reside within a larger cyber ecosystem that features an array of consumer and industrial devices. Given the rapidly changing technology environment, what we call IoT devices today may be described differently in just a few years. In addition, the Chamber, like many cyber stakeholders, believes that public policy should be technology-neutral to avoid picking winners and losers.

The dominant message we hear from industry is that it does not want the added compliance burdens of the federal IoT cyber procurement legislation. Most businesses want to focus on incorporating baseline security capabilities into their devices instead of contending with the bureaucratic processes that accompany a top-down program. Further, the legislation lacks broad incentives (e.g., legal liability and regulatory protections) to make coverage appealing beyond those companies that sell to the U.S. government.

Any legislation that contains a definition of IoT should be as narrowly tailored as possible. The Senate ANS does not contain a definition of IoT, but the House ANS does. Recommended changes to the covered device definition in the House bill are provided in blue text.

House ANS

(2) COVERED DEVICE.—The term "covered device" means a physical object that—
- (A) is ~~capable of being~~ in regular connection with—
  - (i) the Internet; or
  - (ii) a network that is connected to the Internet on a recurring basis;
- (B) has computer processing capabilities of collecting, sending, or receiving data; and
- (C) is not a—
  - (i) general-purpose computing device;
  - (ii) personal computing system;
  - (iii) smart mobile communications device;
  - (iv) programmable logic controller with an industrial control system specifically not designed for connection to the internet;
  - (v) mainframe computing system; or
  - (vi) subcomponent of a device.

CVD PROGRAM

The House ANS would require covered devices to take part in a federal CVD program. Sec. 6(c) calls on the Office of Management and Budget (OMB), in consultation with the General Services Administration (GSA) and the Department of Homeland Security (DHS), to promulgate "standards and regulations" based on NIST guidelines for reporting and mitigating IoT vulnerabilities of government-bought devices.

The Senate ANS also captures IoT devices in a CVD regime. This bill raises a number of concerns. First, the Chamber questions the scope of the CVD program. Sec. 5 would include IoT devices and agencies' information systems, which is a noteworthy change from the introduced version of S. 734. The guidelines developed pursuant to sec. 5(a) would include information about a "potential security vulnerability or *personal information* vulnerability" tied to an agency's information system. The ANS is silent on the meaning and intent behind adding personal information to the CVD program [italics added].

Second, sec. 6(b) calls for DHS, in consultation with OMB, to "develop and issue *procedures* for each agency on reporting, coordinating, publishing, and receiving information about security vulnerabilities of information systems," including IoT devices [italics added]. It is unclear what the procedures are supposed to accomplish in practice. Current law and policies, including the Federal Information Security Modernization Act of 2014 and OMB circulars, already require agencies to report security vulnerabilities to DHS and OMB.

Third, sec. 6(c) calls for contractor and vendor compliance with OMB policies and procedures. However, the government has plenty of security requirements governing businesses that sell to agencies. The Chamber is skeptical of new and possibly confusing terms and redundant authorities and unaware of any gaps in legislative authority. We do not want to give agencies more authority to intervene in private entities' cybersecurity and innovation processes.

Fourth, the Chamber urges lawmakers to ensure that the IoT CVD program applies only to agencies and not to private-sector CVD practices beyond contractors/vendors. The CVD regime should be developed judiciously and align with industry best practices, as well as ISO standards 29147 and 30111. The legislation should also clearly state that there are no requirements to predisclose vulnerabilities to agencies or mandates regarding vulnerability disclosure and mitigation timelines.

Endnotes

[1] The Chamber is assessing the establishment of a Buy Strong IoT Coalition to promote the production, purchase, and deployment of more secure IoT products. If created, the Coalition would explore facilitating a process in the marketplace that generates both security and value for buyers and sellers. Market and/or policy incentives may be needed to initiate progress, but the specifics are yet to be determined.

[2] The Chamber testified before a Senate Commerce, Science, and Transportation Committee subcommittee in April 2019, saying that a fragmented cybersecurity environment—including S. 734 and H.R. 1668, California's device security law, and the European Union's Cybersecurity Act—creates uncertainty for device makers and buyers and splinters the resources that businesses devote to sound device development, production, and assessments.
https://www.commerce.senate.gov/public/index.cfm/2019/4/strengthening-the-cybersecurity-of-the-internet-of-things

[3] https://www.acq.osd.mil/dsb/reports/2010s/dsb-cyberdeterrencereport_02-28-17_final.pdf

[4] House Oversight and Government Reform Committee Information Technology Subcommittee hearing *Cybersecurity of the Internet of Things*, October 3, 2017. See, in particular, endnote number 7 of the Chamber's testimony.
https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=106460
https://docs.house.gov/meetings/GO/GO25/20171003/106460/HHRG-115-GO25-Wstate-EggersM-20171003.pdf