STEVE CHABOT, OHIO
CHAIRMAN

NYDIA M. VELAZQUEZ, NEW YORK
RANKING MEMBER

Congress of the United States

U.S. House of Representatives

Committee on Small Business

2361 Rayburn House Office Building
Washington, DC 20515-0315

Memorandum

To: Members, Committee on Small Business
From: Committee Staff
Date: January 29, 2018
Re: Hearing: "Small Business Information Sharing: Combating Foreign Cyber Threats"

On Tuesday, January 30, 2018 at 11:00 a.m. in Room 2360 of the Rayburn House Office Building, the Committee on Small Business will hold a hearing to discuss H.R. 4668, the Small Business Advanced Cybersecurity Enhancements Act of 2017, and examine how federal agencies are facilitating greater information sharing with small businesses that are vulnerable to foreign-backed cyber attacks.

I. Background

As small businesses increasingly rely on foreign technology products and services, they become even more susceptible to cyber attacks. Many small business owners are underequipped to protect themselves from basic cyber attacks and face significant hurdles in guarding against sophisticated foreign state-backed cyber actors. As the Committee has learned in past hearings, some foreign-backed firms have taken steps to expose small businesses' information technology systems as a means of infiltrating America's critical infrastructure and weakening our national security. A key component in combating these cybersecurity vulnerabilities is strengthening the federal government's engagement with the private sector.

Cyber attacks are a major threat to both the United States' national security and economy. American policymakers and federal agencies are aware that a cyber attack on a small business can be detrimental, not only to the business, but to its customers, employees, and business partners.[1] The Committee on Small Business has learned that cyber attacks on small businesses are carried out by a wide array of cyber bad actors and the scope and capabilities of cyber attackers can vary immensely; they are typically carried out by "individual hackers with purely malicious intent, or criminal groups intending to use information networks for profit seeking."[2] However, foreign governments – through subversive tactics – can also employ state-backed firms to orchestrate cyber attacks, cyber espionage, and other national strategic objectives,

---

[1] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, SMALL BUSINESS INFORMATION SECURITY: THE FUNDAMENTALS, http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf. (last visited Jul. 24, 2017).
[2] Richard Krugler, *Deterrence of Cyber Attacks* 5, *in* CYBERPOWER AND NATIONAL SECURITY (Franklin D. Kramer et al., eds., 2009), *available at* http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-13.pdf.

making it difficult to identify the responsible entity.[3] Additionally, the Small Business Committee has learned through congressional hearings that some foreign-backed firms[4] have reassessed their strategies to expose weaknesses in the United States' information technology infrastructure. Small businesses are at additional risk to these cyber threats because they generally have less capital to purchase security hardware and software, fewer staff members to monitor their systems, and less time to develop cybersecurity defense strategies.

As a global leader in producing intellectual property, America's private and public institutions will continue to be primary targets for cyber criminals. The Internet Crime Complaint Center within the United States Department of Justice recorded 298,728 cybersecurity-related complaints in its 2016 report.[5] There have been steady increases year over year since the year 2000 (3,762,348 total reported complaints).[6] Some of the key targets include the nation's critical infrastructure,[7] federal and state governments, and private businesses. According to a 2012 report by Verizon Enterprise, 71 percent of cyber attacks occurred in businesses with fewer than 100 employees.[8]

In recent years, federal agencies have begun offering resources directly to small businesses to ensure they have the necessary tools to develop stronger information security[9] and cybersecurity systems. Furthermore, threats to information technology infrastructure and Americans' information security have spurred interest among policymakers to investigate looming threats and develop methods to better protect small businesses from cyber attacks.

II. Cybersecurity Information Sharing

As the federal government and private sector work to take steps to strengthen small business cybersecurity, the lack of information sharing between federal and private partners poses a major hurdle to effectively combating cyber attacks.

---

[3] As the U.S.-China Commission has highlighted, circumstantial evidence suggests that cyber incidents are state sponsored because the actors typically target key defense and foreign-policy sources, which are more useful to state and not commercial operations. U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, 2015 ANNUAL REPORT TO CONGRESS 192 (2015), *available at* http://www.uscc.gov/Annual_Reports/2015-annual-report-congress.

[4] *Id*.

[5] INTERNET CRIME COMPLAINT CENTER, 2016 INTERNET CRIME REPORT 14 (2016), *available at* https://pdf.ic3.gov/2016_IC3Report.pdf.

[6] *Id*.

[7] The term "critical infrastructure" is defined as "those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private." Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators, 63 Fed. Reg. 41,804 (Aug. 5, 1998).

[8] VERIZON, 2012 DATA BREACH INVESTIGATIONS REPORT 9 (2012), *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

[9] Information Security is defined as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." 44 U.S.C. §§ 3552(b)(3) (2014).

On February 12, 2013, President Obama issued an Executive Order aimed at improving the critical infrastructure's security against possible cyber attacks.[10] The order established the Department of Homeland Security (DHS) as having a lead role in cybersecurity[11] and encouraged the federal government to increase its information sharing with private-sector entities.[12] The order also directed the National Institute of Standards and Technology (NIST) to develop a framework to reduce cyber risks to the critical infrastructure.[13] The framework incorporates input from government and private industry to identify specific parameters that would support and simplify processes for "addressing and managing cybersecurity risks in a cost-effective way based on business needs without placing additional regulatory requirements on businesses."[14] The framework also enables businesses to implement a set of best practices for assessing cyber threats and reinforcing cybersecurity efforts regardless of their size or sophistication[15] which leads to simplification of information sharing processes.

In 2009, DHS established the National Cybersecurity and Communications Integration Center (NCCIC) to serve as an integral component of the cybersecurity information sharing infrastructure for public and private sectors.[16] The NCCIC operates as a round the clock operations center for situational awareness, incident response and management of coordination of the federal government's cyber and communications activities.[17] DHS states that "the NCCIC shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations."[18] Furthermore, private sector entities can link to the NCCIC for information products, feeds, and services at no cost.[19] Additionally, DHS works to facilitate greater information sharing through its Cyber Information Sharing and Collaboration Program (CISCP),[20] a program that "provides a platform and a trusted forum for exchanging threat and vulnerability information, governed by a Cooperative Research and Development Agreement[21] between DHS and each CISCP participant.[22]

DHS's National Protection and Programs Directorate (NPPD) is also working with Chief Information Security Officers, Chief Security Officers, and insurers to explore the potential development of a cyber incident data repository that could assist in the identification of emerging

---

[10] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).
[11] *Id.* at § 4, 78 Fed. Reg. at 11,739.
[12] *Id.* at § 4(e), 78 Fed. Reg. at 11,740.
[13] *Id.* at § 7, 78 Fed. Reg. at 11,740-41.
[14] *Id.*
[15] NAT'L INST. OF STD. AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, *available at* https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
[16] GOVERNMENT ACCOUNTABILITY OFFICE (GAO), CYBERSECURITY, DHS'S NATIONAL INTEGRATION CENTER GENERALLY PERFORMS REQUIRED FUNCTIONS BUT NEEDS TO EVALUATE ITS ACTIVITIES MORE COMPLETELY 2 (2017) (GAO-17-163), [hereinafter "GAO Cyber"] *available at* http://www.gao.gov/assets/690/682435.pdf.
[17] DEPT. OF HOMELAND SEC., *National Cybersecurity and Communications Integration Center*, https://www.dhs.gov/national-cybersecurity-and-communications-integration-center (last visited Nov. 13, 2017).
[18] *Id.*
[19] *Id,*
[20] GAO Cyber, *supra* note 25, at 12.
[21] The Cooperative Research and Development Agreement allows participants to gain as-needed access to NCCIC, a mechanism to receive security clearances, and the ability to participate in bi-directional information sharing.
[22] GAO Cyber, *supra* note 25, at 12.

cybersecurity best practices across sectors and help stakeholders offer cybersecurity insurance policies that would incentivize businesses for adopting those best practices."[23]

In March 2016, the NPPD sought input from various stakeholders on the cybersecurity insurance market's potential to encourage businesses to improve their cybersecurity in return for more coverage at more affordable rates by seeking comments on three white papers prepared by NPPD staff.[24] The NPPD's white papers address the critical need for information sharing as a means to create a more robust cybersecurity insurance marketplace and improve enterprise cyber hygiene practices across the public and private sectors.[25]

In May 2017, President Trump signed an Executive Order[26] which directs the federal government to responsibly secure its IT and data and states that agencies must manage their cybersecurity risk according to NIST's Framework for Improving Critical Infrastructure Cybersecurity.[27] A recent article from Business Insurance states that "private companies seeking government contracts will likely be held to the same standards as the agencies they deal with, which will lead to the wider adoption of the cyber security framework proposed by the NIST"[28] and that "increased compliance with NIST will make the framework even more influential in businesses in all sectors of the economy."[29]

Another major component of the government-private sector information sharing platform is the integration of Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs). ISACs are non-profit, sector-specific organizations comprised of member organizations from various critical infrastructure entities.[30] For example, banks and credit card processors can engage the Financial Services Information and Sharing Analysis Center (FSISAC) to collaborate on critical security threats to the financial services sector to receive information specifically designed to help protect critical systems and assets from physical cybersecurity threats in an efficient manner.[31] A 2015 Executive Order directing DHS to encourage the development of ISAOs to facilitate and respond to cyber threats to the critical infrastructure in real time[32] was implemented to develop a more efficient means for granting clearances to members of an ISAO and to engage in "continuous, collaborative, and inclusive coordination with ISAOs via the DHS NCCIC."[33]

---

[23] *Id*.
[24] Nat'l Protection and Programs Directorate; Nat'l Protection and Programs Directorate Seeks Comments on Cyber Incident Data Repository White Papers, 81 Fed. Reg. 17,193, 17,194 (Mar. 28, 2017).
[25] DEPT. OF HOMELAND SEC., ENHANCING RESILIENCE THROUGH CYBER INCIDENT DATA SHARING AND ANALYSIS, *available at* https://www.dhs.gov/publication/cyber-incident-data-and-analysis-working-group-white-papers.
[26] Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (May 11, 2017).
[27] *Id*.
[28] *Cyber security framework marches forward*, BUSINESS INSURANCE (Jul. 3, 2017), http://www.businessinsurance.com/article/00010101/NEWS06/912314233/Cyber-security-framework-marches-forward.
[29] *Id*.
[30] DEPT. OF HOMELAND SEC., *Information Sharing*, https://www.dhs.gov/topic/cybersecurity-information-sharing (last visited Nov. 13, 2017).
[31] https://www.fsisac.com/
[32] Exec. Order No. 13,687, 80 Fed. Reg. 819 (Jan. 6, 2015).
[33] https://www.dhs.gov/isao.

Finally, NIST has developed InfraGard, a co-sponsorship agreement with the Small Business Administration (SBA) and the Federal Bureau of Investigation (FBI) to conduct regional workshops that focus specifically on IT security for small businesses.[34] The workshops provide small businesses with access to IT security personnel to provide advice and education on security threats posed to businesses, as well as how to asses vulnerabilities and identify the necessary protections for such threats.[35] InfraGard also emphasizes the importance of information sharing between the federal government – facilitated through the FBI – and private sector entities.[36]

III. H.R. 4668, the Small Business Advanced Cybersecurity Enhancements Act of 2017

There is strong bipartisan commitment from both chambers of Congress and the President to update certain domestic laws related to cybersecurity. The most controversial issues involve the appropriate role of the federal government in working with private industry to protect critical infrastructure.

It is critical that the federal government and the private sector work together to combat cyber threats.[37] The National Cybersecurity and Communications Integration Center was established to encourage collaboration between the public and private sectors. However, many small businesses do not use this resource to its intended capacity simply because they are reluctant to engage with the federal government.[38] Small businesses are more hesitant to share information with the federal government due to uncertainty around potential legal liabilities and concerns about privacy and data protection. Many small businesses are concerned about the type of information that would be provided to the federal government if they use the available information sharing portals.[39]

On December 18, 2017, Chairman Steve Chabot (R-OH) introduced H.R. 4668, the Small Business Advanced Cybersecurity Enhancements Act of 2017.[40] This legislation encourages small businesses to work with the federal government by providing them additional access to resources and greater legal protections. The bill establishes Small Business Administration (SBA) Small Business Development Centers (SBDCs) as the primary interface for federal information sharing for small businesses, ensures small businesses that share cyber threat indicators through SBDCs receive expanded protections and exemptions provided in the Cybersecurity Information Sharing Act of 2015, ensures that any policies or rulemaking adopted by any federal agency as a result of small business cyber information sharing does not unfairly

---

[34] http://csrc.nist.gov/groups/SMA/sbc/overview.html.
[35] *Id*.
[36] *Id*.
[37] *Federal Government and Small Businesses: Promoting Greater Information Sharing for Stronger Cybersecurity: Hearing Before the H. Comm. on Small Business*, 115th Cong. (2017) (Statement of Ola Sage, Chief Executive Officer, e-Management), *available at* https://smallbusiness.house.gov/uploadedfiles/11-15-17_sage_testimony.pdf.
[38] *Id.*
[39] *Federal Government and Small Businesses: Promoting Greater Information Sharing for Stronger Cybersecurity: Hearing Before the H. Comm. on Small Business*, 115th Cong. (2017) (Statement of Morgan Reed, President, ACT | The App Association), *available at* https://smallbusiness.house.gov/uploadedfiles/11-15-17_reed_testimony.pdf.
[40] H.R. 4668, 115th Cong., 1st Sess. (2017).

burden small businesses, and expands liability protections for small businesses that engage with the federal government.

IV. Other Policy Initiatives and Considerations for the 115th Congress

On January 17, 2017, Representative Daniel M. Donovan (R-NY) introduced H.R. 584, the Cyber Preparedness Act of 2017.[41] This legislation would require DHS's State, Local, and Regional Fusion Center Initiative to coordinate with the National Cybersecurity and Communications Integration Center to provide state, local, and regional fusion centers with expertise on DHS cybersecurity resources.[42] The bill passed the House on January 31, 2017 and is awaiting action in the Senate.

On July 10, 2017, Chairman Steve Chabot (R-OH) introduced H.R. 3170, the Small Business Development Center Cyber Training Act of 2017.[43] This bill would amend the Small Business Act to require the SBA to establish a program to provide cybersecurity planning assistance to small businesses.[44] A Senate companion bill, S. 1428, the Small Business Cyber Training Act of 2017, has been introduced in the Senate.[45]

In the 114th Congress, Representative Richard L. Hanna's (R-NY) legislation, H.R. 5064, the Improving Small Business Cyber Security Act of 2016, was enacted.[46] This law eases the burden on small businesses facing cyber threats by providing access to additional tools, resources, and expertise through existing federal cyber resources. Specifically, it permits the DHS and other federal agencies working in coordination with DHS to provide assistance to small businesses through Small Business Development Centers (SBDC). The information and resources distributed by SBDCs will streamline cyber support for small businesses. Additionally, the law requires the SBA and DHS to collaboratively develop a Small Business Development Center Cyber Strategy in consultation with representatives of SBDCs. It also allows SBDCs to offer cyber support to small businesses in accordance with the Cyber Strategy. This strategy will also provide guidance to SBDCs on how best to use existing federal resources to improve cyber support services for small businesses.

In the 114th Congress, a compromise version of Senator Richard Burr's (R-NC) legislation, S. 754,[47] the Cybersecurity Information Sharing Act (CISA), was included in the Consolidated Appropriations Act of 2015.[48] This law required the Director of National Intelligence, the Department of Justice, and DHS to develop procedures to share cybersecurity threat information with private entities. Among other things, it incentivizes businesses to engage in information sharing practices with the federal government by providing specific liability protection for information sharing activities. This language is an important step forward in encouraging greater small business participation in information sharing.

---

[41] H.R. 584, 115th Cong., 1st Sess. (2017).
[42] *Id*.
[43] H.R. 3170, 115th Cong., 1st Sess. (2017).
[44] *Id*,
[45] S. 1428, 115th Cong., 1st Sess. (2017).
[46] H.R. 5064 was included in the National Defense Authorization Act for Fiscal Year 2017. Pub. L. No. 114-328, §§ 1841-1844 (2016).
[47] S. 754, 114th Cong. (as passed by the Senate on Oct. 27, 2015).
[48] Consolidated Appropriations Act of 2015, P.L. 114-113, 129 Stat. 2242 ("CISA")

V. Conclusion

The movement of information and commerce to the Internet has provided a new opportunity for bad actors, both foreign and domestic, to steal sensitive and valuable information from small businesses, as well as exploit vulnerabilities in the global supply chain to engage in criminal activities. Due to small businesses' lack of resources and the complex and technical nature of many cybersecurity information sharing services, small businesses have been slow to adopt information sharing practices that strengthen America's cybersecurity defense and, therefore, remain at increased risk of a foreign-backed cyber attack. Additionally, small businesses remain wary of the potential legal liabilities and privacy concerns related to cybersecurity information sharing and it is vital that the federal government strike a balance between the imposition of overly onerous burdens on small business and the need to protect America's IT from foreign cyber threats.