NSI | THE NATIONAL SECURITY INSTITUTE
At George Mason University's Antonin Scalia Law School

CYBER IMPERATIVE: PRESERVE AND STRENGTHEN PUBLIC-PRIVATE PARTNERSHIPS

***By MEGAN BROWN**
NSI Senior Fellow and Associate Director for Cybersecurity Programs, and Partner, Wiley Rein LLP

THIS WHITE PAPER:

1. Examines the importance of public-private partnerships (PPPs) to United States cybersecurity policy and law.
2. Explains the benefits of collaboration and partnership—domestically and abroad—over regulation and mandates.
3. Describes challenges to cooperation, such as limitations in current law, the overlap in government cyber activities, and fear of post-hoc recrimination.
4. Urges policymakers to strengthen partnership and collaboration through creative solutions that change the culture around private cyber risk and incidents.

**Matthew Gardner, Kathleen Scott, Michael Diakiwski and Paul Coyle, all of the Cybersecurity Practice at Wiley Rein LLP, assisted in the research and drafting of this paper. That representation involves appearing before the agencies referred to herein, including in support of information sharing about cybersecurity threats and responses.*

I INTRODUCTION AND EXECUTIVE SUMMARY

Cybersecurity is a major national and economic security challenge. The United States recognizes the cyber threat, yet it is difficult to "solve" for several reasons: the inherently global nature of the adversary and the battlefield, the rapid evolution of tactics and technology, the involvement of both nation state and non-state actors, and the unsuitability of a regulatory solution or "checklist" approach.

This challenge requires unprecedented collaboration among stakeholders: peer companies, vendors, suppliers, customers, researchers, and government. At the July 2018 National Cybersecurity Summit[1], the Secretary of the U.S. Department of Homeland Security ("DHS") underscored the need for public-private cooperation. "We are taking a clear-eyed look at the threat and taking action—and notably...collective action to combat them."[2] The Secretary continued, "[t]he majority of U.S. infrastructure is owned and operated by the private sector, not the government, so we must be working together...and across industries to better defend... systems and critical functions."[3]

The United States long has chosen collaboration over regulation. But recently, policymakers are expecting more from the private sector and there is a risk that the PPP model may begin to yield to regulatory mandates. This paper looks at the importance of PPPs to U.S. cybersecurity policy and identifies the virtues of PPPs in meeting cybersecurity challenges. It also identifies ways that policymakers can strengthen PPPs.

POLICYMAKERS SHOULD EXPLORE CREATIVE SOLUTIONS, SUCH AS:

- treating U.S. companies that suffer a breach or attack as true victims of crime
- creating safer ways for companies to manage and discuss vulnerabilities
- protecting the exchange of information by expanding exemptions from FOIA and the protections in CISA
- considering safe harbors for reasonable cybersecurity practices

Policymakers should embrace and strengthen the PPP model, and avoid pursuing regulatory or other models that will erode trust.

1 Press Release, U.S. Dept. of Homeland Security ("DHS"), *DHS Hosts Successful First-Ever National Cybersecurity Summit* (Aug. 1, 2018), https://www.dhs.gov/news/2018/08/01/dhs-hosts-successful-first-ever-national-cybersecurity-summit.
2 Secretary Kirstjen M. Nielsen, DHS, Keynote Speech at the National Cybersecurity Summit (July 31, 2018), https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech.
3 *Id.*

II CYBER CHALLENGES REQUIRE CREATIVITY, FLEXIBILITY, AND AGILITY

The private sector cannot meet the diverse and evolving range of cybersecurity challenges alone.[4] As FBI Director Christopher Wray has said:

> *[The cyber] threat now comes at us from all sides. We're worried about a range of threat actors, from multi-national cyber syndicates and insider threats to hacktivists. We're seeing an increase in nation-state sponsored computer intrusions. And we're also seeing a "blended threat"—nation-states using criminal hackers to carry out their dirty work.[5]*

Indeed, the threat is global because of the connectivity that supports our internet-enabled society. Internet service providers ("ISPs") operate globally and more than 800 wireless carriers will build and manage next-generation networks. Supply chains are distributed around the world, as hardware and software cross borders to be used by multinational organizations and governments. Devices connected to the Internet support and provide access to everything from banking to social media. The organizations that are targeted are often global in operation and attackers are dispersed around the world. Finally, methods of attack have become more sophisticated, including global distributed denial of service (DDoS) attacks and other automated, distributed threats that can exploit internet openness from afar.[6]

As technologies have evolved, sectors have increased attention to security, while innovation has fostered new solutions that thrive or fail based on their effectiveness. Put simply: we learn over time and conventional wisdom can fall out of favor. The National Institute of Standards and Technology ("NIST") demonstrated this when it walked away from settled password advice. The architect of that advice "was wrong, and he admits it. 'Much of what I did I now regret,' he says."[7]

Similarly, security approaches have evolved from perimeter defense to rapid detection and recovery. As McKinsey observed, "[p]rogressive corporations are reorienting security architectures from devices and locations to roles and data."[8] Now, networks are being designed with security in mind as software and virtualization offer new protection.

As networks, technologies, and threats evolve, collaboration among all stakeholders must continue.

4 *See* National Institute of Standards and Technology ("NIST"), NIST Internal Report 8192, *Enhancing Resilience of the Internet and Communications Ecosystem: a NIST Workshop Proceedings*, at 15 (Sept. 2017), https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8192.pdf (discussing the "nationalization of state mafias and cyber criminal organizations").
5 Director Christopher Wray, Federal Bureau of Investigation ("FBI"), Keynote Address at the Fordham University FBI International Conference on Cyber Security, Raising Our Game: Cyber Security in an Age of Digital Transformation (Jan. 9, 2018), https://www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation.
6 *See* U.S. Dept. of Commerce ("DOC") & DHS, *Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, at 3 (May 22, 2018) ("Botnet Report"), https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf, (finding that "The majority of the compromised devices in recent noteworthy botnets have been geographically located outside the United States.").
7 Douglas Perry, *Widely Used Password Advice Turns Out to Be Wrong*, NIST Says, Government Technology (Aug. 10, 2017), http://www.govtech.com/security/Widely-Used-Password-Advice-Turns-Out-to-Be-Wrong-NIST-Says.html.
8 James Kaplan et al., *Meeting the Cybersecurity Challenge*, McKinsey (June 2011), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/meeting-the-cybersecurity-challenge.

III THE FEDERAL GOVERNMENT HAS LONG SUPPORTED PPPS, WHICH ARE CENTRAL TO FEDERAL CYBERSECURITY POLICY.

Public private partnerships, in various forms, have existed throughout U.S. history.[9] Partnerships take many forms, depending on the goals and capabilities of participants. PPPs have become particularly vital in cybersecurity because so much critical infrastructure is in private control and because our domestic innovation base has created so many essential digital services.

THE EXECUTIVE BRANCH HAS PIONEERED THE USE OF PPPS TO ADDRESS CYBERSECURITY.

Cybersecurity PPPs have a long history shaped by Executive Orders and Presidential Directives. In 1998, Presidential Decision Directive-63 ("PDD-63") introduced Information Sharing and Analysis Centers ("ISACs"), where critical infrastructure owners and operators come together to "collect, analyze and disseminate actionable threat information . . . and provide members tools to mitigate risks and enhance resiliency."[10]

This spurred the establishment of an ISAC for each critical infrastructure sector and many are now mature. The earliest—the Financial Services ISAC ("FS-ISAC")—was formed in 1999,[11] and most have been in existence for over 10 years.[12] ISACs coordinate with each other, across sectors, and with the government. For example, the Automotive ISAC ("Auto-ISAC") recently signed a Cooperative Research and Development Agreement ("CRADA") with DHS to collaborate on vehicle cyber-threats.[13] This agreement lets Auto-ISAC members obtain security clearances and access government facilities. "As the automotive industry continues to prepare for an increasingly interconnected future, the ability to collaborate with DHS and other private sector companies markedly increases [the Auto-ISAC's] ability to detect and prevent vehicle cybersecurity threats."[14] The Communications ISAC, also known as the DHS National Coordinating Center, is part of DHS's National Cybersecurity and Communications Integration Center ("NCCIC"),[15] which is the "national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement."[16]

President Obama championed PPPs. Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing*,[17] called on DHS to "develop a more efficient means for granting clearances to private

9 Richard Norment, PPPs – *American Style*, Project Finance International Journal, Vol. 39, Oct. 2002, at 26. An early example was initiated by the Pacific Railway Act of 1862, which created a program to grant federal land to corporations to spur economic development along the first transcontinental railroad project. Pacific Railway Act of 1962, 12 Stat. 489, 37th Cong. (July 1, 1862), https://www.loc.gov/law/help/statutes-at-large/37th-congress/session-2/c37s2ch120.pdf.
10 National Council of Information Sharing and Analysis Centers ("ISACs"), *About ISACs*, https://www.nationalisacs.org/about-isacs.
11 National Council of ISACs, *Member ISACs*, https://www.nationalisacs.org/member-isacs.
12 National Council of ISACs, *About ISACs*, https://www.nationalisacs.org/about-isacs.
13 Press Release, Auto-ISAC, *Auto-ISAC signs cybersecurity agreement with DHS* (Jan. 25, 2018), https://www.automotiveisac.com/wp-content/uploads/2018/05/01_25_18_DHS-CISCP-FINAL-Press-Release-1.pdf.
14 *Id.*
15 National Council of ISACs, *Member ISACs*, https://www.nationalisacs.org/member-isacs.
16 DHS, *National Cybersecurity and Communications Integration Center,* https://www.dhs.gov/national-cybersecurity-and-communications-integration-center.
17 Press Release, The White House, *Executive Order -- Promoting Private Sector Cybersecurity Information Sharing* (Feb. 13, 2015), http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

sector individuals" in Information Sharing and Analysis Organizations ("ISAOs") and to "identify a set of voluntary standards or guidelines" for them.[18] ISAOs embody the PPP model, recognizing that "some organizations do not fit neatly within an established sector or have unique needs. . . . [and] those organizations that cannot join an ISAC but have a need for cyber threat information could benefit from membership in an ISAO."[19] Other Executive Orders make PPPs a central element. Executive Order 13636, Improving Critical Infrastructure Cybersecurity, explained that "[w]e can [enhance the security and resilience of the Nation's critical infrastructure and promote innovation and efficiency] through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."[20]

The Trump Administration likewise emphasizes partnerships, as underscored by Vice President Mike Pence at the 2018 National Cybersecurity Summit. Cybersecurity "is a shared responsibility," he said, "[a]nd the President and I need you to continue to be advocates in your industry and among your peers for greater cybersecurity collaboration."[21] Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, emphasized the role of government to "support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure."[22] Follow-on work, such as the Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats, note the importance of public-private partnerships and call for "collaboration" to "improve the ability of ecosystem members to mitigate" botnet threats.[23]

PPPS ACROSS FEDERAL AGENCIES PROMOTE COLLABORATION INSTEAD OF REGULATION TO ADVANCE CYBERSECURITY.

PPPs have been the bedrock of U.S. cyber policy because they combine the expertise and innovation of the private sector with the unique capabilities of government. As described by Rep. Tim Murphy, Chairman of the House Energy and Commerce Subcommittee on Oversight and Investigations:

> ***[For] decades, a cornerstone of the nation's efforts to combat cyber threats have been public-private partnerships designed to facilitate engagement and collaboration between the government and private sector. Over time this model has evolved, but the objective remains the same – unity of effort between those responsible for protecting the nation and those who own and operate the infrastructure that is critical to that mission.***[24]

18 DHS, *Information Sharing and Analysis Organizations*, https://www.dhs.gov/isao.
19 *Id.*
20 Press Release, The White House, *Executive Order -- Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
21 Vice President of the United States Mike Pence, Remarks at the DHS Cybersecurity Summit (July 31, 2018), https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-dhs-cybersecurity-summit/.
22 Executive Order, The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.
23 Botnet Report at 10. https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.
24 *Hearing on Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships Before the H. Subcomm. on Oversight & Investigations,* 115th Cong. (2017) (Statement of Rep. Tim Murphy, Chairman, H. Subcomm. on Oversight & Investigations, Comm. on Energy and Commerce), https://docs.house.gov/meetings/IF/IF02/20170404/105831/HHRG-115-IF02-MState-M001151-20170404.pdf.

Indeed, PPPs exist across federal agencies. A driving force is NIST, which has championed collaboration for over a hundred years.[25] Part of NIST's mission is:

> ***To assist private sector initiatives to capitalize on advanced technology; to advance, through cooperative efforts among industries, universities, and government laboratories, promising research and development projects, which can be optimized by the private sector for commercial and industrial applications; and to promote shared risks, accelerated development, and pooling of skills which will be necessary to strengthen America's manufacturing industries.***[26]

NIST's cybersecurity role has evolved but collaboration is central. The Cybersecurity Enhancement Act of 2014 directs NIST to "facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure."[27] Private collaboration was key to NIST's Framework for Improving Critical Infrastructure Cybersecurity, which "was developed in a year-long, collaborative process in which NIST served as a convener for industry, academia, and government stakeholders."[28] NIST works "in an open and transparent manner that enlists broad industry and academia expertise from around the world."[29]

Other agencies also use cyber-focused PPPs. DHS coordinates much of the information sharing between the government and private sector and is developing sharing technologies. For example, Automated Indicator Sharing ("AIS"), managed by DHS's U.S. Computer Emergency Readiness Team ("US-CERT"), aims to "enable[] the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed."[30]

DHS works with private and government and "strives to protect the physical and cyber infrastructure that we rely on and make it more resilient to what we cannot prevent."[31] For example, the Office of Cybersecurity and Communications "leads efforts to protect the federal '.gov' domain of civilian government networks and to collaborate with the private sector—the '.com' domain—to increase the security of critical networks."[32]

Efforts are underway to shift rolas at DHS to emphasize collaboration, including by raising the profile and mission of the National Protection and Programs Directorate (NPPD) more explicitly to focus on cybersecurity.

In 2018, DHS announced the establishment of the National Risk Management Center to be "the gateway for American companies who want to work with the federal government more closely to strengthen our shared cybersecurity."[33]

25 National Bureau of Standards Act, 31 Stat. 1449, 56th Cong. (Mar. 3, 1901), https://www.loc.gov/law/help/statutes-at-large/56th-congress/session-2/c56s2ch872.pdf.
26 15 U.S.C. § 271.
27 Cybersecurity Enhancement Act of 2014, § 101, Pub. L. No. 113-274, 128 Stat. 2971 (2014), https://www.gpo.gov/fdsys/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf.
28 NIST, Cybersecurity Framework FAQS Framework Basics, https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics.
29 *Hearing on Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry Before the Joint H. Subcomm. on Oversight and Subcomm. on Research & Tech.*, 115th Cong. (2017) (Statement of Charles H. Romine, Director, Information Technology Laboratory), https://www.nist.gov/speech-testimony/bolstering-government-cybersecurity-lessons-learned-wannacry.
30 United States Computer Emergency Readiness Team ("US-CERT"), *Automated Indicator Sharing*, https://www.us-cert.gov/ais.
31 DHS, *NPPD at a Glance*, https://www.dhs.gov/sites/default/files/publications/nppd-at-a-glance-bifold-02132018-508.pdf.
32 DHS, *Office of Cybersecurity and Communications*, https://www.dhs.gov/office-cybersecurity-and-communications.
33 Vice President of the United States Mike Pence, Remarks at the DHS Cybersecurity Summit (July 31, 2018), https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-dhs-cybersecurity-summit/.

This center will:

> ***Move collaborative efforts beyond information sharing and develop a common understanding of risk and joint action plans to ensure our nation's most critical services and functions continue uninterrupted in a constantly evolving threat environment.***[34]

Sector-specific agencies embrace PPPs as well. The Department of Energy's Multiyear Plan for Energy Sector Cybersecurity highlights PPPs as "foundational to DOE's strategy. Facing an ever-evolving threat landscape requires a coordinated approach to improving risk management capabilities, information sharing, and incident response."[35] Its partnership includes funding for "innovative research, development, and demonstration… that will build cyber resilience into energy systems for tomorrow."[36]

The Federal Communications Commission ("FCC") relies on advisory committees—composed of industry experts, among others—to study cybersecurity and identify best practices. For example, the Communications Security, Reliability and Interoperability Council ("CSRIC"), which is in its sixth charter, has developed guidance and best practices for botnet remediation,[37] securing SS7,[38] along with general cybersecurity best practices,[39] among other work.

The Food and Drug Administration ("FDA") is looking to PPPs to address cybersecurity in medical devices. The FDA Commissioner wants to develop a "CyberMed Safety (Expert) Analysis Board, a public-private partnership that would complement existing device vulnerability coordination and response mechanisms and serve as a resource for device makers and the agency" and "promote a multi-stakeholder, multi-faceted approach of vigilance, responsiveness, recovery, and resilience that applies throughout the life cycle of relevant devices."[40]

CONGRESS HAS EMBRACED A COLLABORATIVE APPROACH TO CYBERSECURITY THROUGH PPPS.

Congress has considered and rejected a regulatory approach to cybersecurity—valuing collaboration over mandates. To improve information sharing, Congress passed the Critical Infrastructure Information Act of 2002, which created the Protected Critical Infrastructure Information ("PCII") Program "to protect private sector infrastructure information voluntarily shared with the government for the purposes of homeland security."[41] Under the PCII Program, DHS has uniform procedures for receiving, validating, handling, storing, marking, and using information voluntarily shared by industry.[42] Significantly, PCII information cannot be disclosed through a FOIA request, be disclosed in civil litigation, or be used for regulatory purposes.[43]

34 Press Release, DHS, *DHS Hosts Successful First-Ever National Cybersecurity Summit* (Aug. 1, 2018), https://www.dhs.gov/news/2018/08/01/dhs-hosts-successful-first-ever-national-cybersecurity-summit.
35 U.S. Dept. of Energy ("DOE"), *Multiyear Plan for Energy Sector Cybersecurity* (Mar. 2018), https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf.
36 *Id.* at 5.
37 Communications Security, Reliability and Interoperability Council ("CSRIC") III, Working Group 7, Final Report, *U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)* (Mar. 2012), https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf.
38 CSRIC V, Working Group 10, Final Report, *Legacy Systems Risk Reductions* (Mar. 2017), https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf.
39 CSRIC IV, Working Group 4, Final Report, *Cybersecurity Risk Management and Best Practices* (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.
40 Commissioner Scott Gottlieb, Food and Drug Administration ("FDA"), *Statement on new efforts to enhance and modernize the FDA's approach to medical device safety and innovation* (Apr. 17, 2018), https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm604672.htm.
41 DHS, Protected Critical Infrastructure Information ("PCII") Program, https://www.dhs.gov/pcii-program.
42 *Id.*
43 DHS, *Protected Critical Infrastructure Information Program* (Jan. 2017) ("PCII Fact Sheet"), https://www.dhs.gov/sites/default/files/publications/pcii-fact-sheet-2017-508.pdf.

The Cybersecurity Information Sharing Act of 2015 ("CISA") went further by creating a framework to foster greater information sharing in both directions: industry to government and government to industry. CISA envisions a "voluntary cybersecurity information sharing process that will encourage public and private sector entities to share cyber threat information... [and] allow for greater cooperation and collaboration in the face of growing cybersecurity threats to national and economic security."[44] As the Senate Intelligence Committee stated, "some cybersecurity information that could enable the businesses facing these threats to better protect themselves remains exclusively in the government" due to over-classification and the tendency for parochialism in the Intelligence Community.[45]

Under CISA, DHS's Cyber Information Sharing and Collaboration Program ("CISCP") serves as the hub for data sharing and analytical collaboration.[46] CISCP's mission is to "establish a community of trust between the Federal Government and entities from across the different critical infrastructure sectors and then leverage these relationships for enhanced information sharing and collaboration."[47] Some opposed CISA due to privacy concerns,[48] but the bill helped develop a needed cyber security asset and industry welcomed it to "help businesses achieve timely and actionable situational awareness to improve detection, mitigation, and response capabilities against cyber threats."[49]

Since CISA's enactment, industry has grown more comfortable sharing with the government. Dr. Charles Clancy, Director of Virginia Tech's Hume Center for National Security and Technology, told Congress that he has "seen industries come together in the past three years. Many of the [ISACs] have adopted sharing standards. There's still caution from industry, but industry does appreciate the access to government information [and is] getting more comfortable with these interactions."[50]

Congress continues to explore opportunities to support and expand the use of PPPs. The Senate Committee on Banking, Housing, and Urban Affairs is looking at cyber risks to financial services,[51] and recognizes that private industry-led efforts can be impactful:

> ***Banks are under constant attack every day. Because of this, they and other firms in the financial services industry have devoted substantial resources to protecting information systems, and the industry is widely viewed as one of the most advanced sectors in terms of prioritizing cybersecurity.[52]***

44 S. Rep. No. 114-32, at 2 (2015), https://www.congress.gov/114/crpt/srpt32/CRPT-114srpt32.pdf.
45 *Id.*
46 DHS, *Cyber Information Sharing and Collaboration Program* (CISCP) (June 2013), https://csrc.nist.gov/CSRC/media/Events/ISPAB-JUNE-2013-MEETING/documents/ispab_june2013_menna_ciscp_one_pager.pdf.
47 DHS, *Critical Infrastructure And Key Resources Cyber Information Sharing And Collaboration Program*, https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf.
48 Some tech firms and privacy advocates publicly opposed the bill for lacking adequate privacy protections and limits on permissible uses of the information shared with the government. See Amul Kalia, *Tech Industry Trade Groups Are Coming Out Against CISA. We Need Individual Companies To Do The Same, Electronic Frontier Foundation* (Oct. 20, 2015), https://www.eff.org/deeplinks/2015/10/tech-industry-trade-groups-are-coming-out-against-cisa-we-need-individual.
49 The Financial Services Sector Coordinating Council welcomed the bill as "a strong vote of confidence for information sharing and its importance as a key component of effective cyber risk mitigation." Russ Fitzgibbons & John Carlson, Financial Services Sector Coordinating Council, *Statement on Senate Passage of CISA* (Oct. 28, 2015), https://www.fsisac.com/sites/default/files/news/cisa_statementjwc.pdf. A coalition of industry trade associations, including the U.S. Chamber of Commerce, sent a letter of support to U.S. Senators urging them to pass the bill. U.S. Chamber of Commerce, Letter from Industry Associations to U.S. Senators Urging the Senate to Pass CISA (Dec. 2, 2014), https://www.uschamber.com/sites/default/files/141202_multi-industry_s2588_cisa_senate.pdf.
50 Hearing on Telecommunications, Global Competitiveness, and National Security Before the H. Subcomm. on Commc'ns & Tech., 115th Cong. (2018) (Testimony of Charles Clancy, Director and Professor, Hume Center for National Security and Technology, Virginia Tech).
51 *Hearing on Cybersecurity: Risks to the Financial Services Industry and Its Preparedness Before the S. Comm. on Banking, Housing and Urban Affairs*, 115th Cong. (2018) (Statement of Mike Crapo, Chairman, S. Comm. on Banking, Housing and Urban Affairs), https://www.banking.senate.gov/imo/media/doc/Crapo%20Statement%205-24-18.pdf.
52 *Hearing on Cybersecurity: Risks to the Financial Services Industry and Its Preparedness Before the S. Comm. on Banking, Housing and Urban Affairs*, 115th Cong. (2018) (Statement of Chairman Mike Crapo), https://www.banking.senate.gov/imo/media/doc/Crapo%20Statement%205-24-18.pdf.

The House Energy and Commerce Committee has held hearings investigating how public-private partnerships have strengthened cybersecurity in the healthcare sector:[53]

> ***Effective collaboration between government and the private sector is vital to elevating our security posture. These partnerships provide a vital link between those responsible for the safety and security of the nation with those who own and operate the infrastructure critical to those objectives.***[54]

Appropriations committees have supported PPPs in committee reports for energy appropriations.[55] Congress is concerned about health care sector cybersecurity and recently looked at health care PPPs.[56]

Congress has been a reliable advocate for PPPs, and continued congressional support is critical.

53 See *Hearing on Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships Before the H. Subcomm. on Oversight & Investigations*, 115th Cong. (2017), https://docs.house.gov/meetings/IF/IF02/20170404/105831/HHRG-115-IF02-MState-W000791-20170404.pdf.
54 *Id.* Statement of Greg Walden, Chairman, H. Comm. on Energy & Commerce, https://docs.house.gov/meetings/IF/IF02/20170404/105831/HHRG-115-IF02-MState-W000791-20170404.pdf.
55 H. Comm. on Appropriations, 115th Cong., Rep. on Energy & Water Dev. Appropriations Bill, 2019, at 88-89 (2018), https://appropriations.house.gov/uploadedfiles/energy_report.pdf ("The Committee places a high priority on ensuring the protection of the grid against cyberattacks . . . . Many different actors, governmental and private, play a role in preventing and responding to threats to the nation's energy infrastructure. The Committee expects the Department [of Energy] to continue coordinating its efforts with all stakeholders to ensure the highest priority areas are being addressed effectively in its ongoing efforts to protect the grid."). The Senate Committee on Appropriations also addresses PPPs in the context of infrastructure security. See S. Rep. No. 115-258, at 80 (2018) https://www.congress.gov/115/crpt/srpt258/CRPT-115srpt258.pdf.
56 *Hearing on Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships Before the H. Subcomm. on Oversight & Investigations*, 115th Cong. (2017), https://energycommerce.house.gov/hearings/cybersecurity-heath-care-sector-strengthening-public-private/.

IV PUBLIC-PRIVATE PARTNERSHIPS HARNESS PRIVATE EXPERTISE TO ADDRESS EVOLVING CYBER THREATS.

Effective cybersecurity solutions are industry-driven, flexible, global, and voluntary. Traditional regulation is slow and inflexible.

PPPs work better than regulation to harness private sector expertise and cultivate the right incentives. As one scholar observed, "regulations, after all, were designed in response to earlier technologies and the market failures they generated. They don't cover largely speculative and mostly future-looking concerns."[57]

REGULATION RUNS THE RISK OF BEING BACKWARD LOOKING, STATIC, AND DRIVING A COMPLIANCE MINDSET.

Ultimately, the biggest problem with prescriptive regulation in cybersecurity is that solutions cannot keep pace with the problems they are trying to solve. It is hard to imagine the Code of Federal Regulations keeping pace with the remarkable speed of evolution in cyber threats and defenses. This is why the government has long recognized we need a "dynamic and flexible framework ... to adapt to challenges of rapidly changing technology."[58] At best, regulations are slow and backward-looking, hardly suited to meet rapidly changing threats and trends. At worst, they could make networks less secure. Regulations can provide bad actors with a roadmap of how targets are defending themselves. Regulations also can promote a compliance mindset that focuses entities on the wrong things. As the Ambassador-At-Large and State Department's Coordinator for Counterterrorism observed, prescriptive regulation in the financial sector "might distort firms' cyber-security investments. Rather than expending resources on defenses against the attacks they regard as the most dangerous, or the most likely to occur, financial institutions will tend to prioritize defenses against the one form of intrusion singled out by their regulators...at the expense of increased exposure to many other threats."[59] Addressing cybersecurity with a static set of requirements does not foster agile risk management. This is why PPPs are so important in cybersecurity.

CORPORATIONS HAVE AN INCENTIVE TO PROTECT THEIR INFORMATION, SYSTEMS, CUSTOMER DATA, AND NETWORKS.

Contrary to a popular talking point that market incentives do not align with security, industry is motivated. ISPs want to bring consumers ultra-fast, high capacity, and secure Internet services. Cyberattacks not only divert billions of dollars from ISPs' efforts, but they reduce customer confidence. Because cybersecurity is fundamental to the viability of networks, protecting them is part of the bottom line. Likewise, IT service providers do not want customers' confidence shaken by cyber incidents, so

57 Larry Downes, *How More Regulation for U.S. Tech Could Backfire*, Harvard Business Review (Feb. 9, 2018) https://hbr.org/2018/02/how-more-regulation-for-u-s-tech-could-backfire (opining that in our system of government, "[t]here's no framework for pre-emptively regulating nascent industries and potential new technologies.").
58 Department of Commerce, Internet Policy Task Force "Green Paper" on CYBERSECURITY, INNOVATION AND THE INTERNET ECONOMY (2011) https://www.nist.gov/sites/default/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf.
59 Nathan A. Sales, *Regulating Cyber-Security*, 107 Nw. U. L. Rev. 1503, 1538-38 (2013), https://pdfs.semanticscholar.org/b388/0abe3af2102154cc10b4093eea7d45f5a48a.pdf.

they use risk management principles to safeguard their assets and the systems on which their customers depend. Retailers invest in security to reduce the risk of consumer breaches, and utilities are looking at their operations. More can always be done, but the private sector has incentives to take reasonable cybersecurity measures.

PRIVATE ORGANIZATIONS KNOW THEIR CYBER INFRASTRUCTURE AND VULNERABILITIES.

Organizations, networks, data, and dependencies vary. And each organization is best positioned to develop appropriate solutions. Take wireless carriers. They have innovated, built, and run sophisticated networks that enable the connectivity that drives every aspect of modern life. They invest billions in securing these systems, deploying multiple layers of security. These experts, with intimate knowledge of the networks, their capabilities, and their defenses, should drive policy that impacts security of those networks.

CORPORATIONS ARE DEVELOPING SOLUTIONS TO DATA AND CYBERSECURITY CHALLENGES.

The tech sector innovates at breakneck pace. Competition and speed to market drove many of the advances in technology, and security was not always at the forefront. But that is changing. Technology companies are prioritizing security and working collaboratively—not competitively—in the face of changing cyber challenges. Coalitions have emerged[60] "to combine technology, public policy and economics to create a sustainable system of cybersecurity"[61] and establish "forum[s] through which diverse parties can work together to create and maintain a trusted [digital] ecosystem."[62] And an entire ecosystem of cybertools and services is emerging.

The PPP model harnesses these dynamics. It does not shut government out; to the contrary, government is a key stakeholder. Government has access to intelligence and methods unavailable to the private sector, like taking down botnets. The FBI worked closely with the private sector and international partners to take down the GameOver Zeus botnet, which was "believed to be responsible for the theft of millions of dollars from businesses and consumers in the U.S. and around the world."[63] The government can act against bad actors in ways that are impossible for the private sector.

60 *See, e.g.*, Press Release, U.S. Telecom, *Council to Secure the Digital Economy Announces 2018 Priorities* (May 11, 2018), https://www.ustelecom.org/news/press-release/council-secure-digital-economy-announces-2018-priorities. The council is comprised of senior internet and communications technology leaders and experts representing the leading global technology companies with a diversity of interests and a strongly-shared commitment to working collaboratively toward securing our digital economy from current and future cyber threats; see also Council to Secure the Digital Economy, http://securingdigitaleconomy.org/.

61 Internet Security Alliance has three core goals: (1) To demonstrate thought leadership in advancing the development of a sustainable system of cyber security; (2) To advocate for public policy that will advance the interests of cybersecurity; and (3) To create increased awareness and programs that will result in more rapid adoption of cybersecurity standards, practices and technologies. See Internet Security Alliance, Mission and Goals, https://isalliance.org/about-isa/mission-and-goals/.

62 Cloud Security Alliance harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. See Cloud Security Alliance, Membership, https://cloudsecurityalliance.org/membership/#_overview.

63 FBI, *GameOver Zeus Botnet Disrupted, Collaborative Effort Among International Partners* (June 2, 2014, *updated* July 11, 2014), https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted; see also Lorenzo Franceschi-Bicchierai, *How the FBI Took Down the Botnet Designed to Be 'Impossible' to Take Down, VICE* (Aug. 12, 2015), https://motherboard.vice.com/en_us/article/539xy5/how-the-fbi-took-down-the-botnet-designed-to-be-impossible-to-take-down.

V POLICYMAKERS SHOULD BOLSTER INCENTIVES FOR CYBERSECURITY PPPS.

Even though policymakers have recognized that PPPs are essential to security, collaboration involves risks related to public disclosure, responsibility, and liability.[64]

To enhance collaboration we must address continuing barriers to participation—including liability and regulatory exposure—otherwise companies may hesitate to provide government with access to their networks or information about identified vulnerabilities. For example, if information provided is not kept confidential, then reporting a cyber attack could damage corporate reputation or expose a network to more risk if sensitive information were to get in to the hands of malicious actors. Some disclosures can also cause confusion for consumers, leading the public to believe relatively insignificant vulnerabilities may be more serious than they are. Further, the risk of civil litigation and potential class actions remains, even for diligent organizations that manage risks, monitor their networks, and participate in information sharing structures.

DHS and other agencies recognize this: "Policymakers, legislators, and stakeholders need to consider ways to better incentivize efforts to enhance the security of IoT" by looking at "how tort liability, cyber insurance, legislation, regulation, voluntary certification management, standard-setting initiatives, voluntary industry-level initiatives, and other mechanisms could improve security" while encouraging economic activity and "groundbreaking innovation."[65]

DHS and the Department of Commerce further note that:

> ***Care must be taken to ensure that our liability laws benefit consumers, protect stakeholders when appropriate, and avoid chilling innovation in today's digital environment. As public-private sector collaboration in this area continues, the federal government should continue to monitor whether protection from liability related to information sharing is sufficient in today's environment to effectively address ongoing and new threats.***[66]

In drafting CISA, lawmakers acknowledged these key industry concerns:

> ***Entities appropriately monitoring their systems for cybersecurity threats and sharing information necessary to protect against those threats should not be exposed to costly legal uncertainty for doing so. Moreover, it is these same companies who are the victims of malicious cyber activity, and their appropriate efforts to protect themselves and other future victims from cyber threats should not only be authorized but protected from unnecessary litigation."***[67]

CISA "creates narrowly tailored liability protection to incentivize companies' efforts to identify cybersecurity threats and share information about them."[68] It grants "liability protection and other legal protections—such as

64 Concerns have been raised by private companies and security professionals. In a recent proceeding before DHS and Commerce, "stakeholders stressed the importance of minimizing uncertainty and legal risk to encourage private-sector collaboration with law enforcement agencies, more information sharing, vulnerability disclosure, and the ability to conduct effective countermeasures. Many also emphasized the need to harmonize legal approaches across sectors to avoid a patchwork of laws that could impede the IoT market." Botnet Report at 24, https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.
65 DHS, *Strategic Principles for Securing the Internet of Things* (IoT), at 13-14 (2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.
66 Botnet Report at 24-25, https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.
67 S. Rep. No. 114-32, at 3 (2015), https://www.congress.gov/114/crpt/srpt32/CRPT-114srpt32.pdf
68 *Id.*

antitrust protections, exceptions from disclosure laws and certain regulatory uses, and protections from privilege waivers—to private entities that share cyber threat indicators and defensive measures in compliance with the Act."[69]

However, despite its laudable goals, CISA does not go far enough.

First, CISA does not provide the same level of protection for private-to-private information sharing as for private-to-government sharing. Information on cyber threat indicators and defensive measures shared with the federal government, "shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection."[70] While this promotes sharing with the federal government, there is no provision protecting privilege for information shared between private organizations. Such sharing could constitute a waiver of privilege and expose organizations to additional legal risk, simply for participating in an information sharing structure.

Second, CISA's protections are limited to sharing "cyber threat indicators" and "defensive measures."[71] The protections do not clearly extend to the sharing and development of best practices, cybersecurity strategies, and other advancements outside of these categories. The importance of this limitation is reflected in recent litigation to compel production of information shared with an ISAC. In *Flynn v. FCA U.S. LLC and Harman International Industries*,[72] stemming from the hacking of an Internet-connected vehicle,[73] plaintiffs subpoenaed the Auto-ISAC—a non-party—to compel disclosure of a vast amount of materials from the ISAC, including "[d]ocuments reviewed, considered, published or otherwise related to Auto-ISAC's creation of the automotive cybersecurity 'Best Practices'" and all communications with the automaker from 2010-2016.[74] The Auto-ISAC argued against disclosure, which "could chill information sharing that is vital to national security,"[75] because "if companies believe that confidential information [provided] to ISACs will be easily accessible through third-party subpoenas, they will not provide such information."[76] Ultimately, the court quashed the subpoena, because it placed an undue burden on Auto-ISAC.[77] The court did not address the security concerns or the potential chilling effect raised by the ISAC.

Third, CISA's antitrust exemptions could be stronger. Under CISA, "it shall not be considered a violation of any provision of antitrust laws for [two] or more private entities to exchange or provide a cyber threat indicator or defensive measure, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes..."[78] Guidance was issued by DHS and the DOJ in which they reiterated protection;[79] but its contours remain unclear. Given the vital role standards bodies and certifications will play, uncertainty is counterproductive. The language on this topic should clearly cover critical tools, best practices, and forward-looking strategies for enhancing cyber preparedness, defense, and response.

69 Botnet Report at 24, https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.
70 6 U.S.C. § 1504(d)(1).
71 *Id.*, see 6 U.S.C. §§ 1501-1510.
72 *Flynn v. FCA U.S. LLC*, No. 16-mc-00078, 2016 WL 6996181 (S.D. Ill. Nov. 30, 2016).
73 See Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me In It, WIRED* (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
74 Non-Party Auto-ISAC, Inc.'s Motion to Quash Third-Party Subpoena at 2, 6, *Flynn*, 2016 WL 6996181 (S.D. Ill. Sept. 27, 2016).
75 Non-Party Auto-ISAC, Inc.'s Reply in Support of Motion to Quash Third-Party Subpoena at 17, *Flynn*, 2016 WL 6996181 (S.D. Ill. Oct. 21, 2016).
76 Non-Party Auto-ISAC, Inc.'s Motion to Quash Third-Party Subpoena at 13, *Flynn*, 2016 WL 6996181.
77 Order, *Flynn*, 2016 WL 6996181 (S.D. Ill. Nov. 30, 2016).
78 6 U.S.C. § 1503(e) (This only applies to "information that is exchanged or assistance provided in order to assist with—(A) facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system; or (B) communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system.").
79 DHS & DOJ, *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015,* at 16 (June 15, 2016), https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf ("The Act provides a statutory exemption to federal antitrust laws for sharing between and among private entities of cyber threat indicators, defensive measures, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat for a cybersecurity purpose.").

VI POLICYMAKERS SHOULD HARMONIZE CYBER EFFORTS AND EVANGELIZE PUBLIC-PRIVATE PARTNERSHIPS ABROAD.

POLICYMAKERS SHOULD SUPPORT PPPS BY FOCUSING GOVERNMENT EFFORTS AND REDUCING OVERLAP IN CYBER ACTIVITIES.

Policymakers can help promote PPPs by reducing regulatory uncertainty and overlapping jurisdiction. U.S. cybersecurity includes a patchwork of laws, regulations, and guidance, often with intersecting authorities. Many agencies have sector-specific regulatory authority, but they are expanding their involvement on cyber issues, with far-reaching impacts.

Numerous agencies are engaged on Internet of Things ("IoT") security. Activities range from drafting guidelines and regulations to investigations and enforcement actions.

- The Consumer Products Safety Commission has been looking at possible consumer safety hazards from connected devices.[80]
- DOJ issued IoT guidelines with the Consumer Technology Association,[81] and made multiple recommendations to address cybersecurity and botnets in its Cyber Digital Task Force Report.[82]
- The Federal Trade Commission ("FTC") pursues data security enforcement actions, which touch many industries. The FTC brought enforcement actions against IoT device manufacturers, including manufacturers of smart TVs, home security cameras and baby monitors, and routers.[83]
- The Food and Drug Administration has issued guidelines and developed a Medical Device Safety Action Plan to enhance connected device security.[84]
- The National Highway Traffic Safety Administration is engaged in automotive security and connected vehicles.[85]
- NIST has numerous workstreams on IoT, including an effort to map international IoT standards[86] and a project identifying security and privacy considerations.[87]

This is a sample of federal agency activity on IoT alone. PPPs can be diluted and lose their value with too many ongoing activities that strain limited industry resources.

80 The Internet of Things and Consumer Product Hazards, 83 Fed. Reg. 13122-01 (Mar. 27, 2018), https://www.federalregister.gov/documents/2018/03/27/2018-06067/the-internet-of-things-and-consumer-product-hazards.
81 DOJ, Consumer Technology Association ("CTA"), *Securing Your "Internet of Things" Devices* (July 2017), https://www.justice.gov/criminal-ccips/page/file/984001/download.
82 DOJ, *Report of the Attorney General's Cyber Digital Task Force* (July 2, 2018), https://www.justice.gov/ag/page/file/1076696/download.
83 Federal Trade Commission ("FTC"), Public Comment on "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers" (June 2017), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications-information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf ("The FTC's enforcement actions send an important message to manufacturers about the need to take reasonable steps to safeguard the privacy and security of IoT devices.").
84 FDA, *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health*, https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf. This plan highlights several existing or proposed public-private partnerships.
85 *See*, e.g., U.S. Dept. of Transportation ("DOT"), NHTSA, Vehicle-to-Vehicle Communication, https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communication; DOT, Vehicle Cybersecurity, https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity; DOT, NHTSA, Automated Vehicles for Safety, https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety.
86 NIST, NISTIR 8200: *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things* (IoT) (Feb. 2018), https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf.
87 NIST, *Pre-Read Document for the NIST Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks Workshop* (June 28, 2018), https://www.nist.gov/sites/default/files/documents/2018/06/28/draft-iot-workshop-pre-read-document.pdf.

Policymakers should coordinate, streamline overlapping efforts, and highlight key initiatives. This will create more impactful PPPs, benefitting the security ecosystem.

INTERNATIONAL PPPS WILL BE CRITICAL TO MEET THE FUTURE GLOBAL CYBER CHALLENGES.

Policymakers can support successful PPPs by championing collaboration abroad. As cybersecurity approaches are developing around the world, international regulation could challenge companies and threaten U.S. technological dominance. Multiple activities are looking to set standards and increase regulation across the globe. From the EU's General Data Protection Regulation ("GDPR") and directive on security of network and information systems ("NIS Directive"), to Chinese cybersecurity law, countries are passing laws that amount to forced data localization and promise to complicate international trade and global data flow. These laws will complicate and stifle the work of PPPs, including information sharing entities.[88]

As the United States considers national strategies for data security and privacy, it is imperative that industry and government treat security as a global issue. When market solutions emerge, U.S. companies should identify them to global standards groups. The U.S. government can champion these standards globally to discourage regulation, which can stifle innovation and global trade.

Multinational companies and governments should encourage better cross-border information sharing and cooperation. "To increase the resilience of the Internet and communications ecosystem against these threats, many of which originate outside the United States, we must continue to work closely with international partners."[89] International engagement and the deterrence of adversaries on a global scale must be a priority. In May 2018, the State Department outlined a strategy for the United States to work with international partners.[90] The State Department "suggests a new U.S. vision to help guide efforts to deter adversaries and better protect the American people from cyber threats and recommends follow-on work aimed at advancing these efforts."[91] The United States should champion its successful PPP model abroad and encourage other countries to support information sharing and collaboration.

88 Rick Weber, *DHS' Manfra: EU's GDPR could hamper cyber info-sharing; botnet report sent to White House, Inside Cybersecurity* (May 23, 2018), https://insidecybersecurity.com/daily-news/dhs-manfra-eus-gdpr-could-hamper-cyber-info-sharing-botnet-report-sent-white-house (reporting the DHS is considering whether GDPR will hamper information sharing).
89 *See* Botnet Report at 3, https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.
90 U.S. Dept. of State, *Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Attacks* (May 31, 2018), https://www.state.gov/s/cyberissues/eo13800/282011.htm.
91 *Id.*

VII CREATIVE SOLUTIONS CAN ENHANCE CYBERSECURITY.

The cyber challenge to our infrastructure, economy, and values is not going away. Companies will be victimized, often by nation states. Consequences range from massive data loss to disruption of operations. Instead of waiting for a "digital 9/11" and then enacting corrective legislation, we should be looking for creative ways to expand the partnerships that will enable fast responses and collaboration.

Trust is the key ingredient. "One of the key hesitations in the private sector to form a public-private partnership concerns issues of trust, control, and disclosure."[92] So, "[c]ybersecurity PPPs must be based on a foundation of mutual trust, and open dialogue between private companies and the government can help to ameliorate some of the reluctance in the private sector."[93] Our adversaries are not following the traditional playbooks, so U.S. policymakers need to think big. They should ask how to create conditions for companies to do the right things without fear of recrimination. Far too often, a U.S. company that suffers an attack is revictimized by Congressional oversight, lawsuits and public approbation. We need to expand effective partnerships and create an environment that supports companies' good faith efforts to address risk and collaborate with peers, suppliers, and the government.

1 POLICYMAKERS SHOULD TREAT CORPORATIONS WHO SUFFER CYBER ATTACKS AS VICTIMS AND DO MORE TO HELP THEM RESPOND AND RECOVER.

FBI Director Chris Wray promises that "at the FBI, we treat victim companies as victims."[94] This sentiment is hardly new but needs to be turned into meaningful action. In the last Administration, Commerce Secretary Pritzker lamented that companies hit with a cyber attack often see only "the downsides of engagement – potential liability, the risk of punitive action, and the investigations that may result from even basic interactions."[95] Congress and the Administration should be looking for ways to mitigate these concerns.

Companies attacked by malicious cyber actors can be subject to lawsuits, congressional scrutiny and state and federal enforcement. A national study conducted in 2018 pegged the average costs of a data breach at $3.86 million dollars per incident, up six percent from 2017.[96] The Deputy Attorney General has taken note, "one large retailer reported spending $291 million in breach-related expenses, related to one attack on its network."[97] Responding to and recovering from

92 Arnav Jagasia, *A Look into Public Private Partnerships for Cybersecurity*, Wharton School of Business (Apr. 18, 2017) https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for.
93 *Id.*
94 Director Chris Wray, FBI, Remarks Prepared for Delivery at Boston College/FBI - Boston Conference on Cyber Security, *Digital Transformation: Using Innovation to Combat the Cyber Threat* (Mar. 7, 2018), https://www.fbi.gov/news/speeches/digital-transformation-using-innovation-to-combat-the-cyber-threat.
95 Secretary Penny Pritzker, DOC, Remarks Prepared for Delivery at U.S. Chamber of Commerce Cyber Security Summit (Sept. 27, 2016), https://www.commerce.gov/news/secretary-speeches/2016/09/us-secretary-commerce-penny-pritzker-delivers-keynote-address-us.
96 IBM, 2018 Cost of a Data Breach Study by Ponemon, *available for download upon registration at*, https://www.ibm.com/security/data-breach.
97 Deputy Attorney General Rod J. Rosenstein, DOJ, Remarks Prepared for Delivery at the Global Cyber Security Summit, London, United Kingdom (Oct. 13, 2017), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-global-cyber-security-summit.

breaches is particularly hard on small- and medium-sized organizations. As Deputy Attorney General Rosenstein continued, "breaches sometimes drive smaller businesses into bankruptcy."[98] The consequences can be far worse for incidents that involve business disruptions, theft of proprietary information, or attacks on critical infrastructure.

Policymakers should be thinking about how to change the culture around incident reporting, vulnerability management, and public discussions of companies that have suffered an attack.

Several years ago, DOJ developed Best Practices for Victim Response and Reporting of Cyber Incidents,[99] but more can be done to help businesses that are victims of cybercrime. The DOJ Crime Victims Fund is a potential model. DOJ's Crime Victims Fund was established in 1984 by the Victims of Crime Act to compensate victims with the "fines and penalties paid by convicted federal offenders."[100] The Fund has almost $9 billion.[101] Crime victim compensation from the Fund is direct reimbursement for crime-related expenses.[102] Congress could look into a similar effort for corporate victims of cybercrime, with a focus on small and medium businesses. If the amount of compensation rewarded to victims to assist their recovery is tied to the use of voluntary security standards or best practices, this could incentivize better cybersecurity at all levels. This may be more productive than the array of federal agency cyber tip sheets for small businesses.[103]

2 POLICYMAKERS SHOULD CREATE SAFER WAYS FOR COMPANIES TO MANAGE AND DISCUSS VULNERABILITIES.

Companies should have better and safer ways to handle vulnerabilities in software, products and devices, which can be discovered by ethical hackers or internal security experts. Companies face varied challenges when they face claimed or known vulnerabilities. They may need to validate a speculative or theoretical issue found by a researcher. The issue may be hard to exploit in the real world or have a complex mitigation. They may confront complex software and hardware supply chains, and there are often multiple layers between companies and end users who may need to deploy patches.

Some companies have "Bug Bounty" programs in which "white hat" hackers discover and report vulnerabilities, sometimes for a reward. According to HackerOne, "with hacker-powered security testing, organizations can identify high-value bugs faster with help from the results-driven ethical hacker community."[104] As the founder of BugCrowd says, "cybersecurity isn't a technology problem — it's a human one — and to compete against an army of adversaries we need an army of allies."[105]

98 *Id.*
99 DOJ, *Best Practices for Victim Response and Reporting of Cyber Incidents* (Apr. 2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf. Thus document "reflects lessons learned by federal prosecutors while handling cyber investigations and prosecutions, including information about how cyber criminals' tactics and tradecraft can thwart recovery. It also incorporates input from private sector companies that have managed cyber incidents.
100 DOJ, Office for Victims of Crime, Crime Victims Fund, https://www.ovc.gov/about/victimsfund.html.
101 *Id.*
102 DOJ, Office for Victims of Crime, Crime Victims Fund, OVC Fact Sheet, https://www.ovc.gov/pubs/crimevictimsfundfs/intro.html.
103 Tip sheets and materials abound from the Small Business Administration ("SBA"), FCC, FTC, NIST, DHS, among many. *See, e.g.*, SBA, Cybersecurity, https://www.sba.gov/managing-business/cybersecurity; FCC, Cybersecurity for Small Business, https://www.fcc.gov/general/cybersecurity-small-business; Press Release, FTC, *FTC to Launch Campaign to Help Small Businesses Strengthen Their Cyber Defenses* (Apr. 10, 2018), https://www.ftc.gov/news-events/press-releases/2018/04/ftc-launch-campaign-help-small-businesses-strengthen-their-cyber; NIST, Small Business Information/Cybersecurity Workshop Presentation (Dec. 9, 2014), https://csrc.nist.gov/csrc/media/projects/small-business-community/documents/sbc_workshop_presentation_2015_ver1.pdf; DHS, Stop.Think.Connect. Small Business Resources, https://www.dhs.gov/publication/stopthinkconnect-small-business-resources.
104 HackerOne, Inc., The Hacker-Powered Security Report 2018 (July 2018), https://www.hackerone.com/sites/default/files/2018-07/The%20Hacker-Powered%20Security%20Report%202018.pdf.
105 Bugcrowd, *Why Crowdsource Security?,* https://ww2.bugcrowd.com/rs/453-IJC-858/images/why-crowdsourced-security-bugcrowd-032118.pdf.

Government agencies are embracing coordinated vulnerability disclosure (CVD) programs and members of Congress have been exploring them as a best practice.[106]

Google Project Zero, which employs researchers to look for vulnerabilities in third parties' products, has been driving CVD discussions.[107]

Project Zero has had to become more flexible as its high-minded ideals collide with the complexities of the real world. The team initially kept to a strict 90-day disclosure deadline, or just seven days for "actively exploited" bugs, but several instances of disclosure shortly before companies had scheduled to release updates, such as Microsoft and its recurring "Patch Tuesday," caused the group a lot of backlash.[108]

The vulnerability disclosure process is not always smooth, and companies reasonably worry about fallout. "Public disclosure — particularly premature disclosure — can scare consumers, inform competitors of weakness, inspire government oversight, result in litigation, and of course, facilitate attacks by hackers exploiting the vulnerability."[109] Lawsuits sometimes follow disclosure and "fear of such litigation could be a serious deterrent to active participation in vulnerability disclosure efforts."[110]

Even when all goes well, companies are criticized for not disclosing quickly enough, for not including more parties, or for mitigations that some deem inadequate. Senators recently questioned the process used by industry to address and disclose vulnerabilities in microprocessors, despite general recognition that they confronted a novel and challenging vulnerability.[111] Criticizing and suing companies who are handling difficult vulnerabilities does not encourage more candid discussions.

Policymakers should consider how to create incentives for vulnerability discovery and appropriate disclosures, which may include immunities from liability or safe harbors for companies that have robust CVD programs.

3 POLICYMAKERS SHOULD CONSIDER MORE ROBUST EXEMPTIONS FROM FOIA.

Companies are concerned about the security and confidentiality of information they share with the government – be it about device security, critical infrastructure, or new technology. Fears about disclosures under the Freedom of Information Act ("FOIA") can be a deterrent to discussions. A lot of information shared can be protected from FOIA disclosure, but it can be difficult within the existing exemptions. Statutory protections are preferable to agency application of FOIA, because FOIA decisions are subject to judicial challenge and there is no guarantee that information shared will be protected.

Congress could add a cybersecurity exception to FOIA or expand an existing program that has fostered information sharing. As discussed above, Congress created the PCII Program in 2002 to protect private sector infrastructure information that was voluntarily shared with DHS for homeland security purposes. PCII information cannot be disclosed through a FOIA (or similar state/local) request, disclosed in civil litigation, or used for regulatory purposes.[112] The PCII program was featured in industry work to promote information

106 *See, e.g.*, Alex Rice, *U.S. Senate Hearing – Data Security and Bug Bounty Programs: Lessons Learned*, HackerOne, Inc. (Feb. 6, 2018), https://www.hackerone.com/blog/US-Senate-Hearing-Bug-Bounty-Lessons-Learned.
107 See Google, Project Zero Blogspot, https://googleprojectzero.blogspot.com/.
108 Robert Hackett, *Google's Elite Hacker SWAT Team vs. Everyone*, Fortune (June 23, 2017), http://fortune.com/2017/06/23/google-project-zero-hacker-swat-team/.
109 Megan Brown, *Considering a Vulnerability Disclosure Program? Recent Push Raises Questions for General Counsel*, CircleID (Feb. 10, 2017), http://www.circleid.com/posts/20170210_considering_a_vulnerability_disclosure_program/.
110 *Id.*
111 *See Hearing on Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown Before the S. Comm. on Commerce, Science, & Transp.*, 115th Cong. (2018), https://www.commerce.senate.gov/public/index.cfm/hearings?ID=77835497-EC96-41E8-B311-5AF789F38422.
112 PCII Fact Sheet, https://www.dhs.gov/sites/default/files/publications/pcii-fact-sheet-2017-508.pdf.

sharing and it has enabled sharing by and with third parties, including the Association of American Railroads, Berkshire Hathaway Energy, the State, Local, Tribal, and Territorial Government Coordinating Council, and the Communications Sector Coordinating Council. The PCII program should be carefully reviewed as a model for similar efforts.

4 POLICYMAKERS SHOULD CONSIDER ADDITIONAL SAFE HARBORS AND IMMUNITY PROVISIONS.

Companies remain worried about class actions and other litigation arising out of claims based on hindsight about the security measures they could or should have taken. They also reasonably fear reproach over the specificity of their descriptions of risk and preparedness, which the Securities and Exchange Commission has been encouraging. Companies may be more candid if they have less fear of shareholder litigation over judgment calls about disclosures related to cyber risk and incidents. Such fears may also give companies pause before engaging in gap analyses or critical self-reflection, lest documents and reports be discoverable in litigation or investigations.

If policymakers want companies to engage in more self-assessment and speak freely about risks, they should consider protecting them from the obvious downsides, like class actions and post-hoc litigation over the adequacy of disclosures that are inherently imperfect.

VIII CONCLUSION

The bedrock of federal cyber policy for the private sector has been voluntary standards, industry collaboration, and public private partnerships. Now is not the time to retreat from that successful model.

To the extent policymakers are concerned about the pace of uptake and collaboration after CISA, or a lack of visibility into corporate practices, they should look to creative solutions and incentives. More robust sharing of information and best practices and smoother cooperation with the federal government to address cybersecurity risks are key, and now is the time to think boldly about changing the culture around blame for companies on the front lines.