For internal review (revised June 5, 2018)

WORKING SUMMARY

State of Negotiations Regarding S. 1691, the Internet of Things (IoT) Cybersecurity Improvement Act of 2017

On Friday, June 1, the U.S. Chamber communicated to Sens. Mark Warner (Rafi Martina, senior policy adviser) and Cory Gardner (Sam Love, legislative assistant) that our organization is neutral on the latest version of S. 1691 (dated June 1). This new draft is dubbed the redline/blueline version, reflecting both BSA's May 18 edits and bill writers' May 31 edits, respectively. The Chamber's neutral position is in keeping with the understanding that Sen. Warner and Chamber CEO Tom Donohue discussed in May.

On Friday, the Chamber's Cybersecurity Working Group members discussed the possibility of supporting the bill on two calls. We heard that concerns still remain, especially the scope of covered devices, which makes support for the bill a tough climb. Members also have questions about how the legislation would work in practice. The Chamber suggested to Hill staff a few tweaks to the redline/blueline draft, which are highlighted in yellow (see attachment), such as urging that the device database(s) not be publicly available.

HIGHLIGHTS

- The U.S. Chamber is neutral on the latest version of S. 1691 (aka the redline/blueline version), which is dated June 1.
- The revised legislation narrows the scope of covered devices and reduces the security requirements that are written into law.
- The updated version of S. 1691 steers policymakers away from mandating specific requirements in legislation toward ensuring that agencies' acquisition clauses can adapt to changing security environments. The bill directs OMB to align security clauses with existing voluntary consensus standards.
- The updated legislation no longer relaxes protections granted to businesses under the CFAA and the DMCA.
- S. 1691 could get marked up in Senate HSGAC on June 13. The agenda is not set yet. Industry stakeholders should continue to communicate with bill writers and HSGAC.

The Chamber welcomes the constructive changes that have been made to the bill. However, it wants to continue contributing to the writing of S. 1691 as it moves through the legislative process. The sponsors of S. 1691 are advocating for their bill to get included on the agenda of a Senate HSGAC markup on June 13.

Industry stakeholders should weigh in with bill writers and HSGAC staff (Patrick Bailey, chief counsel for governmental affairs; Dan Lips, policy director) so that their views are taken into account.

A number of problematic provisions in S. 1691 have been eliminated, for example, the bill's widespread vulnerability tracking and notification regime. The bill is moving toward an approach to strengthening connected devices that is rooted in voluntary, globally accepted, and industry-led standards—a view that the Chamber is strongly championing to both U.S. and foreign officials. Some of the key changes to the legislation are provided here:

- **Reducing legislated security requirements.** S. 1691, as introduced, would require that vendors' IoT devices (1) are patchable, (2) do not contain known vulnerabilities, (3) use standard protocols, and (4) do not feature hard-coded passcodes. The revised draft cuts the security requirements in half. The bill stipulates that covered devices must be patchable and prohibits the use of fixed credentials for updates.

  Devices may use nonstandard protocols and contain known vulnerabilities—which do not always pose security challenges—at the time of sale to federal executive agencies. However, contractors must utilize a coordinated vulnerability disclosure program for addressing vulnerabilities in devices aligned with specific ISO standards (i.e., 29147 and 30111).

- **Narrowing the definition of covered devices.** The new version replaces "internet-connected devices" with the term "covered devices." It specifically excludes "general-purpose computing devices," including PCs, mobile devices, PLCs, and mainframes.

- **Expediting exemptions.** The latest version of S. 1691 provides for an expedited petition process for "interested parties" (e.g., vendors) to request that devices not covered in the bill be considered outside the scope of "covered devices"—and thus exempt from the bill's requirements.

- **Adapting security requirements to changing threat environments.** Notwithstanding the current legislation's stipulations that covered devices must be patchable and do not contain hard-coded passwords, the bill's language says that OMB should address "aspects of device security" in procurement guidelines.

OMB would be tasked with issuing guidance for each agency to include security clauses in contracts that address identity and access management, security vulnerabilities, coordinated vulnerability disclosure, etc.

In addition, OMB should address device security that is tailored to individual devices, technology neutral, risk based, and aligned with industry standards. OMB is required to ensure that the guidelines are consistent with FISMA and do not conflict with any applicable federal information security policies and practices.

The idea is to move policy away from mandating specific requirements in legislation to ensuring that agencies' acquisition clauses can adapt as technology and security circumstances change. Legislated mandates are unlikely to keep pace with changing threat environments. This approach injects nuance into managing the cyber risk profile of covered devices in ways that legislation could never do.

Leveraging industry-led standards. The latest version directs OMB to ensure that the content of security clauses "reflect and align with existing voluntary consensus standards." OMB must sunset the bill's security requirements if a voluntary consensus standard for a device is available that provides an equivalent or greater level of security. OMB must also modify the security clauses to "reflect conformity with that voluntary consensus standard."

- **Limiting agencies' use of LPTA sourcing.** The updated legislation calls on OMB to issue guidelines for each agency to limit the use of lowest price technically acceptable, or LPTA, criteria in procurements that are "predominately for the acquisition of a covered device." This provision is important to watch because covered devices should increasingly gain market share in the federal space under S. 1691.

- **Maintaining protections afforded to private organizations under the CFAA and the DMCA.** The provisions in S. 1691, as introduced, that would loosen protections afforded to businesses under the CFAA and the DMCA are eliminated in the most recent draft, which is consistent with the Chamber's feedback to bill writers from last fall.

  For more information on the Chamber's critique of this and other provisions in S. 1691, as introduced, see our November 2017 comment piece.