Cybersecurity Working Group (CWG)
Library | 1615 H Street, N.W.
Tuesday, March 12, 2019
10:00 a.m.–noon

AGENDA

10:00 a.m.–10:05 a.m. — **Welcome and Introductions**
Matthew Eggers, Vice President, Cybersecurity Policy, U.S. Chamber of Commerce

10:05 a.m.–11:00 a.m. — **Recent CWG Activities, Notable Developments, and Member "Homework" (in red text)**

- **IoT**
  - Feedback is requested from CWG members by **Monday, March 18** on the NIST discussion draft, *Considerations for a Core IoT Cybersecurity Capabilities Baseline*, which was covered at the Chamber on February 28 with NIST principals. The Chamber intends to support the baseline, while noting that the suite of considerations should likely be narrowed.
  - The Chamber is considering the creation of a Buy Strong IoT Coalition (#BuyStrongIoT)[1] to spur the purchase and deployment of more secure IoT products across the U.S. and globally while leveraging the IoT cyber baseline developed by NIST and the private sector.
- **Supply Chain**
  - At the time of this writing, it is unclear when or if the administration plans to issue an executive order (EO) targeting Chinese tech firms such as Huawei, which has been extensively reported on.[2] This EO is of significant interest to many in industry.
  - Other cyber supply chain events or topics of interest (e.g., the ICT Supply Chain Risk Management Task Force).
- **Legislation/Regulation**
  - Last September, the Chamber released its privacy principles to benefit consumers and provide businesses with policy certainty. We'll discuss expected next steps concerning data security and breach notification legislation, which was not included in the Chamber's model privacy bill that was released on February 13.

Data Security and Breach Notification
As part of a national privacy framework, Congress should include risk-based data security and breach notification provisions that protect sensitive personal information pertaining to individuals. Keeping this information secure is a top industry priority. Security is different for individual businesses and one-size-fits-all approaches are not effective; therefore, companies should have flexibility in determining reasonable security practices. Preemptive federal data security and breach notification requirements would provide consumers with consistent protections and would also reduce the complexity and costs associated with the compliance and enforcement issues resulting from different laws in the 50 states and U.S. territories.
[Excerpt from the Chamber's September 6, 2018, privacy principles.]

- Cyber SAFETY Act (SA) materials from the 115th Congress were distributed on March 1 to Cyber SA Coalition members. Please send us your feedback/edits on these items by **Tuesday, March 19**. The Chamber supports the reintroduction of this bill (amended) in the 116th Congress.

- The Chamber has been meeting with Capitol Hill staff regarding DoD's plans to implement sections 1654–1655 of the FY19 NDAA. Staff members, including ones on the Senate Armed Services Committee (SASC), are uncertain about DoD's intentions but are apparently reaching out to department officials to learn more.

- Sens. Mark Warner (D-VA) and Cory Gardner (D-CO) are expected to reintroduce their federal IoT cyber procurement bill, the Internet of Things Cybersecurity Improvement Act of 2019 (or the IoT Cybersecurity Improvement Act of 2019), which was S. 1691 in the last Congress. The Chamber is "neutral" on this legislation, which has been discussed at recent IoT Cyber Subgroup meetings.

  The IoT Cyber Subgroup is considering a proposal that would blend NIST's IoT cyber baseline with sec. 101 (Public-private collaboration on cybersecurity) of the Cybersecurity Enhancement Act of 2014 (P.L. 113–274). The Chamber indicated its intentions to NIST officials on February 28.

- Sen. Jack Reed (D-RI) et al. introduced S. 592, the Cybersecurity Disclosure Act of 2019, on February 28. Rep. Jim Himes (D-CT) is expected to introduce companion legislation in the House. The Chamber opposes this legislation, which was first introduced in 2015.

- Reps. Jim Langevin (D-RI) and Glenn "GT" Thompson (R-PA), co-chairs of the Congressional Career and Technical Education (CTE) Caucus, introduced H.R. 1592, the Cybersecurity Skills Integration Act, on March 7.

11:00 a.m.–noon — **Recap of March 5 P3/Operational Collaboration Subgroup Meeting on Deepening Business/Government Operational Collaboration Against Foreign Cyber Threats: Identifying 1–3 Objectives[3]**

- **Two topics were principally addressed on March 5:**

  - Discussing security clearance reform with Colleen Berny, a professional staff member on the Senate Homeland Security and Governmental Affairs Committee (HSGAC).

  - Identifying 1–3 objectives regarding deepening business and government operational collaboration against foreign cyber threats.

- **Top 3 takeaways from the meeting were:**

  - **Improving security clearance reciprocity.** HSGAC's Berny, who handles critical infrastructure issues at the committee, **requested input from Chamber members as soon as possible** on improving agency-to-agency reciprocity concerning professionals' security clearances (e.g., getting DoD to recognize a DHS security clearance). The committee's interest includes people who retire from the federal government but want to keep their clearances active as private-sector employees. Chamber members said that they would take this ask back to their organizations.

    Berny will join the CWG by phone on March 27 at 3:00 p.m. Still, members should feel free to contact her directly at Colleen_Berny@hsgac.senate.gov.

    Separately, the broader security clearance backlog issue is being handled by the governmental affairs side of HSGAC (Patrick Bailey, chief counsel, and Courtney Allen, deputy chief counsel—both of whom are with the majority).

  - **Making private entities intelligence *customers*.** Chamber members said that the federal government needs to collect and share classified cyber threat data with businesses that are critical to the economy. To be sure, there is substantial sharing of cybersecurity threat information between agencies and industry. However, there is a strong consensus that we need to do much better, particularly against the persistent, malicious activity initiated by nation states or their surrogates and criminal groups.

    Chamber members emphasized that some private entities need to be voluntarily identified as customers of the *intelligence community (IC)*. High-level discussions have been ongoing for years, but concrete results are difficult to pinpoint.

    The Chamber is engaging Capitol Hill, including authorizing and appropriations committees and the administration on how our organization can help the intelligence community deliver actionable threat information to business actors in a timely way. Such an outcome should be viewed as a win-win for the public- and private-sectors. The Chamber has downplayed a legislative fix over the last few years, but the lack of tangible outcomes benefiting industry suggests that legislation is necessary.[4]

- Note: By April 1, the Chamber anticipates submitting a request to the House and Senate Appropriations Committees (Defense Subcommittees) to specifically fund classified IC cyber information sharing and analyst engagement with critical infrastructure entities that voluntarily participate in such arrangements. A one pager will be circulated soon to the CWG.

- **Determining thresholds for government intervention against cyberattacks.** On February 14, Grant Schneider, federal chief information security officer and special assistant to the president for cybersecurity, addressed the Chamber's Cyber Leadership Council. Among other things, he said that the White House *National Cyber Strategy* (pg. 8) calls for refining the roles and responsibilities of federal agencies and the expectations of the private sector related to cyber risk management and incident response, which tracks with the Chamber's 2019 cyber priorities.

  Schneider noted that he would welcome discussing the so-called threshold issue—that is, seeking public-private agreement on when the federal government would likely intervene against foreign cyber attackers on behalf of private entities. (See the 2016 Cyber Incident Severity Schema.) Chamber members expressed support for discussing this issue with the White House and other stakeholders.

Cyber Incident Severity Schema (*National Cyber Incident Response Plan*, December 2016)

	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

	Observed Actions	Intended Consequence[1]
↑	Effect	Cause physical consequence
		Damage computer and networking hardware
	Presence	Corrupt or destroy data
		Deny availability to a key system or service
	Engagement	Steal sensitive information
		Commit a financial crime
	Preparation	Nuisance DoS or defacement

Endnotes

---

[1] Buy Strong IoT Coalition (#BuyStrongIoT) is a working title; it could change.

[2] See, for example, "Trump expected to issue new order laying groundwork to bar Chinese tech firms from U.S. networks," *The Washington Post*, February 12, 2019.

Senate Commerce Subcommittee on Security hearing, *China: Challenges for U.S. Commerce*, Thursday, March 7, 2019.

Even NPR's Wait Wait … Don't Tell Me! mentioned Huawei on a recent show, March 9, 2019.

[3] Optional readings: Aspen Institute, *An Operational Collaboration Framework for Cybersecurity* (November 2018); Carnegie Endowment for International Peace, *Protecting Financial Institutions Against Cyber Threats: A National Security Issue* (September 2018); and the Council on Foreign Relations, *Sharing Classified Cyber Threat Information With the Private Sector* (May 2018).

[4] See section 310 of S. 3017, the Intelligence Authorization Act for Fiscal Year 2017, which called on "the Director of National Intelligence and the Secretary of Homeland Security to establish a program to provide assistance and support to certain critical infrastructure entities, on a voluntary basis, for the purpose of reducing the likelihood of catastrophic harm resulting from a cyber attack." Senate Intelligence Committee report (S. Rept. 114-277, June 15, 2016, pg. 4) accompanying S. 3017.

Businesses Should Prioritize Cyber Risk Management—But Not Through SEC Mandates
The Cybersecurity Disclosure Act of 2017 Isn't a Workable Approach to Cybersecurity
October 2017

The Chamber has been leading on cybersecurity for years. In 2014, it launched a campaign under the banner *Improving Today. Protecting Tomorrow* to advance sound policies and educate businesses about cyber risks and how to mitigate them. In 2017, this public-private campaign initiative included five regional events and its 6th Annual Cybersecurity Summit at the Chamber on October 4.

The Chamber does not take a back seat to any organization in promoting sound cyber risk management practices domestically and overseas. Despite a spate of high-profile cyberattacks on public and private entities, the Chamber has seen a surge of business and government investments and innovations in the field of cybersecurity. Policy developments used to be driven almost exclusively by government, but today companies are valuable partners in the quest to protect U.S. networks and information systems.

The Chamber welcomes constructive discussions with Congress on ways to help strengthen the cybersecurity of the business community and increase pushback on malicious hackers. It urges private entities, including publicly traded companies, to proactively prioritize cyber risk management activities. However, the Chamber opposes S. 536, the Cybersecurity Disclosure Act of 2017, because it will not foster a positive approach to cybersecurity.

- **Companies disclose material information.** The Chamber recognizes the importance of SEC Chairman Jay Clayton's statement, "Public companies have a clear obligation to disclose material information about cyber risks and cyber events."[1] Companies already take seriously their requirement to disclose material information about risks and events in a timely and accurate manner.[2] Corporate leaders increasingly view their enterprises' information security as a leadership issue and market differentiator.

- **So-called board experts should not proliferate via government directives.** From a broad industry standpoint, the SEC should not be given the power to dictate which experts sit on companies' governing bodies, which S. 536 grants the agency. Today it's cyber, but tomorrow it's another politically hot topic. The number of experts on boards could quickly grow unwieldly.

- **Cyber talent is scare globally.** From a personnel standpoint, it's unclear where companies will get the required cyber expertise that the bill demands. There is a well-known scarcity of cyber talent for the public and private sectors.[3] What's more, neither the National Institute of Standards and Technology nor any other organization can define what constitutes "expertise or experience in cybersecurity" that will earn widespread agreement among cyber professionals.

- **Malicious actors shouldn't get a free pass.** The legislation lacks an appreciation of fairness. Policymakers need to strengthen public-private cooperation to beat back cyberattacks in concerted ways, not blame the victims of cyber incidents vi-a-vis the

promotion of "transparency." The Chamber believes that the call for transparency should not be limited to boards and cyber experts. Policymakers must also assess how successfully the United States is imposing consequences on malicious actors to deter cyberattacks. Such initiatives are sorely inadequate, despite the solid efforts of law enforcement.

The Chamber has a shared interest with policymakers in urging companies' governing bodies to prioritize cyber throughout their organizations and with their business partners, but S. 536 is not a workable way to facilitate this goal.

Endnotes

---

[1] SEC Chairman Jay Clayton, "SEC Remarks at the Economic Club of New York," July 12, 2017. www.sec.gov/news/speech/remarks-economic-club-new-york

U.S. Chamber of Commerce's Center for Capital Markets Competitiveness, *Essential Information: Modernizing Our Corporate Disclosure System*, winter 2017. www.centerforcapitalmarkets.com/wp-content/uploads/2013/08/U.S.-Chamber-Essential-Information_Materiality-Report-W_FINAL-1.pdf?x48633

[2] For example, see PWC's *Global State of Information Security Survey 2016*, c. October 2015. PwC found that approximately 91% of companies that it surveyed in 2015 adopted a risk-based information security framework, such as the NIST Cybersecurity Framework or the ISO 27011 guidelines. www.cyberriskinsuranceforum.com/content/pwc-global-state-information-security-survey-2016-report www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/takeaways-from-the-2016-pwc-global-state-of-information-security-survey

[3] For example, see (ISC)[2] blog, "Cybersecurity Workforce Shortage Projected at 1.8 Million by 2022," February 15, 2017. By one estimate, the cyber workforce gap is estimated to be growing, with the projected shortage reaching 1.8 million professionals by 2022. http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html

House Homeland Security Committee Cybersecurity and Infrastructure Protection Subcommittee hearing, "Challenges of Recruiting and Retaining a Cybersecurity Workforce," September 7, 2017. https://homeland.house.gov/hearing/challenges-recruiting-retaining-cybersecurity-workforce

Title: To leverage Federal Government procurement power to drive industry standards for Internet of Things device security, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Internet of Things Cybersecurity Improvement Act of 2019" or the "IoT Cybersecurity Improvement Act of 2019".

SEC. 2. DEFINITIONS.

In this Act:

(1) AGENCY.—The term "agency" has the meaning given such term in section 3502 of title 44, United States Code.

(2) COVERED DEVICE.—

(A) IN GENERAL.—The term "covered device"—

(i) means a physical object that—

(I) is capable of connecting to and is in regular connection with the Internet; and

(II) has computer processing capabilities that can collect, send, or receive data; and

(ii) does not include general-purpose computing devices, including personal computing systems, smart mobile communications devices, programmable logic controls, and mainframe computing systems.

(B) MODIFICATION OF DEFINITION.—The Director of the Office of Management and Budget shall establish a process by which—

(i) interested parties may petition for a device that is not described in subparagraph (A)(ii) to be considered a device that is not a covered device; and

(ii) the Director acts upon any petition submitted under clause (i) in a timely manner.

(3) SECURITY VULNERABILITY.—The term "security vulnerability" means any attribute of hardware, firmware, software, process, or procedure or combination of 2 or more of these factors that could enable or facilitate the defeat or compromise of the confidentiality, integrity, or availability of an information system or its information or physical devices to which it is connected.

SEC. 3. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CONSIDERATIONS AND RECOMMENDATIONS REGARDING MANAGING

INTERNET OF THINGS CYBERSECURITY RISKS.

(a) Completion of Ongoing Efforts Relating to Considerations for Managing Internet of Things Cybersecurity Risks.—

(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall ensure that the efforts of the Institute in effect on the date of the enactment of this Act regarding considerations for managing Internet of Things cybersecurity risks, especially regarding examples of possible cybersecurity capabilities of Internet of Things devices, are completed no later than September 30, 2019.

(2) MATTERS ADDRESSED.—In ensuring efforts are completed under paragraph (1), the Director shall also ensure that such efforts address, at a minimum, the following considerations for Internet of Things devices:

(A) Secure development.

(B) Identify management.

(C) Patching.

(D) Configuration management.

(b) Development of Recommended Standards for Use of Internet of Things Devices by Federal Government.—

(1) IN GENERAL.—Not later than March 31, 2020, the Director of the Institute shall develop recommendations for the Federal Government on the appropriate use and management by the Federal Government of Internet of Things devices owned or controlled by the Federal Government, including minimum information and security requirements for managing cybersecurity risks associated with such devices.

(2) CONSISTENCY WITH ONGOING EFFORTS.—The Director of the Institute shall ensure that the recommendations and standards developed under paragraph (1) are consistent with the efforts referred to in subsection (a), especially with respect to the examples of possible cybersecurity capabilities referred to in such subsection.

SEC. 4. POLICIES FOR FEDERAL AGENCIES ON USE AND MANAGEMENT OF INTERNET OF THINGS DEVICES.

(a) In General.—Not later than 180 days after the date on which the Director of the National Institute of Standards and Technology completes the development of the recommendations required under section 3(b), the Director of the Office of Management and Budget shall issue policies for each agency that are consistent with such recommendations.

(b) Quinquennial Reviews and Revisions.—Not less frequently than once every 5 years—

(1) the Director of the Office of Management and Budget and the Director of the National Institute of Standards and Technology shall review the policies issued under subsection (a); and

(2) the Director of the Office of Management and Budget shall, in consultation with the

Director of the National Institute of Standards and Technology, revise such policies.

SEC. 5. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY GUIDANCE ON COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO INTERNET OF THINGS DEVICES.

(a) In General.—Not later than 180 days after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology shall, in consultation with such cybersecurity researchers and private-sector industry experts as the Director considers appropriate, publish guidance on policies and procedures for the reporting, coordinating, publishing, and receiving of information about—

(1) a security vulnerability relating to a covered device used by the Federal Government; and

(2) the resolution of such security vulnerability.

(b) Elements.—The guidance published under subsection (a) shall include the following:

(1) Policies and procedures described in subsection (a) that, to the maximum extent practicable, are aligned with Standards 29147 and 30111 of the International Standards Organization, or any successor standards. Such policies and procedures shall include policies and procedures for a contractor or vendor providing a covered device to the Federal Government on—

(A) receiving information about a potential security vulnerability relating to the covered device; and

(B) disseminating information about the resolution of a security vulnerability relating to the covered device.

(2) Guidance, including example content, on the information items that should be produced through the implementation of the security vulnerability disclosure process of the contractor.

SEC. 6. GUIDELINES FOR FEDERAL AGENCIES ON COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO INTERNET OF THINGS DEVICES.

(a) Agency Guidelines Required.—Not later than 180 days after the date on which the guidance required under section 4 is published, the Director of the Office of Management and Budget shall, in consultation with the Administrator of the General Services Administration, issue guidelines for each agency on reporting, coordinating, publishing, and receiving information about—

(1) a security vulnerability relating to a covered device used by the agency; and

(2) the resolution of such security vulnerability.

(b) Contractor and Vendor Compliance With NIST Guidance.—The guidelines required by subsection (a) shall include a limitation that prohibits an agency from acquiring or using any covered device from a contractor or vendor if the contractor or vendor fails to comply with the guidance published under section 5(a).

(c) Consistency With Guidance From National Institute of Standards and Technology.—The Director shall ensure that the guidelines issued under subsection (a) are consistent with the guidance published under section 5(a).

Preliminary Feedback on Sen. Collins' Critical Cyber Infrastructure Measures
May 13, 2016

The U.S. Chamber of Commerce appreciates the opportunity to consider the critical cyber infrastructure measures that Sen. Collins is circulating. We have had positive conversations with her staff member Ryan Kaldahl, who is writing the legislation.

The Chamber is reviewing the two draft cybersecurity measures. The first item—**Intelligence Community Assistance for Critical Infrastructure (assistance), version EAS16489**—focuses on intelligence community (IC) support and assistance to critical cyber infrastructure to prevent major cyberattacks.[1] The second measure—**Assessment and Report on Efforts to Improve Protection of Critical Cyber Infrastructure (assessment), version EAS16398**—emphasizes assessing attempted or significant intrusions of critical infrastructure assets and reporting them to policymakers.

What is most important, the Chamber does not seek legislation at the moment but, rather, a constructive dialogue with the IC, Sen. Collins and her staff, and the Senate Intelligence Committee. Our organization wants to discuss industry and government perspectives concerning the cybersecurity of critical infrastructure, including exploring our mutual interests in detecting, preventing, and mitigating malicious cyber threats (e.g., nation-states, terrorists, and criminal organizations) to American businesses.

At the time of this writing, the Senate Intelligence Committee is expected to mark up in about two weeks its annual Intelligence Authorization Act (IAA). The Chamber's Cybersecurity Working Group is analyzing the two measures. The Chamber wants to continue a dialogue with Sen. Collins and her staff as we tap our members' thinking on the legislation. Our organization is working to offer constructive revisions to the draft legislation, especially regarding the assistance piece.

Given the truncated time that stakeholders have to work on the draft legislation before markup, and given the unknown implications of the legislation, the Chamber will be unable to support adding either measure to the IAA at this time. Our organization thinks that win-win policy solutions are possible, but we may not be able to achieve agreement with lawmakers in time for committee action.

With regard to the assessment measure, the Chamber strongly believes that the anecdotal and quantitative data collected under the bill would ultimately be made public and possibly politicized, running the risk that the data could be used against private organizations. To be sure, Chamber members share the goal of mitigating cybersecurity risks and are committing billions of dollars to the security and resilience of their enterprises. However, the Chamber does not want to see cyber threat data used to the detriment of businesses, whether the issues concern liability, regulation, public disclosure, and/or antitrust matters.

The Chamber understands that Sen. Collins has invited the IC to discuss her cybersecurity measures, including the challenges that they are intended to address. We strongly welcome the engagement.

[1] The three versions of the assistance legislation are EAS16370 (4/25), EAS16462 (5/5), and EAS16489 (5/11), respectively.