CARROTS AND STICKS IN CYBERSPACE: ADDRESSING KEY ISSUES IN THE CYBERSECURITY INFORMATION SHARING ACT OF 2015

Jamil N. Jaffer*

I. INTRODUCTION

On December 18, 2015, President Barack Obama signed into law the Consolidated Appropriations Act, an omnibus piece of legislation containing a compromise version of the Cybersecurity Information Sharing Act of 2015

---

* Jamil N. Jaffer is an Adjunct Professor of Law and Director of the Homeland and National Security Law Program at George Mason University Law School. Professor Jaffer previously served as senior counsel to the House Permanent Select Committee on Intelligence (HPSCI) under Chairman Mike Rogers (R-MI), where he was the principal architect of the original version of the Cyber Intelligence Sharing and Protection Act (CISPA). Professor Jaffer also previously served in the Bush Administration as Counsel to the Assistant Attorney General for National Security at the U.S. Department of Justice, where he led a team of lawyers from the Justice Department's National Security Division working on the President's Comprehensive National Cybersecurity Initiative, an effort for which the team was awarded the Director of National Intelligence's Team of the Year Award – Cyber Legal.

(CISA) passed by the Senate a few months earlier.[1] The enactment of this legislation was, in many respects, a watershed moment, as it marked the culmination of a four-plus year effort by bipartisan majorities in both Houses of Congress to legislate in this critical area.[2] Indeed, CISA represents the first major piece of cybersecurity legislation enacted into law that seeks to directly address the relationship between the private and public sectors. Addressing this relationship is particularly important for the United States government and, in particular, its nascent efforts to protect the nation against serious threats in cyberspace, principally because of the significant portion of the U.S. critical infrastructure that is owned and operated by the private sector.[3] Moreover, because the legislation did not explicitly seek to regulate private actors, the legislation likewise represented a major win for industry, having successfully pushed back against early efforts by the Obama Administration and key players in the Senate to impose significant regulatory requirements upon certain critical infrastructure entities in the private sector.[4]

Thus, it is unsurprising when, around the passage and enactment of CISA, there was much self-congratulation and numerous laudatory statements were made on Capitol Hill.[5] And while, to be sure, there is much cause for celebration in the enactment of this legislation—given that it provides new, clear authorities for cybersecurity threat collection and sharing and the use and sharing of certain types of defensive measures, as well as useful liability protection for such

---

1. *See* Consolidated Appropriations Act of 2015, P.L. 114-113, 129 Stat. 2242 ("CISA"); *see also* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (as passed by the Senate on Oct. 27, 2015).

2. *See* Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (introduced on Nov. 30, 2011) ("CISPA").

3. *See, e.g.*, *Critical Infrastructure and Key Resources*, INFORMATION SHARING ENVIRONMENT, https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources (last visited July 2, 2016) ("The private sector owns and operates an estimated 85% of infra-structure and resources critical to our Nation's physical and economic security. It is, therefore, vital to ensure we develop effective and efficient information sharing partnerships with private sector entities."); see also, *e.g.*, CHRIS BRONK, CYBER THREAT: THE RISE OF INFORMATION GEOPOLITICS IN U.S. NATIONAL SECURITY 63 (Praeger 2016) ("Because so much of the U.S. critical infrastructure is operated by entities within the private sector, the figure of 85% is commonly cited, the process of securing that infrastructure from cyber attack is inherently [a] public-private process.").

4. *Compare, e.g.*, CISA P.L. 114-113, 129 Stat. 2242; The White House Office of the Press Secretary, *Securing Cyberspace- President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts*, THE WHITE HOUSE (Jan. 13, 2015), https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat; *with* The White House Office of the Press Secretary, *Fact Sheet: Cybersecurity Legislative Proposal*, THE WHITE HOUSE (May 12, 2011), https://www.whitehouse.gov/the-press-office/2011/052/fact-sheet-cybersecurity-legislative-proposal; *see also,* Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012).

5. Cory Bennett & Katie Bo Williams, *Senate Passes First Major Cyber Bill in Years*, THE HILL (Oct. 27, 2015), http://thehill.com/policy/cybersecurity/258260-senate-passes-first-major-cyber-bill-in-years; Cory Bennett, *Congress Approves First Major Cyber Bill in Years*, THE HILL (Dec. 15, 2015), http://thehill.com/policy/cybersecurity/263696-congress-approves-first-major-cyber-bill-in-years.

activities when conducted consistent with the new law—one needs wonder why, if this legislation was so critically important, the private sector response was relatively muted.

The answer, unfortunately, lies in the text of the legislation itself and the compromises made in order to get the legislation out of Congress and onto the President's desk for signature. Key provisions of the enacted law were significantly modified from the original text passed by the House in 2012 when significant bipartisan majorities voted in favor of the bill in the face of a White House veto threat. For better or for worse, there is a reasonable argument to be made that while the bill provides very helpful authorities for the private sector, it may nonetheless result in very little new cybersecurity threat sharing, at least as between the private sector and the government. This Article will briefly lay out some of the key provisions of CISA as enacted, highlighting the important benefits for the private sector in the legislation and the strong opportunities it provides for enhanced cybersecurity defensive activities by industry and expanded threat sharing, particularly private-to-private sharing. The Article will also identify key flaws in the legislation and will conclude with a brief set of recommendations for Congress to consider as it continues to examine the intersection between public and private sector cybersecurity efforts.

II. CORE CISA AUTHORITIES FOR DETECTING AND MITIGATING CYBERSECURITY THREATS

Perhaps the most obvious group of benefits provided by CISA are the clear, positive grant of authorities it provides for private sector cybersecurity threat monitoring and use of defensive measures.

First, CISA provides a specific, but broad grant of authority to private sector entities to conduct monitoring, for cybersecurity purposes, of their own systems and the systems of customers that provide authorization and written consent for such monitoring.[6] This authority permits a private sector entity to conduct fairly comprehensive cybersecurity monitoring efforts on its own information systems and those of its authorized customers, including, most importantly, information stored on, processed by, or transiting such systems.[7] The latter provision, permitting the monitoring of information transiting a given private sector actor's information system, is particularly important for Layer 1 providers, who can use

---

6. *See* CISA, P.L. 114-113, § 104(a)(1), 129 Stat. 2242 (2015). ("(a) Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—(A) an information system of such private entity; (B) an information system of another non-Federal entity, upon the authorization and written consent of such other entity; . . . and (D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.").

7. *See id.*

this authority to protect their systems and those of their consenting customers from threats neither originating nor destined for the provider's own systems.[8]

Second, CISA provides a significantly large carrot to incentivize private entities for conducting such monitoring in the form of specific liability protection for such activities.[9]

Third, CISA provides a specific (and similarly broad) grant of authority to private sector entities to operate defensive measures on their own systems, as well as on the systems of their customers that provide appropriate authorization and written consent for the operation of such measures.[10]

These provisions, at least as to monitoring, are similar to the language contained in the original House-passed CISPA bill.[11] Indeed, with the addition of the defensive measures authority, CISA is stronger than the original CISPA legislation on these positive authorities. These provisions, taken together, can be read to significantly enhance the ability of corporate Chief Information Officers (CIOs), Chief Security Officers (CSOs), and Chief Information Security Officers (CISOs) to conduct their network defense activities with less concern about legal challenges (at least within certain clearly delineated bounds as provided in the bill). In essence, these positive authorities serve to get the lawyers out of the room—at least once the determination has been made that the proposed activities and purposes meet the definitions in CISA—allowing the cybersecurity professionals to do their job.

---

8. *See, e.g.*, H.R. Rept. No. 112-45 (accompanying H.R. 3523) (2011) 11, https://www.congress.gov/112/crpt/hrpt445/CRPT-112hrpt445.pdf ("CISPA Committee Report") ("In this context, it is the Committee's intent that the protection of the rights and property of a corporate entity includes, but is not limited to, the protection of the systems and networks that make up its own corporate internal and external information systems but also the systems and networks over which it provides services to its customers. For example, the Committee expects that an internet service provider or telecommunications company may seek to protect not only its own corporate networks but also the backbone communications systems and networks over which it provides services to its customers.") (discussing related language in the original Cyber Intelligence Sharing and Protection Act).

9. *See id.* at § 106(a), 2950–51 ("No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of an information system and information under section 104(a) that is conducted in accordance with this title.")

10. *See id.* at § 104(b)(1), 2941 ("Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—(A) an information system of such private entity in order to protect the rights or property of the private entity; [and] (B) an information system of another non-Federal entity upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity.").

11. *See* CISPA H.R. 3523 112th Cong. § 1104(b)(1) (2011) ("Notwithstanding any other provision of law, a cybersecurity provider, with the express consent of a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes, may, for cybersecurity purposes- (i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such protected entity; and (ii) share such cyber threat information with any other entity designated by such protected entity.")

Undoubtedly, any prudent CIO, CSO, or CISO will still consult in-house or outside counsel for guidance as needed, but barring significant changes in the law or its interpretation by the courts, these provisions in CISA ought make such monitoring and use of defensive measures by the private sector significantly easier and more efficient, principally because the new law puts these activities on firm legal footing pursuant to positive authority that is explicitly carved out from other potentially applicable laws.

III. CORE CISA AUTHORITIES FOR INFORMATION SHARING

CISA also provides a fairly broad grant of authority to private sector entities in order to enhance information sharing. Specifically, CISA provides a general authority to private sector entities to share cyber threat indicators and defensive measures with one another for cybersecurity purposes (and with the federal government, as discussed *infra*) and to use such shared threat indicators and defensive measures for cybersecurity purposes, so long as the sharing and use complies with any lawful restrictions imposed by the entity providing them (and, in the case of use, retention, and further sharing by a receiving entity, any restriction imposed by law).[12] This broad sharing authority—like the monitoring authority—also comes with a carrot: private sector entities sharing with other private sector entities under the aegis of CISA are entitled to liability protection for such sharing.[13]

There are three critical caveats to this broad sharing authority and its accompanying carrot of liability protection, however. The first caveat—the minimization requirement—will be discussed in this section because it relates both to sharing with the government and within the private sector, while the second caveat—the single path into government—will be discussed in the context of private-to-government sharing,[14] and the third caveat—the limitations

---

12. *See* CISA § 104(c)(1) ("Except as provided in paragraph (2) and notwithstanding any other provision of law, a non-Federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-Federal entity or the Federal Government a cyber threat indicator or defensive measure."); *see id.* § 104(c)(2) ("A non-Federal entity receiving a cyber threat indicator or defensive measure from another non-Federal entity or a Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing non-Federal entity or Federal entity."); *see also* id § 104(d)(3) ("Consistent with this title, a cyber threat indicator or defensive measure shared or received under this section may, for cybersecurity purposes . . . be used by a non-Federal entity to monitor or operate a defensive measure . . . and [] be otherwise used, retained, and further shared by a non-Federal entity subject to . . . an otherwise lawful restriction placed by the sharing non-Federal entity or Federal entity on such cyber threat indicator or defensive measure[]or [] an otherwise applicable provision of law.")

13. *See id.* at § 106(b)–(b)(1) ("No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 104(c) if . . . such sharing or receipt is conducted in accordance with this title[.]").

14. *See infra* Part IV.

on liability protection—will be discussed in the context of private-to-private sharing because of its likely impact (or lack thereof) on the incentives for such sharing.[15]

First, CISA requires private sector entities, prior to sharing any cyber threat indicators, to review such indicators in order to assess whether they contain any information known to be a specific individual's personal or identifying information that is not directly related to a cybersecurity threat.[16] If such information is found, it must be removed prior to sharing.[17] Alternatively, the legislation permits a private sector entity to utilize technical capabilities configured to remove such information.[18]

This provision—while not as onerous as earlier versions—could have a significant limiting effect on both private-to-private sharing as well as private-to-government sharing because it essentially requires private sector entities to conduct a form of minimization—as the government does when it collects communications content. That is, it imposes upon the private sector for the sharing of cybersecurity threat information—not communications content—a requirement that is typically imposed upon the government only when it captures the substance and purport of a communication. In the typical law enforcement context, minimization is handled at the time of collection when the individual conducting the wiretap make the decision whether an ongoing conversation is relevant to the investigation.[19] In other contexts, like foreign intelligence surveillance, minimization is conducted pursuant to specific guidelines and employs the use of redactions and the like.[20] Indeed, the imposition of minimization on the government is a heavy burden, typically required in order to protect the privacy of individual communicants. To impose such a burden on the

---

15. *See infra* Part V.

16. *See* CISA § 104(d)(2) ("A non-Federal entity sharing a cyber threat indicator pursuant to this title shall, prior to such sharing—(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information.").

17. *See id.*

18. *See id.* at § 104(d)(2)(A)–(B) ("... [O]r (B) implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.").

19. *See, e.g.*, United States v. Rivera, 527 F.3d 891, 904-07 (9th Cir. 2008) (describing certain criminal minimization procedures).

20. *See, e.g.*, NATIONAL SECURITY AGENCY, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION, PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 12, (declassified), https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf ("A dissemination based on communications of or concerning a United States person may be made in accordance with Section 7 or 8 below if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person.")

private sector, particularly in the context of a threat sharing mechanism where concerns about private communications are fairly limited, is to put a significant barrier in the path of robust information sharing for limited privacy benefits.

To be sure, the minimization requirement in CISA is somewhat limited: all that companies are required to look for and remove is information not directly related to a cybersecurity threat that the sharing party *knows at the time of sharing* to be personal information a specific individual or identifies such individual.[21] Nonetheless, imposing a minimization-like requirement, somewhat narrow though it might be, will likely make companies less likely to share in the first instance, at least until the market develops CISA-compliant sharing systems or mechanisms that employ a technical capability along the lines authorized by statute. Indeed, given the fact that the entire CISA regime is voluntary and the government is ostensibly seeking to *incentivize* private actors to share both with the government and one another to improve the collective defense posture of the nation and key private sector entities, particularly in the critical infrastructure area,[22] it is an odd (and potentially counterproductive) move to impose a costly requirement on voluntary actors. It is also worth noting that the imposition of such a minimization requirement on a private sector actor—much less one who you hope to incent into sharing—is unprecedented. For example, in every surveillance context that the author is aware of, it is the government, not the private party that is responsible for minimization in the first instance. This is true even in the most privacy-sensitive case where the government is affirmatively collecting communications content for the specific purpose of reviewing the content pursuant to appropriate legal authority; in that scenario, the provider gives the government access to the full content of communications and it is the government that is responsible for applying the relevant minimization process.

IV. SHARING WITH THE GOVERNMENT

As noted above, CISA's broad sharing provisions also apply to the government, in that they authorize private sector entities to share cyber threat indicators and defensive measures with the government.[23] And in the opposite direction (i.e., government-to-private), CISA actually requires the government to develop procedures to facilitate and promote the sharing of both classified and

---

21. *See* CISA § 104(d)(2).

22. *See, e.g.*, Protecting America's Cyber Networks Coal., *Cybersecurity Information-Sharing Legislation: 'Voluntary' Means Voluntary—Separating Fact from Fiction*, U.S. CHAMBER OF COMMERCE WEBSITE (August 26, 2015), https://www.uschamber.com/file/cisa-voluntary-separating-fact-fictionpdf (describing how the voluntary nature of CISA's provisions are essential to its legislative purposes).

23. *See* CISA § 104(c)(1).

unclassified cyber threat information with the private sector.[24] The Department of Homeland Security is charged with creating the capability to receive cyber threat indicators and defensive measures in real time from the private sector within ninety days of enactment of the legislation.[25] While on their face these provisions ought to create the basis for a strong information sharing relationship between the private sector and the government, again, key provisions of CISA serve to limit the usefulness of these authorities.

And this leads us to the second major caveat to broad sharing authority and liability protection for sharing mentioned above. When it comes to sharing with the government, CISA is very clear that private sector entities may share with whomever they want in the federal government and that there are no sharing mandates.[26] Indeed, the bill as enacted contains specific language making clear that nothing in the legislation may be construed to "limit or modify an existing information sharing relationship[,] to prohibit a new information sharing relationship[,] to require a new information sharing relationship between any non-Federal entity and a Federal entity or another non-Federal entity[,] or to require the use of the [real-time] capability and process within the Department of Homeland Security."[27] At the same time, though, the part of the legislation that requires DHS to create a real-time receipt capability makes clear that once the Secretary of DHS certifies that this real time process operates fully and effectively, the DHS system "*shall* . . . be *the process* by which the Federal Government receives cyber threat indicators and defensive measures . . . shared by a private entity with the Federal Government...."[28] And while this provision has an exception for "communications between a Federal entity and a non-Federal entity regarding a previously shared cyber threat indicator [and] . . . communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat," these fairly minor exceptions principally serve to underline the central role that CISA envisions for

---

24. *See id.* at § 103(a)–(a)(1) ("Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall jointly develop and procedures to facilitate and promote—(1) the timely sharing of classified cyber threat indicators and defensive measures in the possession of the Federal Government with representatives of relevant Federal entities and non-Federal entities that have appropriate security clearances[.]").

25. *See id.* at § 105(c)(1)–(1)(A) ("Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—(A) shall accept from any non-Federal entity in real time cyber threat indicators and defensive measures, pursuant to this section[.]").

26. *See, e.g.*, *id.* at § 108(f)(1)-(4); *id.* at § 108(i) ("Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized in this title.").

27. *Id.* at § 108(f)(1)–(4).

28. *Id.* at § 105(c)(1)(B) (emphasis added).

DHS.[29] Namely, CISA explicitly highlights the key compromise made to get the bills to the President's desk: that DHS is to be the central receiving point for all private sector shared threat information for the federal government. This feature of the legislation is underlined by the fact that CISA further provides that in order to take advantage of the bill's key carrot for information sharing with the federal government—liability protection—private sector entities must share cyber threat information with the government through the real-time process created by DHS.[30] And while CISA provides the potential for relief by permitting the President to designate other agencies to receive information,[31] the limitations imposed on this authority (namely that perhaps the most capable agency available to deal with such information, the National Security Agency, is explicitly barred from receiving such information in the first instance), the conditions required for the use of this authority (that the President find such additional designation is *necessary* to receive threat information), and the odds it will be actually employed (particularly given the White House's insistence on this provision) all make this carve-out fairly cold comfort for those looking for options.

Requiring all private sector entities to go only through the DHS portal could result in significant reduction in uptake by industry of the voluntary information process for a variety of reasons. First, DHS is generally seen as facing major challenges in capability in the cyber area[32] and a number of other agencies, from DOD/NSA to FBI, are seen by industry as more capable, reliable, or secure[33]

---

29. *Id.* at § 105(c)(1)(B)(i)–(ii).

30. *See id.* at § 106(b)–(b)(2) ("No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 104(c) if—(1) such sharing or receipt is conducted in accordance with this title; and (2) in a case in which a cyber threat indicator or defensive measure is shared in a manner that is consistent with section 105(c)(1)(B) . . . ").

31. *See id.* at § 105(c)(2)(B)-(B)(I) ("[T]he President may designate an appropriate Federal entity, other than the Department of Defense (including the National Security Agency), to develop and implement a capability and process as described in paragraph (1)…if, not fewer than 30 days before making such designation, the President submits to Congress a certification and explanation that—(I) such designation is necessary to ensure that full, effective, and secure operation of a capability and process for the Federal Government to receive from any non-Federal entity cyber threat indicators or defensive measures under this title . . . .")

32. *See, e.g.*, GAO-16-294, DHS NEEDS TO ENHANCE CAPABILITIES, IMPROVE PLANNING, AND SUPPORT GREATER ADOPTION OF ITS NATIONAL CYBERSECURITY PROTECTION SYSTEM (2016), 16-25 (describing challenges in DHS's core cybersecurity defensive system for the federal government); Daniel Wilson, *DHS Needs To Improve Cybersecurity Efforts, Watchdog Says,* LAW360 (Sept. 15, 2015), http://www.law360.com/articles/702887/dhs-needs-to-improve-cybersecurity-efforts-watchdog-says.

33. William Jackson, *McCain Slams DHS, wants DOD to Defend Cyberspace*, GCN (Mar 27, 2012), https://gcn.com/Articles/2012/03/27/Cyber-defense-hearing-McCain-slams-DHS-favors-DOD.aspx; Susan Hennessey, *CISA in Context: The Voluntary Sharing Model and that "Other" Portal*, LAWFARE (Jan. 13, 2016), https://www.lawfareblog.com/cisa-context-voluntary-sharing-model-and-other-portal ("First, let's air a bit of widely-known governmental dirty laundry. There are members of the executive branch and Congress who oppose a DHS-lead information sharing

and, in some cases, are actively working to reach out to the private sector to be the primary government agency that industry calls in the event of a cyber incident.[34]

Perhaps more importantly, DHS's broad regulatory mandate and role in ensuring critical infrastructure identification, protection, and—ostensibly—regulation, has many industry participants quite reasonably concerned about sharing cyber threats with the very agency that is at the forefront of a larger regulatory movement. And CISA does little to ameliorate such concerns. While the legislation explicitly states that "cyber threat indicators and defensive measures provided to the Federal Government under this title shall not be used . . . to regulate . . . the lawful activities of any non-Federal entity or any activities taken by a non-Federal entity pursuant to mandatory standards"[35] it also provides a major exception that raises at least the same amount of regulatory questions and concerns that the general provision seeks to resolve.[36] The exception specifically provides that "[c]yber threat indicators and defensive measures provided to the Federal Government under this title may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, *inform the development or implementation of regulations* relating to such information systems."[37]

The upshot of this regulatory back-and-forth appears to be that while the government may not *directly* regulate an entity based on its disclosure of a

---

portal. For complex reasons involving cultural values, agency evolution, historical performance, and mission sets, there are factions across the government that simply do not trust DHS to get the job done. As I discussed in my previous post, despite the unanimous consent provision, DHS holds a trump card over other federal agencies in that it can elect to not ingest particular information to the portal by setting STIX TAXII fields. In the unlikely event DHS and the rest of the designated federal entities simply cannot agree, CISA permits the President to set up an alternative path and presumably allow private entities to choose where to share. The provision offers skeptics of DHS—both those who accuse it of plain incompetence and those who fear the agency is "all privacy, no mission"—a presidentially-controlled escape value. If, for whatever reason, DHS is unable to fully, effectively, and securely operate the portal, the President can give the job to someone else.").

34. *Compare, e.g.*, DHS, Information Sharing, available online at https://www.dhs.gov/topic/cybersecurity-information-sharing ("The Cyber Information Sharing and Collaboration Program (CISCP) is DHS's flagship program for public-private information sharing. In CISCP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities. Information shared via CISCP allows all participants to better secure their own networks and helps support the shared security of CISCP partners. Further, CISCP provides a collaborative environment where analysts learn from each other to better understand emerging cybersecurity risks and effective defenses.") *with, e.g.*, INFRAGARD, https://www.infragard.org/node ("InfraGard is a partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.").

35. CISA § 105(d)(5)(D)(i).

36. *See id.* at § 105(d)(5)(D)(ii)(I).

37. *Id.* (emphasis added).

particular cyber threat indicator or defensive measure, a federal or state department or agency (or independent agency) may nonetheless—assuming it has the requisite regulatory authority—use the shared information to inform and develop broader cybersecurity regulations that apply to a class of entities that may or may not include the specific entity that originally shared the information. If this reading of the compromise is accurate, it strongly suggests that those chary about sharing information with the federal government generally, and DHS in particular, because of the specter of coming cybersecurity regulation have more than a reasonable basis for concern.

Thus, while the bill suggests the federal government might consider creating alternate sharing mechanisms,[38] and makes clear that CISA, in and of itself, does not authorize new regulations,[39] the explicit nod to the use of shared information for potential regulatory ends remains a major cause for concern and a likely reason that information sharing with the government may not nearly as broad or deep as supporters of CISA might hope or expect.

V. SHARING AMONGST PRIVATE SECTOR ENTITIES

While CISA provides strong authorities and some incentives for sharing amongst private sector entities as noted above, including liability protection for the act of sharing, more could be done to further incentivize private sector sharing. For example, in moving from CISPA to CISA, legislators abandoned a key aspect of the original legislation's liability protection provision: that not only would private sector entities sharing information be protected from liability for the act of sharing itself, but that they would likewise be protected from actions taken—or not taken—on the basis of information received from others sharing under the legislation's provisions.[40] That is, subject to certain critical caveats

---

38. *See id.* § 105(c)(2)(B).

39. *See id.* at § 108(l) ("Nothing in this title shall be construed—(1) to authorize the promulgation of any regulations not specifically authorized to be issued under this title; (2) to establish or limit any regulatory authority not specifically established or limited under this title; or (3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.").

40. *See* CISPA H.R. 3523 112th Cong. § 1104(b)(4)-(4)(B) ("No civil or criminal cause of action shall lie or be maintained in Federal or State court against a protected entity, self-protected entity, [or] cybersecurity provider . . . acting in good faith— . . . (B) for decisions made based on cyber threat information identified, obtained, or shared under this section."); *see also* CISPA Committee Report, H. Rept. 112-445 at 13-14 ("The Committee's intent is likewise to provide strong liability protection to entities when they engage in robust cyber threat information sharing so that they are not held liable for not acting on every piece of cyber threat intelligence provided by the government or every piece of cyber threat information that they detect or receive from another private sector entity. The Committee believes that if information sharing does become truly robust, the amount of cyber threat information and the speed with which such information will be shared will make it nearly impossible to always protect against every threat in real-time and, as such, private sector entities ought not be held liable for such actions. Similarly, the Committee recognizes that particular entities may engage in a cost-benefit analysis with respect to

designed to address potential moral hazard issues associated with such broad liability protection, including exceptions preserving existing liability rules for activities undertaken in bad faith,[41] CISPA provided a major carrot to industry to incentivize sharing that was simply left out of the final CISA language.

Such incentives may be critical to the broad uptake of information sharing amongst industry participants for a range of reasons. First, while it is true that key industry groups—like the financial services and energy sectors—have made major progress on cyber threat sharing even in the absence of significant federal incentives (indeed, industry organizations such as the FS-ISAC and the E-ISAC are role models for threat sharing), such sharing is likely to be the exception and not the rule. Both of these industries—potentially unlike others—have built-in structural and economic incentives or lack typical barriers that, in combination, make them more likely to share critical threat information. For example, given the highly integrated and interreliant nature of key financial institutions, particularly at the top level with major custodian banks and central security depositories, the systemic nature of the threat to the entire system can create a strong internal incentive for undertaking collective defense measures, including robust threat sharing. Similarly, the remnants of the highly regulated, segmented, and regionalized structure of the electric industry likewise removes some of the competitive pressures that might otherwise inhibit cooperative measures like threat sharing. Other industries, however, may lack some of these inherent incentives or still face competitive issues that could limit robust cooperation. For such highly competitive industries, where a risk to one or two major entities may not create a systemic risk for other players, additional incentives may be necessary. And given the structure of U.S. industry, it is likely that such industries are the norm, not the exception.

As such, CISA's lack of the additional carrot of expanded liability protection offered by CISPA may likewise mean that CISA—while a step in the right direction given the strong authorizing language—may still lack sufficient incentives to encourage even truly robust private-to-private sharing, at least in industries where sufficient incentives are already lacking or where competitive barriers to sharing remain in place.

---

implementing protections against particular threats and the Committee intends this provision to help ensure that a private sector entity making such a judgment not be held liable for making such reasonable determinations.").

41. *See id.* CISPA at § 1104(b)(4) (requiring a provider or other protected entity to "act[] in good faith" in order to obtain liability protection under CISPA); *see also id.* CISPA Committee Report at 14 ("At the same time, the Committee was fully cognizant of the concern that it not create a moral hazard by providing too broad a liability protection provision and that it not incentivize bad acts. As a result, Paragraph (3) requires that the entity be acting in good faith to obtain the benefits of this liability protection. That is, where an entity acts in bad faith, it does not receive the benefit of the strong liability protection provided by the legislation.").

VI. OPPORTUNITIES FOR CONGRESS TO ADDRESS CISA'S KEY FLAWS

If in fact this Article is correct and both private-to-private and, more likely, private-to-government sharing is slower to take off under CISA than expected, there are a few potential quick fixes that could be put in place, should Congress see fit to do so.

First, Congress could easily shift the heavy burden of minimization away from private actors to government recipients, as it does in the classic—and significantly more intrusive—content surveillance context. While this would have the benefit of removing a significant economic and practical barrier to information sharing, it would, admittedly have the downside of not addressing the sharing of personally identifiable information as between private sector actors. In many ways, however, this is an issue that exists even outside the cybersecurity context. With few exceptions, companies like Google, Apple, Microsoft and others, with consent from the individual, regularly collect and share personally identifiable information about their customers, typically consistent with their contractual and licensing provisions and their applicable privacy policies. As such, returning to the status quo ante with respect to private-to-private sharing, while retaining a private-to-government minimization requirement but shifted to the government would have the benefit of taking the pressure off industry while still getting the bulk of the ostensible privacy benefit sought by advocates.

Second, Congress could simply bar the use of any information shared by the private sector for any regulatory purposes—general or otherwise—and remove yet another major economic and psychological barrier limiting industry's sharing with the government.

Third, Congress could work with the President to encourage him to certify additional routes into the government, including providing liability protection for them, or could simply legislate this itself (and potentially opening up the space to some of the most capable actors in government). In either event, freeing industry up from solely working through DHS may be a win for both industry and the government, given its own challenges and the practical reality associated with DHS's apparent regulatory interests in the critical infrastructure space.

Finally, Congress could expand the liability protection offered for cyber threat information sharing beyond just the act of sharing itself to the decisions made by companies in receipt of shared information. Such an expansion, appropriately crafted to avoid potential moral hazard issues, would serve to further incentivize both robust private-to-private sharing, as well as ingest and utilization of government-to-private shared information.

VII. CONCLUSION

On balance, the enactment of CISA is a strong step in the right direction for both private industry and the government. Nonetheless, as is often the case with the legislative process, the compromises made to get to a bill that could pass

both chambers and be signed into law have clearly resulted in a less-than optimal bill, at least with respect to its core goal of encouraging and empowering broad-based cybersecurity information sharing between the private sector and the government. As such, things remain to be done and, should Congress find itself with an opportunity to make additional changes, there are at least a handful of options that, with some artful drafting, could provide a significant impact to further incentivize and promote cyber threat information sharing both within private industry as well as with the government.