U.S. Chamber of Commerce
Preliminary Feedback on S. 1691, the Internet of Things (IoT) Cybersecurity Improvement Act of 2017[1]
November 13, 2017

Summary: Smart Risk Management Policies and Regulatory Humility Are Fundamental to Sound IoT Security

The U.S. Chamber of Commerce shares policymakers' interest in helping the federal government buy secure internet-connected devices. Securing the IoT must be a top U.S. objective.[2] The Chamber argues that businesses and government need to prioritize certain actions, particularly managing cyber risk and avoiding regulations that would stunt IoT innovation and deployments.

This paper provides an initial critique of S. 1691, the Internet of Things (IoT) Cybersecurity Improvement Act of 2017, which establishes minimum security requirements for government buying connected devices. The legislation stresses that devices shouldn't contain known vulnerabilities. It emphasizes mitigating vulnerabilities through patching and prohibiting the use of hard-coded passwords, among other contractor mandates.

However, the bill warrants scrutiny on a number of issues, including the extraordinary scope of the devices and services that it would cover, the widespread vulnerability tracking and notification regime, and the relaxation of protections afforded to device makers under the Computer Fraud and Abuse Act (CFAA) and the Digital Millennium Copyright Act (DMCA). Many unanswered considerations need to be discussed. If Congress wants to strengthen cybersecurity through extending liability protections, the Chamber urges lawmakers to consider the Cyber SAFETY Act of 2017 (currently a draft).

The Chamber urges Congress to resource a multistakeholder effort on IoT cybersecurity comparable to the joint industry-NIST cybersecurity framework process *before* advancing IoT legislation.

The legislation presupposes devices being hacked illegally, but it does not contemplate putting tough pressure on countries that harbor bad actors. Policymakers should not put new mandates on businesses while leaving cyberattackers frequently untouched.[3]

Industry Shares Policymakers' Goal of Helping Government Buy Secure Devices

The Chamber supports the federal government's efforts to procure secure internet-connected, or IoT, devices. We especially embrace cyber processes built on dynamic nonregulatory risk management principles. The Chamber is optimistic about the future of the IoT, which continues the decades-long trend of connecting networks of objects through the internet. We believe that the expansion of the IoT must progress hand in hand with sound security practices, including upgrading and patching software to mitigate vulnerabilities.

The Chamber said on October 3 before the House Oversight and Government Reform (OGR) IT Subcommittee and on October 19 at NIST that we would advocate for several cyber principles to foster beneficial outcomes of the IoT:

- The IoT is incredibly complex, and there's no silver bullet to cybersecurity.

- Managing cyber risk across the internet and communications ecosystem is central to growing the IoT and increasing businesses' gains.

- The business community will promote policies favorable to the security and competitiveness of the digital ecosystem.

- IoT cybersecurity is best when it's embedded in global and industry-driven standards.

- Public-private collaboration needs to advance industry interests.[4]

The Legislation Needs Constructive Scrutiny

S. 1691 deserves scrutiny through constructive dialogue. Among other things, the legislation establishes new federal mandates for how companies develop their software and devices through the imposition of requirements on government contractors. The Chamber supports robust device security and resilience, but the bill raises several concerns about how agencies—led by the OMB in consultation with the DoD, the Commerce Department, the DHS, and others—would write guidelines and practically implement them.

- **Broad scope of device coverage, unwieldy vulnerability notifications.** The legislation takes a one-size-fits-all approach to addressing federal IoT cybersecurity. It doesn't distinguish among the extraordinary array of devices covered under the bill based on their types and unique risk environments.[5] In other words, S. 1691 would impact every internet-connected item in roughly the same manner (e.g., military mission-critical devices would be treated the same as connected dishwashers purchased by agencies).

  The bill's vulnerability notification regime could easily become unwieldy, and disclosure should not become an end in itself. Even some security researchers who are proponents of vulnerability disclosure programs argue that S. 1691 creates unrealistic expectations for contractors.[6]

- **Prescriptiveness vs. risk management.** The bill is quite prescriptive. It imposes substantial new obligations on entities that sell IoT devices to the government, which could potentially discourage innovative offerings and stifle the market for device-management solutions. The Chamber believes that mandating standards, guidance, and best practices shunts entities' resources away from effective risk-based cybersecurity measures and toward suboptimal tasks, including practices involving devices. The momentum of regulations can easily take on a life of their own, and they are next to impossible to pare back and harmonize.[7]

- **Top-down compliance vs. speed and inventiveness.** A static and cumbersome checklist mentality can lull enterprises (e.g., device contractors and government buyers) into a false sense of security. Adopting a single certification standard—or a set of them—can also jeopardize security because no security solution can mitigate all risk. The terms of S. 1691 are likely to become outmoded quickly. Regulation is little match for the fast-paced commercial demands and risks that companies face online. Top-down approaches to enhancing the security of technology, including codifying rigid definitions, strict contractor requirements, and universal evaluation standards are unworkable. Red tape could readily quash business inventiveness, which lawmakers should not want.

- **Exemptions and intellectual property (IP).** The legislation would unnecessarily relax protections (e.g., IP and trade secrets) afforded to device makers under the Computer Fraud and Abuse Act (CFAA), which prohibits unauthorized access to another's computer, and the Digital Millennium Copyright Act (DMCA).

- **Device security and pricing.** It's not clear if S. 1691 is trying to address a real or perceived lack of secure, connected devices being bought by agencies. Policymakers should explain why agencies lack the ability to buy secure devices that the market provides. Part of the problem is the government's bias toward a "lowest price technically acceptable source selection process" rather than procuring strong devices.[8] Getting federal acquisition processes straightened out ought to precede the passage of legislation.

  During the October 3 House OGR IT Subcommittee hearing on the cybersecurity of the IoT, a lawmaker said that S. 1691 could set a "positive example for the IoT industry at large." The Chamber believes that government needs to set an example of demanding strong devices and paying for them. Hearing witnesses noted that the requirements (e.g., secure updates) could raise the costs of some devices.[9]

Policymakers Need to *First* Support the Commerce Department Convening Stakeholders

S. 1691 tackles important questions that will affect the future of the IoT and how it's secured. The Chamber strongly believes that the Commerce Department is well suited to bring together public and private stakeholders to create a framework to enhance the security and resilience of the IoT. Such a framework would help inform the benefits and drawbacks of setting minimum security standards for IoT devices through the federal procurement process, among other key topics.[10] The Chamber urges Congress to resource a framework-like effort comparable to the joint industry-NIST cybersecurity framework process *before* moving IoT legislation.[11]

Pressure on Bad Actors Should Accompany Policies That Impact Industry

The legislation, which was referred to the Senate Homeland Security and Governmental Affairs Committee, presupposes devices being hacked illegally but does not contemplate bringing pressure on countries that allow bad actors to operate.[12] While attributing attacks to individuals and organizations is a challenge, it is far from impossible.[13] Prominent cyber authorities agree that certain foreign powers or their proxies represent high-end threats against the business community and the U.S.[14]

Goals worth pursing include reducing the number of safe havens from which malicious persons and groups can launch attacks against American interests with impunity. There's no disincentive to attacking U.S. industry from certain countries around the world. Recalcitrant governments too frequently will not help the U.S. government round up illicit hackers and turn them over to the FBI or the Secret Service.[15] Congress and the administration need to collaborate with industry to identify ways to put more pressure on bad actors.

Sec. 2 Definitions

(Pgs. 2–4, sec. 2) S. 1691 does not define "Contractor," which bears the responsibility for selling secure devices to the government. At issue is what party—e.g., vendors or system integrators—has the obligation to mitigate security vulnerabilities, which is a diffuse role today.[16] The Chamber doesn't anticipate that the definition of contractor will be clarified further, but these parties will be saddled with managing a suite of burdens that they may or may not be able to adequately control.

(Pg. 3, lines 3–9, sec. 2(6)) The definition of an "Internet-connected device"—aka an IoT device—is extraordinarily broad. The bill defines an IoT device as "a physical object" that "(A) is *capable of connecting* to and is in *regular connection* with the Internet; and (B) has computer processing capabilities that can collect, send, or receive data" [italics added]. This wide-ranging definition encompasses almost every object that the government could procure, including vehicles, industrial sensors, agricultural equipment, and medical devices, not to mention smartphones, tablets, and laptops. To be sure, bill writers understand the breadth of the device definition and appreciate it will need refining.

In addition, a device that's behind an appropriate security appliance (e.g., a firewall) to protect computer networks and equipment from unwanted traffic should not be considered an "Internet-connected device." The bill recognizes the importance of defense-in-depth methods to secure devices. Secondary objects (e.g., programmable logic controllers, or PLCs) that are connected to covered devices via a security appliance should be excluded from S. 1691's definition of an "Internet-connected device," not just given a potential waiver.

(Pg. 3, line 6, sec. 2(6)) The language "is capable of connecting to [the internet]" is too expansive. Many relatively low-end devices (e.g., PLCs) are capable of connecting to the internet, but customers are explicitly warned against doing so without accompanying technical, support, and training protocols. The Chamber suggests changing the wording "is *capable* of connecting" to "is *intended* by the manufacturer to be connected to the Internet" [italics added]. While agencies may issue a waiver to purchase the device, S. 1691 should not sweep in devices that aren't intended to be connected online in the first case.

(Pg. 3, lines 8–9, sec. 2(6)) The phrase "has computer processing capabilities" is vague. The bill text should say, instead, "includes a processor executing instructions and can send or receive data."

(Pg. 3, lines 18–21, sec. 2(7)) The provision “Properly Authenticated Update” addresses the trustworthiness of updates. The phrase “contains some method of authenticity protection” suggests that a contractor would be required to embed processing capabilities or some other mechanism to verify firmware or software updates. The legislation should also allow for human-mediated protections such as using a trusted hash signature (roughly akin to a digital fingerprint).

Methods to establish the authenticity of patches vary from product to product. Some fixes are signed, while others are checked for integrity prior to an update. Unsigned patches are typically delivered with a hash function so that users can validate the integrity of the patch before installing it. Such capabilities depend on the security level of the device in question. The Chamber suggests removing the “such as a digital signature” requirement, which is too prescriptive technically for writing into law.

(Pg. 3, lines 22–25, sec. 2(9)) The definition of “security vulnerability” is overly expansive. The definition encompasses known vulnerabilities in the device and “any attribute of hardware, firmware, software, process, or procedure or combination of 2 or more of these factors” that could defeat an information system or a device. It is practically impossible for a contractor to anticipate the myriad ways a government customer will use a device, which can trigger and/or reveal the existence of previously unknown vulnerabilities, thus increasing contractors’ notification workload.

(Pg. 4, lines 3–4, sec. 2(9)) The Chamber interprets the language “or physical devices to which it [information system] is connected” as extending the scope of the legislation to devices that are connected to a covered device. Defense-in-depth approaches to security allow for devices with different protection capabilities to be linked within a network but guarded by technologies that are designed to be connected to the internet. S. 1691 should not cover IoT devices that *aren’t* meant to be connected online. Such a fundamental change to the bill would lessen the need for agencies to issue multiple waivers.

Sec. 3 Contractor Responsibilities With Respect to Internet-Connected Device Cybersecurity

(Pg. 5, lines 5–18, sec. 3(a)(1)(A)) The legislation insufficiently explains what “known security vulnerabilities” would capture. While S. 1691 defines a vulnerability as “known” if listed in NIST’s National Vulnerability Database (NVD), the bill would also authorize the selection of another—yet to be selected—database by the OMB. Such language makes “known security vulnerabilities” difficult to interpret with precision.[17]

Contractors strive to weed out most vulnerabilities by using commercially sound practices for delivering robust IoT products to the marketplace. If bill writers use the NVD, the legislation should specify a severity threshold. Setting a severity ranking of “Low” will generate much noise and become an unreasonable burden for contractors to comply with the bill’s certification requirements. Agencies, too, will be encumbered by the need to evaluate a potential flood of incoming vulnerability data that are not useable.

Under S. 1691, contractors would need to police all vulnerabilities in devices that they market to agencies. The list of sources (e.g., customers, distributors, media, researchers, and domestic and international CERTs) that contractors would need to monitor for vulnerabilities is lengthy and runs contrary to prudent risk management practices. Vulnerabilities do not need to be mitigated equally, which the legislation's writers appreciate, but this thinking (aside from waivers) is not sufficiently evident in the bill.

(Pg. 5, line 13, sec. 3(a)(1)(A)(i)(I)(bb)) The bill provides for maintaining a public database (i.e., see "any additional database . . . that tracks security vulnerabilities") of devices procured by agencies. However, the Chamber is concerned that creating a device directory is potentially unwise and could provide a path for nefarious actors to exploit. What's more, a "publicly accessible database" would also list devices whose security support has ended, helping further spotlight targets for malicious hackers.

(Pg. 5, lines 23–25; pg. 6, lines 1–6, sec. 3(a)(1)(A)(i)(III)) Many industrial control systems (ICS) sold today use deprecated industry standard protocols to communicate with older devices, some of which may be decades old. Leveraging such protocols is vital while commercial facilities continue to make the transition from analog to digital technology. If S. 1691 prohibits the use of deprecated protocols, then some ICS would likely be unable to communicate with newer IoT devices. Asset owners/operators would incur the expense to upgrade ICS equipment and the covered devices that they're linked to. Such a requirement could unintentionally slow the adoption of secure digital technologies because of the inefficient expenditure of enterprises' cyber resources.

Some suppliers use proprietary protocols to facilitate communication between devices for certain configurations, improved performance, and increased security. Such protocols are frequently layered atop standard protocols but use nonstandard ports for network traffic. Special protocols can provide a competitive edge for companies and foster innovation. The ability to use any port (there are some 65.5K channels) is an important security option and should be preserved so that traffic can be segregated and made harder for bad actors to exploit.

(Pg. 6, lines 7–10, sec. 3(a)(1)(A)(i)(IV)) Some older, low-end devices contain "any fixed or hard-coded credentials" used in communications, which S. 1691 prohibits. Such credentials are being phased out of the private market through attrition. Nonetheless, the government could have difficulty buying equipment with requirements that the marketplace does not presently demand en masse.

Bill writers should not allow the legislation's broad prohibition against fixed/hard-coded credentials in IoT devices to prevent contractors from employing anti-piracy verification tools. The Chamber wants to flag that prohibiting the use of anti-piracy tools, including as part of businesses' authentication tools, could prevent devices from lawfully accessing copyrighted works or require a special exception for accessing such devices.

This section also requires federal contractors to certify that a device they are providing does not "include any fixed or hard-coded credentials for . . . communication." This is so broad it could conceivably prohibit federal contractors from employing anti-piracy verification tools, whether for software, streaming of copyrighted works, etc. It's uncertain how often such authentication tools as they are employed fit the bill's definition of "fixed or hard-coded," but it seems likely that at least some are. Prohibiting their use would require that devices do not have lawful access to the corresponding copyrighted works, or at least require a special exception for such access controls.

(Pg. 6, lines 11–20, sec. 3(a)(1)(A)(ii)) S. 1691 would seemingly grant limited exceptions (i.e., waivers) to contractors that supply devices to the government with known vulnerabilities. Contractors must explain to the agencies why the device should be considered secure and provide a description of any "mitigating actions" employed to limit the exploitability of the vulnerability.

It's worth noting that many factors go into deciding when and how businesses disclose vulnerabilities in a device, particularly if the weaknesses affect multiple products or are comparatively severe in nature. Software vulnerabilities are often disclosed in cooperation with US-CERT.[18] The existing public-private disclosure system frequently gives stakeholders the opportunity to implement compensating controls until a vulnerability patch is developed and deployed.

However, section 3 of the bill could lessen the likelihood of early voluntary disclosures by contractors. Contractors may be unable to bid on proposals unless waiver applications are granted for devices with known vulnerabilities. Penalizing companies for researching and disclosing vulnerabilities is in no one's interest. The bill could have the unintended consequence of reducing voluntary disclosures, thereby upending a key element of U.S. and international cybersecurity best practices. Sometimes it's in the public interest for a vulnerability to be disclosed before it can be patched, and sometimes it isn't because of reasonable risk management determinations.

Complicating matters further, parts of the U.S. government have a history of weaponizing vulnerabilities for clandestine and covert programs that, while understandable, can significantly dampen industry's willingness to voluntarily disclose vulnerabilities to the government.[19]

(Pg. 7, lines 19–24; pg. 8, lines 1–2, sec. 3(a)(1)(B)) The "Notification Required" clause requires a contractor to disclose to the purchasing agency both vulnerabilities reported by an external researcher and vulnerabilities or defects "which the vendor otherwise becomes aware of for the duration of the contract," which is sweeping. The House OGR IT Subcommittee hearing in October highlighted that it's probable complex cyber systems will have several vulnerabilities over the course of a year.

(Pg. 8, lines 12–13, sec. 3(a)(1)(C)) The phrase "properly authenticated and secure manner" under the "Updates" subsection requires further discussion and clarification. Suppliers update software and firmware in various manners. Some devices can be updated remotely; others need to be taken offline and managed physically. For remote updates, proper authentication and security required depend on the level of trust in the network (e.g., whether it is isolated within a protected facility). The legislation should accommodate differences between comparatively secure and insecure environments.

(Pg. 8, lines 14–22, sec. 3(a)(1)(D)) Under the "Timely Repair" subsection, S. 1691 mandates that contractors "provide a repair or replacement" of devices that cannot be "remediated through an update." Such a requirement could be impractical to implement and expensive for some vendors to meet. Suppliers do not always provide updates for "any new security vulnerability" that is discovered. Depending on the severity of the vulnerability, the age of the product, and the availability of mitigating controls, suppliers may decide not to push an update or require the customer to upgrade both the hardware and software in order to receive an update—activities that can be very disruptive to the availability of entities' networks and information systems.

Steps in the vulnerability mitigation process come with costs to the supplier, and updates are often a part of a service contract. It's unlikely that a supplier will agree to provide updates to clients, including the government, at no cost. The bill needs to recognize that updates are a commercial offering. A remedy could be to add "timely repair at negotiated cost" to the "Updates" and "Timely Repair" subsections of S. 1691.

(Pg. 9, lines 10–12, sec. 3(a)(1)(D)) The statement "any additional information recommended by the National Telecommunications and Information Administration" is opaque. While unlikely, this language could allow for an NTIA rulemaking, which the Chamber would oppose.

(Pg. 10, lines 3+, sec. 3(a)(2)(A)(ii)) Many components that comprise ICS systems would fall under the clause "(ii) Alternate conditions to mitigate cybersecurity risks." ICS devices generally shouldn't be connected to the internet without the appropriate use of cyber defenses. Low-end devices aren't automatically weak links of a network, which this provision suggests, especially if adversaries cannot access these devices because they're guarded behind a security appliance or air-gapped.

(Pg. 11, lines 17–25; pg. 12, lines 1–6, sec. 3(a)(2)(A)(iii)) S. 1691 calls for "additional requirements for management and use of non-compliant devices, including deadlines for the removal, replacement, or disabling of non-compliant devices (or their Internet-connectivity). . . ." Deadlines for the replacement or removal of some devices is cause for concern. It's unclear that ICS devices would be granted an exception from the bill's rigid requirements. The legislation needs greater clarity about how exceptions will accommodate devices that can't necessarily be removed, replaced, or disabled because of sound business and risk management decisions.

(Pg. 12, lines 7–22, sec. 3(a)(2)(B)) It is uncertain if third-party conformance programs are the optimal or only way to "demonstrate compliance with . . . [third-party security] standard[s]," which S. 1691 demands. Third-party certifications can add significant costs and lead times to product development and deployment. Conformance programs can also prove problematic if agencies support them (actively or passively), and if they conflict with or are duplicative of competing security obligations, which is an all too common occurrence.

The requirement that a third party must provide written certification that a device complies with industry standards is unclear. The S. 1691 spurs several issues—including the standards that will be selected and by what agencies, the methods that will be used to demonstrate compliance, and how long certifications will remain in effect—that bill sponsors should address with stakeholders.

(Pg. 12, lines 23–25+, sec. 3(a)(2)(B)(iii)) NIST would need to differentiate among the security requirements based on the type of device to be certified. For instance, internet-facing security appliances (e.g., a firewall) should feature higher security levels compared with devices that are internet capable but designed for use behind the security appliance.

(Pg. 13, lines 8–19, sec. 3(a)(2)(C)) S. 1691 allows agencies to employ "a security evaluation process or criteria for Internet-connected devices that the agency believes provides an equivalent or greater level of security" compared with the agency guidelines that contractors are expected to meet under paragraph (1)(A) (see pg. 4 of the bill). Such an approach, while understandable, could be problematic. Cybersecurity efforts are optimal when they reflect global standards and industry-driven practices. Section 3(a)(2)(C) should be eliminated or reworded to ensure that it's consistent with the U.S. international standards strategy and applicable laws.

Allowing a fragmentation of the cybersecurity standards landscape would create negative outcomes for industry and government. The Chamber strongly supported NIST's *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* (the report). The Chamber also supported the enactment of the Cybersecurity Enhancement Act of 2014 (P.L. 113-274), which called on NIST to produce the strategy paper.[20] Efforts to improve the cybersecurity of the public and private sectors should reflect the borderless and interconnected nature of our digital environment.

Government-directed or centrally coordinated standards, procurement, and regulatory regimes—which are common in other countries—are poor architectures for cybersecurity and would spread companies' security budgets much too thinly to meet the dictates of regional, state, and local magistrates.[21] A witness at the October House OGR IT Subcommittee hearing cautioned that lawmakers could "go too far" by "adopt[ing] indigenous standards [for devices]" that put the U.S. at odds with the rest of the world. Policymakers could "segment" the internet, and we'd lose the ability to transact business efficiently around the world, the witness emphasized.

(Pg. 14–15, sec. 3(b)) Many suppliers have established methodologies to receive information about vulnerabilities and disseminate fixes. Some organizations' processes are publicly available for review on the internet.[22] Many organizations are still developing them, which the Chamber supports as a sound business practice. The NTIA is doing quality work in this space that should be reflected in similar legislation and agencies' implementation activities.[23]

(Pg. 16–18, sec. 3(c)) According to S. 1691, the liability protection provisions "shall [not] be construed to establish additional obligations or criminal penalties for individuals engaged in researching the cybersecurity of Internet-connected devices." However, the apparent relaxation of protections afforded to private organizations under the CFAA and the DMCA are potentially significant and could have negative consequences, especially on IP. Lawmakers should not grant exemptions to researchers—even while acting in "good faith"—if their actions could harm IP safeguards. The good faith requirement does not begin to encompass the precautions necessary for an exemption from criminal liability for hacking into other people's computers.

The legislation would also amend the DMCA to exempt from civil liability and criminal penalties anyone who violates the anti-circumvention provisions of the DMCA for purposes of good faith cybersecurity research. A statutory provision already exists in the DMCA for allowing certain security research.[24] Expanded versions of this provision have been made in triennial rulemakings conducted by the Copyright Office and have been submitted again in the current rulemaking process. These nuanced issues are contentious among multiple stakeholders, and it would be inappropriate for Congress to resolve them in this bill without full vetting.

To be sure, the Chamber urges businesses to collaborate with security researchers on vulnerability disclosure programs, but decisions to waive protections granted under the CFAA and the DMCA should lie with individual companies, not government officials.[25]

If Congress is interested in advancing cybersecurity through limitations on liability, the Chamber urges lawmakers to continue to work on the draft Cyber SAFETY Act of 2017. The Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) provides legal liability protections for providers of qualified anti-terrorism technologies, including products and services. The goal of the SAFETY Act is to encourage the development and deployment of effective anti-terrorism products and services by providing liability protections.[26]

The Cyber SAFETY ACT would amend the 2002 law to cover *qualifying cyber incidents* in addition to acts of terrorism. Indeed, devices covered under S. 1691 should earn expedited, if not automatic, SAFETY Act approval by DHS (which administers the program).

Endnotes

[1] S.1691, the Internet of Things (IoT) Cybersecurity Improvement Act of 2017, introduced August 1, 2017.
(Legislation) www.congress.gov/bill/115th-congress/senate-bill/1691
(Fact sheet) www.warner.senate.gov/public/_cache/files/8/6/861d66b8-93bf-4c93-84d0-6bea67235047/8061BCEEBF4300EC702B4E894247D0E0.iot-cybesecurity-improvement-act---fact-sheet.pdf
(Press release) www.warner.senate.gov/public/index.cfm/2017/8/enators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices

[2] https://oversight.house.gov/wp-content/uploads/2017/10/Ross_Testimony_IOT_10032017.pdf

[3] Clearly, organizations such as the Department of Justice/FBI and the Secret Service are doing yeoman work, but few federal agencies are doing much to deter malignant actors. The table, taken from a 2016 Chamber letter to the Cybersecurity Forum for Independent and Executive Branch Regulators, is meant to illustrate the numeric mismatch between government entities, including members of the cyber forum, that are empowered to regulate the business community and government entities that are tasked with investigating and prosecuting cybercrimes. We need more private sector and government capacity beyond the FBI and the Secret Service—which are just 2 federal entities out of 15 executive branch departments and dozens of independent agencies—pushing back on malicious actors. (See *The United States Government Manual, 2015*.)
www.uschamber.com/sites/default/files/u_s_chamber_letter_to_cyber_forum_july_8_final_2.pdf
www.nrc.gov/docs/ML1501/ML15014A296.pdf
www.archives.gov/federal-register/publications/government-manual.html

(Go to next page.)

Cybersecurity Forum for Independent and Executive Branch Regulators	
Members	Law enforcement role comparable to the FBI and the Secret Service? (Y/N)
Nuclear Regulatory Commission (NRC), chair	N
Federal Communications Commission (FCC)	N
Federal Energy Regulatory Commission (FERC)	N
Securities and Exchange Commission (SEC)	N
Federal Trade Commission (FTC)	N
Federal Reserve Board (Fed)	N
Federal Financial Institutions Examination Council (FFIEC)	N
Financial and Banking Information Infrastructure Committee (FBIIC)	N
National Association of Insurance Commissioners (NAIC)	N
Other agencies or departments may participate as appropriate	TBD
National Institute of Standards and Technology (NIST), a nonregulatory body, serves as an adviser to the Cyber Forum	NA

[4] https://oversight.house.gov/hearing/cybersecurity-internet-things, www.nist.gov/news-events/events/2017/10/iot-cybersecurity-colloquium

[5] A single health care organization can procure thousands of medical devices. The federal government would seemingly acquire and manage thousands, if not millions, of covered devices under S. 1691.

[6] Congressional Internet Caucus Advisory Committee event, "Hacking: What Color Is Your Hat? Vulnerability Disclosures and the Law," October 13, 2017.

[7] www.hsgac.senate.gov/hearings/cybersecurity-regulation-harmonization, www.uschamber.com/sites/default/files/10-11-17_chamber_comments_uscg_nvic_cyber_guidance_final.pdf

[8] www.acquisition.gov/far/html/Subpart%2015_1.html

[9] "House Oversight and Government Reform Subcommittee on Information Technology Holds Hearing on Internet of Things Cybersecurity," *CQ Congressional Transcripts*, October 3, 2017. http://plus.cq.com/doc/congressionaltranscripts-5191654?0

[10] "House lawmakers draft IoT security procurement bill, gather feedback from industry," October 4, 2017, Inside Cybersecurity. https://insidecybersecurity.com/share/7232

[11] www.nist.gov/blogs/taking-measure/framework-protecting-our-critical-infrastructure?utm_source=govdelivery&utm_medium=email&utm_campaign=ncsam2017-nov-1&utm_content=tm-frame

[12] S. 1691 was referred to the Senate Homeland Security and Governmental Affairs, which could take up issues tied to the U.S. pushing back on threat actors.

[13] www.lawfareblog.com/attribution-malicious-cyber-incidents-soup-nuts

[14] www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf

[15] www.uschamber.com/sites/default/files/u.s._chamber_letter_nist-wh_cyber_commission_rfi_sept._9_final_v2.1.pdf

[16] The Chamber, which has members operating throughout the entire IoT landscape, urges stakeholders to mitigate risks in this technological environment so that hazards to businesses' cybersecurity do not pool at any given point. Unmitigated risk and threats could create perils not only for companies and sectors but also for the IoT at large.

Software Update as a Mechanism for Resilience and Security: Proceedings of a Workshop (2017), The National Academies Press. https://doi.org/10.17226/24833

[17] https://nvd.nist.gov/vuln-metrics/cvss#

[18] www.us-cert.gov

[19] See, for example, Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown, 2014).

See, too, the Chamber's comments on the draft Protecting Our Ability to Counter Hacking Act (PATCH Act). www.uschamber.com/sites/default/files/revised_preliminary_feedback_patch_act_bag17354_final_may_15.pdf

[20] www.uschamber.com/sites/default/files/september_24_2017_chamber_comments_draft_nistir_8074_intl_cyber_standardization_final.pdf

[21] See, for example, IEC-62443 (formerly ISA-99), which provides a series of standards, technical reports, and related information that define procedures for implementing electronically secure industrial automation and control systems. This guidance applies to end users (e.g., an asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems. https://en.wikipedia.org/wiki/Cyber_security_standards

[22] See, for example, the Siemens vulnerability handling process. www.siemens.com/id/en/home/products/services/cert/vulu.html

[23] At the time of this writing, the NTIA will convene a virtual meeting of a multistakeholder process on IoT security upgradability and patching on November 8, 2017. www.ntia.doc.gov/notice-11082017-iot-multistakeholder-meeting

[24] www.ftc.gov/news-events/blogs/techftc/2016/10/dmca-security-research-exemption-consumer-devices

[25] See, for example, the Department of Justice's *A Framework for a Vulnerability Disclosure Program for Online Systems*, July 2017. www.justice.gov/criminal-ccips/page/file/983996/download

[26] www.safetyact.gov