University of Michigan Journal of Law Reform

Volume 50 | Issue 4

2017

Automating Threat Sharing: How Companies Can Best Ensure Liability Protection When Sharing Cyber Threat Information With Other Companies or Organizations

Ari Schwartz
Venable LLP

Sejal C. Shah
Venable LLP

Matthew H. MacKenzie
Venable LLP

Sheena Thomas
Venable LLP

Tara Sugiyama Potashnik
Venable LLP

Automating Threat Sharing: How Companies Can Best Ensure Liability Protection When Sharing Cyber Threat Information With Other Companies or Organizations

Authors
Ari Schwartz, Sejal C. Shah, Matthew H. MacKenzie, Sheena Thomas, Tara Sugiyama Potashnik, and Bri Law

AUTOMATING THREAT SHARING: HOW COMPANIES CAN BEST ENSURE LIABILITY PROTECTION WHEN SHARING CYBER THREAT INFORMATION WITH OTHER COMPANIES OR ORGANIZATIONS

Ari Schwartz*
Sejal C. Shah**
Matthew H. MacKenzie***
Sheena Thomas****
Tara Sugiyama Potashnik*****
Bri Law******

This Article takes an in-depth look at the evolution of cybersecurity information sharing legislation, leading to the recent passage of the Cybersecurity Information Sharing Act (CISA) and offers insights into how automated information sharing mechanisms and associated requirements implemented pursuant to CISA can be leveraged to help ensure liability protections when engaging in cyber threat information sharing with and amongst other non-federal government entities.

INTRODUCTION

For several years on Capitol Hill, cybersecurity policy became synonymous with liability protection for cyber threat information sharing. While it is clear now—and was clear to many of us at the time—that information sharing is only a small part of the long-term management solution for ongoing cybersecurity threats, it was treated as almost a panacea. On the other hand, privacy and open Internet groups reacted with great concern to almost any proposal to address cyber threat information sharing. In some cases that level of concern was clearly warranted, but in others it seemed that

* Managing Director of Cybersecurity Services, Venable LLP; former Special Assistant to the President and Senior Director for Cybersecurity, National Security Council, the White House; Brandeis University, B.A. 1993. The Authors would like to thank Diana Carr, Megan Stifel, and Peri Tennenbaum.

** Counsel, Venable LLP; American University, Washington College of Law, J.D. 2004; American University, Kogod School of Business, M.B.A. 2006; New York University, B.A. 2000.

*** Associate, Venable LLP; University of Maryland School of Law, J.D. 2011; Davidson College, B.A. 2006.

**** Associate, Venable LLP; Cornell Law School, J.D. 2015; Wellesley College, B.A. 2010.

***** Counsel, Venable LLP; University of Michigan Law School, J.D. 2007 and former Managing Editor, University of Michigan Journal of Law Reform; Yale University, B.A. 2002.

******Cybersecurity Services Analyst, Venable LLP; University of California, Santa Barbara, B.A. 2007.

such groups would not support any solution seeking to minimize liability, even with strong privacy protections in place.

The Cybersecurity Information Sharing Act ("CISA"), which was signed into law in 2015, like much legislation, was a compromise that addressed the main concerns of all sides but left open many questions for implementation. In its guidance, the Department of Homeland Security ("DHS"), working with the Department of Justice ("DOJ"), decided to focus on the major goal of the legislation, promoting the automated sharing of threat information. This decision helped clarify how information would be shared from the private sector to the government, but provided less guidance about how liability would work among private sector actors. A lack of clarity around liability protections for sharing potentially private or confidential information and antitrust concerns among competing businesses led the call for legislation.[1]

For organizations looking to engage in business-to-business cyber threat information sharing, CISA and its guidance offer liability protections in a way that protects privacy. However, it takes some interpretation and an understanding of the law's history to fully grasp how best to take advantage of the provisions that promote information sharing.

In this Article, we offer suggestions for how organizations can engage in greater automated sharing by offering a window into the law, its guidance, and legislative history. Part I of this Article provides a historical overview of the evolution and development of cyber threat information sharing legislation, including the recent passage of CISA. Part II discusses the Structured Threat Information eXpression (STIX) and the Trusted Automated Exchange of Indicator Information (TAXII) framework for cyber threat information sharing. Part III discusses the implementation of the DHS Automated Information Sharing (AIS) capability pursuant to CISA and its use of STIX/TAXII to facilitate cyber threat information sharing between the private sector and the federal government. Part IV examines the various CISA guidance documents issued by DHS and DOJ and suggests that private sector entities seeking to share cyber threat information with other private sector entities should develop processes that closely follow the DHS AIS STIX/TAXII framework in order to ensure that the liability protections provided under CISA attach with the information shared. This section also suggests that private entities that use STIX/TAXII alone

1. *See* David Navetta & Utsav Mathur, *Sharing Cyber Threat Information: A Legal Perspective,* ISSA J. (Jan. 2015), http://www.dataprotectionreport.com/wp-content/uploads/sites/489/2015/01/Sharing-Cyber-Threat-Information_ISSAS0115.pdf.

without using the AIS limitations to share covered information may not enjoy the same liability protections.

I. HISTORY

A. Obama Administration 2011 Cybersecurity Legislative Proposal

In the years preceding, and into the Obama administration, the number of cyber threats and cyber incidents affecting the public and private sectors continued to rise significantly. To address this growing problem, U.S. Senate Majority Leader Harry Reid and six U.S. Senate committee chairs asked President Barack Obama to provide input on the direction of cybersecurity legislation in 2011.[2] At that point, approximately fifty cyber-related bills had been introduced in the last session of Congress.[3] In May of the same year, the Obama administration released its Cybersecurity Legislative Proposal ("2011 Proposal").[4] The 2011 Proposal included a recommendation for legislation providing immunity from civil or criminal causes of action to businesses, states, and local governments that engage in voluntary cyber threat information sharing with the federal government within certain parameters.[5]

1. Information Sharing and Liability Protection

The 2011 Proposal included a provision that would limit the liability for businesses that disclose any communication, record, or other information that they lawfully obtain with a designated office within the federal government, so long as the records were shared

2. Press Release, White House Office of the Press Sec'y, Fact Sheet: Cybersecurity Legislative Proposal (May 12, 2011), https://obamawhitehouse.archives.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

3. *Id.*

4. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, LEGISLATIVE LANGUAGE: DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AUTHORITY AND INFORMATION SHARING (2011), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/dhs-cybersecurity-authority.pdf [hereinafter 2011 PROPOSAL]; *see also* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, LEGISLATIVE LANGUAGE: COMPLETE CYBERSECURITY PROPOSAL (2011), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf (The complete legislative proposal addressing several additional topic areas).

5. 2011 PROPOSAL, *supra* note 4, § 246.

for the purpose of protecting information systems from cybersecurity threats[6] and the business sharing such records removed any personal information before sharing the records with the federal government.[7] This type of information sharing was relatively common prior to 2011, but many businesses were not participating because of liability concerns.[8] It was within this construct that the 2011 Proposal included a provision that protected businesses that shared records with the federal government from civil and criminal liability.[9] This liability protection extended to instances of good faith reliance on the proposed legislation's authorization to share cyber threat information with the federal government or a good faith determination that the proposed legislation permitted the conduct at issue.[10] The 2011 Proposal also included a provision that would authorize government agencies to share cyber threat information within the agency, with the designated office for cyber threat information sharing, and with certain private entities.[11]

2. Privacy Protections

The 2011 Proposal also addressed the protection of individual privacy in two ways. First, it required businesses and state or local governments that shared cyber threat information to remove personal information from any records before sharing them with the federal government. Additionally, the 2011 Proposal required the federal government to develop and review policies and procedures

---

6. The proposal defined a cybersecurity threat as "any action that may result in unauthorized access to, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information stored on or transiting an information system, or unauthorized exfiltration of information stored on or transiting an information system." *See* 2011 PROPOSAL, *supra* note 4, § 242(8).

7. 2011 PROPOSAL, *supra* note 4, § 245(a)(1).

8. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFF., GAO-04-780, CRITICAL INFRASTRUCTURE PROTECTION: IMPROVING INFORMATION SHARING AND INFRASTRUCTURE SECTORS (2004), http://www.gao.gov/assets/250/243318.pdf (describing information sharing in 2004).

9. 2011 PROPOSAL, *supra* note 4, § 246.

10. *Id.* at § 246(b).

11. The 2011 Proposal would have permitted government agencies to share cyber threat information with a private entity that is acting as a provider of electronic communication services, remote computing services, or cybersecurity services. The 2011 Proposal did not define "electronic communication services" or "remote computing services;" however, it defined "cybersecurity services" as "products, goods, or services used to detect or prevent activity intended to result in unauthorized access to, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information stored on or transiting an information system, or unauthorized exfiltration of information stored on or transiting an information system." 2011 PROPOSAL, *supra* note 4, 242(7).

"governing the acquisition, interception, retention, use, and disclosure"[12] of information that businesses or state and local governments share with it.[13] These policies and procedures would have to: (1) minimize the impact on privacy and civil liberties of sharing cybersecurity threats with the federal government; (2) reasonably limit the acquisition, interception, retention, use and disclosure of information related to cybersecurity threats; (3) include requirements for safeguarding information that can be used to identify specific individuals; and (4) protect the confidentiality of information associated with specific individuals to the extent possible while also informing the recipients of cyber threat information that the disclosed information may only be used for the specific purpose of protecting against or mitigating cybersecurity threats or law enforcement purposes.[14]

3. Reactions

Industry was generally supportive of the 2011 Proposal. Many viewed the recommendations as an encouraging step towards creating uniform procedures for sharing cybersecurity threat indicators. However, the 2011 Proposal was criticized by both trade associations and privacy advocates.[15] The 2011 Proposal specifically provided for information sharing between private entities and the federal government, and between government entities, but did not address sharing between private entities.[16] Additionally, stakeholders were concerned about locating the cybersecurity "portal" within the federal government, as opposed to creating an independent, centralized entity to facilitate information sharing.[17] Privacy groups advocated that private network operators, not the federal government, should be responsible for monitoring and securing private sector systems.[18] In her testimony before Congress, Leslie Harris, President and CEO of the Center for Democracy and Technology

12. 2011 PROPOSAL, *supra* note 4, § 248(a).

13. *Id.*

14. *Id.* at §§ 248(a)(1)–(4). The 2011 proposal permitted sharing cybersecurity threat indicators with law enforcement "when the information was evidence of a crime that has been, is being, or is about to be committed."

15. *Cybersecurity: Innovative Solutions to Challenging Problems: Hearing Before the Subcomm. on Intellectual Prop., Competition & the Internet of the H. Comm. on the Judiciary,* 112th Cong. 56 (2011), (statement of Leslie Harris, President and CEO, Center for Democracy & Technology) https://judiciary.house.gov/_files/hearings/printers/112th/112-38_66541.PDF [hereinafter Harris, *Hearing*].

16. 2011 PROPOSAL, *supra* note 4, § 243(c).

17. *See* Harris, *Hearing, supra* note 15, at 61.

18. *Id.*

(CDT), explained that the proposal raised serious concerns. She noted that the privacy and civil liberties protections in the proposal were "weak and principally center[ed] on the purpose limitation: limiting information sharing to cybersecurity and law enforcement purposes."[19] She expressed concerns about DHS's level of discretion with respect to the privacy and civil liberties policies and procedures and noted that "there is no effective way for an aggrieved party to enforce compliance with the policies and procedures because there is no private right of action for violations."[20]

Additionally, there was substantial debate in Congress about the 2011 Proposal.[21] Several members of Congress advocated for including information sharing as part of a larger package of bills, rather than continuing to advance individual cybersecurity bills.[22] There was also no consensus in Congress regarding the most appropriate federal entity for asserting jurisdiction over information sharing.[23]

B. Cyber Intelligence Sharing and Protection Act (CISPA)

In November 2011, Representative Mike Rogers introduced H.R. 3523, the Cyber Intelligence Sharing and Protection Act (CISPA), with 112 cosponsors.[24] CISPA brought information sharing back to the forefront of cybersecurity legislation, aiming to facilitate and increase cyber intelligence information sharing by private and public entities.[25] CISPA was a proposed amendment to the National Security Act of 1947, and required the Director of National Intelligence to establish procedures to allow the intelligence community to share cyber threat intelligence with private sector entities and utilities and to encourage the sharing of cyber threat intelligence.[26]

---

19. *See* Harris, *Hearing*, *supra* note 15, at 62.

20. *Id.*

21. *See, e.g., Protecting Cyberspace: Assessing the White House Proposal: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 112th Cong. (2011), https://www.gpo.gov/fdsys/pkg/CHRG-112shrg67638/pdf/CHRG-112shrg67638.pdf.

22. *See id.* at 5 (statement by Sen. Susan Collins, member, S. Comm. on Homeland Sec. & Governmental Affairs).

23. *See generally Draft Legislative Proposal on Cybersecurity: Hearing Before the H. Subcomm. on Cybersecurity, Infrastructure Prot., and Sec. Technologies of the H. Comm. on Homeland Sec.*, 112th Cong. (2011), https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg74646/pdf/CHRG-112hhrg74646.pdf.

24. Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2011).

25. *See id.*

26. *Id.*

CISPA defined "cyber threat intelligence" as "information in the possession of an element of the intelligence community directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system network from efforts to degrade, disrupt, or destroy such system or network."[27] CISPA allowed "cybersecurity providers," with the express consent of the protected entity, to share cyber threat information with "any other entity designated by a protected entity" including the Federal Government.[28] Information shared with the government was to be provided to the National Cybersecurity and Communications Integration Center (NCCIC) within DHS.[29] Information shared with the NCCIC could be shared with other federal agencies or departments.[30] CISPA prohibited the federal government from using cyber threat information for regulatory purposes.[31] Furthermore, CISPA limited the government's use of cyber threat information to cybersecurity purposes, for the investigation and prosecution of cybersecurity crimes, protection against danger or serious physical threats of harm, and to protect national security.[32]

1. Privacy Group Concerns about CISPA

Most of industry actively supported CISPA.[33] In a letter to members of the U.S. House of Representatives, the U.S. Chamber of Commerce (speaking on behalf of a coalition of all of the industry groups that were in favor of the bill) expressed support for CISPA.[34] The coalition letter advocated for legislation that would put "timely, reliable, and actionable information into the hands of business owners and operators . . . while protecting privacy and civil liberties."[35]

---

27. *Id.* § 1104(f)(2).
28. *Id.* § 1104 (b)(1).
29. *See generally id.* § 1104(b).
30. *See generally id.* § 1104(b).
31. *See id.* § 1104(b)(2)(C)(iii).
32. *See id.* § 1104 (c)(1).
33. Coalition Letter from the U.S. Chamber of Commerce to Mike Rogers and C.A. Dutch Ruppersberger, Representatives, U.S. House of Representatives (Feb. 12, 2013), https://www.uschamber.com/letter/coalition-letter-regarding-cispa.
34. *Id.*
35. *Id.*

Privacy groups, while in favor of improving information sharing for cybersecurity purposes, had several concerns with CISPA.[36] The CDT was primarily concerned with (1) the broad definition of information that could be shared with the government; (2) the potential for the growth of government surveillance of private communications as a result of the bill's information sharing mechanisms; (3) the shift in control of government cybersecurity efforts from civilian agencies to military entities; and (4) the absence of any limitation on the government's use of information shared for cybersecurity purposes.[37] A coalition of privacy groups, including New America Foundation's Open Technology Institute and the Electronic Frontier Foundation, among many others, urged Congress to vote "no" on CISPA, noting many of the same concerns as CDT.[38]

2. Statement of Administration Policy on CISPA

On April 25, 2012, the Obama administration released a Statement of Administration Policy, which explained that the administration strongly opposed CISPA and that senior advisors would recommend that the President veto the bill if presented to him.[39] The Statement of Administration Policy noted that CISPA did not adequately protect privacy, confidentiality, and civil liberties.[40] Unlike the 2011 Proposal, CISPA would have allowed broad sharing of cybersecurity information with the federal government without establishing requirements to promote minimization and to protect personally identifiable information.[41] The Statement of Administration Policy also noted that CISPA failed to establish sufficient limitations on the sharing of personally identifiable information between private entities and that it did not establish adequate oversight or accountability measures to ensure that cyber

36. Greg Nojeim, *Cyber Intelligence Bill Threatens Privacy and Civilian Control*, CTR. FOR DEMOCRACY & TECH. BLOG (Dec. 1, 2011) https://cdt.org/blog/cyber-intelligence-bill-threatens-privacy-and-civilian-control/.

37. *Id.*

38. Coalition Letter from ACLU et al., to Members of the U.S. House of Representatives (Apr. 26, 2012), https://www.aclu.org/sites/default/files/field_document/coalition_letter_strongly_urging_no_vote_on_h_r__3523-cispa_-_4_26_12.pdf.

39. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY: H.R. 3523—CYBER INTELLIGENCE SHARING AND PROTECTION ACT (2012), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/sap/112/saphr3523r_20120425.pdf.

40. *Id.*

41. *Id.*

threat information is used exclusively for appropriate purposes.[42] The House passed CISPA in April 2012, but the Senate did not. CISPA was reintroduced in the following Congress as H.R. 624.[43] Again, the House passed the bill in April 2013, but the Senate failed to advance similar legislation. In January 2015, CISPA was again reintroduced in the House, but ultimately failed to pass.[44]

C. Executive Order 13636

In February 2013, recognizing a lack of progress in Congress, President Obama issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity.[45] Regarding cybersecurity information sharing, E.O. 13636 contains a provision that requires the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence to issue instructions "to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a targeted entity."[46] E.O. 13636 also requires the Attorney General to establish a process for disseminating cyber threat information, including "the dissemination of classified reports to critical infrastructure entities authorized to receive them."[47] Additionally, E.O. 13636 requires the Secretary of Homeland Security and the Attorney General to work with the Director of National Intelligence to establish a system for tracking these reports.[48]

E.O. 13636 requires the expansion of the Enhanced Cybersecurity Services program to all critical infrastructure sectors.[49] The Enhanced Cybersecurity Services program is a voluntary information sharing program created to provide "classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure."[50] E.O. 13636 also requires that government agencies incorporate privacy and civil

42. *Id.*

43. H.R. Res. 624, 113th Cong. (2013).

44. H.R. 234, 114th Cong. (2015).

45. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

46. *Id.*

47. *Id.*

48. *Id.*

49. *Id.*

50. *Id.*

liberty protections into information sharing activities.[51] Such protections should be based on the Fair Information Practice Principles and other privacy and civil liberty frameworks.[52]

D. Cybersecurity Information Sharing Act

E.O. 13636 focused on interagency sharing but did not fully address issues regarding private sector information sharing with the government.[53] Following E.O. 13636, Senate Intelligence Committee Chairman Richard Burr and Vice Chairman Dianne Feinstein introduced the Cybersecurity Information Sharing Act (CISA) in the Senate on July 10, 2014.[54] CISA required the Director of National Intelligence, the Department of Defense, and the Department of Justice to develop procedures to promote the timely sharing of cyber threat indicators with private entities, non-federal government agencies, state, tribal, and local governments, the public, and entities under threat.[55]

CISA permitted private entities to monitor and operate defensive measures to detect, prevent, or mitigate cybersecurity threats or security vulnerabilities on: (1) their own information systems; and (2) with authorization and written consent, the information systems of other private or government entities.[56] To protect unauthorized access and address privacy concerns, CISA required the federal government and entities monitoring, operating, or sharing indicators or defensive measures to use security controls to protect against unauthorized access or acquisition and to remove personal information identifying a specific person not directly related to a cybersecurity threat.[57]

CISA directed DHS to develop a process for real-time automated cyber threat indicator and defensive measure information sharing.[58] Indicators and defensive measures shared under CISA could be used to: (1) protect a system or information from a cybersecurity

---

51. *Id.*

52. *Id.* The Fair Information Practice Principles are privacy standards for commercial websites that collect personal information from or about consumers. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., MEMORANDUM NO. 2008-01, PRIVACY POLICY GUIDANCE MEMORANDUM (2008), https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

53. Due to the limited scope of an executive order, solutions for addressing private sharing with government would have to rely on legislation.

54. S. 2588, 113th Cong. (2014).

55. *Id.* § 3(a).

56. *Id.* § 4(a)(1).

57. *Id.* § 4(d)(2).

58. *Id.* § 7(a)(2)(B).

threat or security vulnerability; (2) respond to or mitigate a serious threat of harm; (3) prevent or investigate a serious threat of harm; and (4) to identify the use of an information system by a foreign adversary or terrorist.[59] CISA also directed DOJ to develop guidelines to assist entities in sharing indicators with the federal government, including guidance for identifying and protecting personal information.[60] The DOJ was required to establish privacy and civil liberties guidelines to limit receipt, retention, use, and dissemination of personal or identifying information.[61] The information sharing provisions under CISA were voluntary.[62] The government could not require an entity to provide information to the government.[63] Entities that monitored information systems or decided to share or receive indicators or defensive measures were afforded liability protections as long as the information was shared in accordance with the procedures set forth by DHS.[64]

Similar in scope and intent to the 2011 Proposal, CISA received broad support from much of the business community and trade associations.[65] The U.S. Chamber of Commerce expressed strong support for the bill, stating that companies need legal certainty to promote the sharing of cyber threat information.[66] The Chamber of Commerce viewed CISA as establishing this legal certainty while still protecting individual privacy interests.[67] Opposition to CISA came from privacy groups and tech companies who expressed concerns

59. *See id.*

60. *Id.* § 5(b)(2)(C).

61. *Id.* § 5(d)(5)(C).

62. *Id.* § 8(h).

63. *Id.* § 8(f).

64. *Id.* § 6(a).

65. *See, e.g.*, Press Release, Am. Bankers Ass'n, ABA Statement on Senate Passage of Cybersecurity Information Sharing Act (Oct. 27, 2015), http://www.aba.com/press/pages/102715cybersecuritystatement.aspx; Press Release, Fin. Services Roundtable, FSR Lauds House on Passage of Critically-Needed Cyber Threat Info Sharing Bill (Apr. 23, 2015), http://fsroundtable.org/fsr-lauds-house-on-passage-of-critically-needed-cyber-threat-info-sharing-bills/; Press Release, Large Pub. Power Council, The Electric Power Sector Supports S. 754, the Cybersecurity Information Sharing Act (CISA) and Opposes Weakening Amendments (Dec. 2015), http://www.lppc.org/wp-content/uploads/2015/12/Electronic-Power-Sector-Support-of-S.-754.pdf; Letter from the Protecting Am.'s Cyber Networks Coal. to the Members of the U.S. Senate (Oct. 19, 2015), https://www.uschamber.com/sites/default/files/documents/files/10.19.15_coalition_s754_cisa_senate.pdf; Letter from the U.S. Chamber of Commerce to the Members of the U.S. Senate (Oct. 22, 2015), https://www.uschamber.com/sites/default/files/documents/files/10.22.15.kv_.s754.cisa_.senate.pdf.

66. Letter from the U.S. Chamber of Commerce to the Members of the U.S. Senate (Oct. 22, 2015), https://www.uschamber.com/sites/default/files/documents/files/10.22.15.kv_.s754.cisa_.senate.pdf.

67. *Id.*

about sharing information with the government.[68] These organizations expressed concern that the information shared with the government could be used to conduct surveillance on individuals, that the bill imposed inadequate use limitations on the government, and that the bill failed to protect personally identifiable information.[69]

E. Obama Administration 2015 Cybersecurity Legislative Proposal

Thereafter, in January 2015, the Obama administration updated its 2011 Cybersecurity Legislative Proposal. The 2015 Cybersecurity Legislative Proposal ("2015 Proposal") called for the creation of "mechanisms for enabling cybersecurity information sharing between private and government entities, as well as among private entities."[70] The 2015 Proposal suggested authorizing private entities to disclose cyber threat indicators to private entities called information sharing and analysis organizations (ISAO), the NCCIC, and law enforcement in conjunction with an investigation.[71] Under the provisions of the 2015 Proposal, the Secretary of Homeland Security, along with the Secretary of Commerce, the Attorney General, the Director of the Office of Management and Budget, and other agency leaders were to select a private entity to identify or develop a "common set of best practices for the creation and operation of private information sharing and analysis organizations."[72]

With respect to the use and protection of information, under the 2015 Proposal, private entities: (1) could use, retain, or further disclose cyber threat indicators solely for the purpose of protecting an information system; (2) were required to take reasonable steps to minimize information that could be used to identify specific individuals and reasonably believed to be unrelated to a cyber threat,

---

68. Letter from the Ctr. for Democracy & Tech. to the Members of the U.S. Senate Select Comm. on Intelligence (June 26, 2014), https://cdt.org/files/2014/06/CISA-Letter-62614.pdf; Press Release, Comput. & Commc'n Indust. Ass'n, CCIA Urges Senate to Improve Cybersecurity Information Sharing Act, http://www.ccianet.org/2015/10/ccia-urges-senate-to-improve-cybersecurity-information-sharing-act/.

69. *Id.*

70. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, LEGISLATIVE PROPOSAL: UPDATED DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AUTHORITY AND INFORMATION SHARING (2015), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/updated-information-sharing-legislative-proposal.pdf [hereinafter 2015 PROPOSAL]. The 2015 Proposal differed from CISA because of its focus on sharing information through information sharing and analysis organizations. CISA allowed companies to share information without becoming an information sharing organization.

71. *See id.* at §§ 103(a)–(b).

72. *Id.* at § 104(a).

and to safeguard information that could be used to identify specific individuals from unintended disclosure and unauthorized access; and (3) were required to comply with reasonable restrictions on subsequent disclosure or retention of cyber threat indicators disclosed to other private entities.[73]

Importantly, the 2015 Proposal designated the NCCIC to receive and distribute cyber threat indicators from the civilian portal as well as from federal agencies in as close to real time as possible.[74] The 2015 Proposal required the Secretary of Homeland Security and the Director of the National Institute for Standards and Technology to "develop a program that supports and rapidly advances the development, adoption and implementation of automated mechanisms for the real time sharing of cyber threat indicators."[75] The real-time sharing provision also provided that, to the extent feasible, the Secretary of Homeland Security would "ensure that the program relies on open source software development best practices."[76]

The 2015 Proposal also included increased privacy and civil liberty safeguards, as well as provisions protecting entities from civil and criminal liability. The legislative proposal exempted all entities from civil or criminal causes of action for voluntarily disclosing or receiving a cyber threat indicator consistent with the information sharing requirements.[77] With respect to privacy and civil liberties, the Attorney General was directed to work with various agencies to develop policies and procedures governing the receipt, retention, use, and disclosure of cyber threat indicators.[78] The policies and procedures were to: (1) limit the acquisition, interception, retention, use and disclosure of cyber threat indicators that are likely to be linked to specific individuals; and (2) establish public guidelines to allow law enforcement to use threat indicators for limited purposes.[79]

Stakeholders generally supported the recommendations set forth in the 2015 Proposal.[80] The 2015 Proposal promoted information sharing through organizations rather than directly through the federal government, relieving fears about the government's access to

73. *Id.* at § 103(c).

74. *Id.* at § 105(a)–(b).

75. *Id.* at § 105(c).

76. *Id.*

77. *Id.* at § 106.

78. *Id.* at § 107.

79. *Id.*

80. Aaron Boyd, *Industry Backing Obama's Cybersecurity Agenda*, FED. TIMES, (Jan. 19, 2015), http://www.federaltimes.com/story/government/cybersecurity/2015/01/19/industry-obama-cybersecurity-legislative-agenda/21994717/.

information.[81] Companies were in favor of sharing information with each other in order to improve the cybersecurity of all.[82]

F. Executive Order 13691

Building upon the foundation established in E.O. 13636 and other administrative documents, in February 2015 President Obama issued Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing (E.O. 13691), encouraging the development of ISAOs.[83] E.O. 13691 provides that ISAO membership can be based on a variety of factors, including sector, subsector, region, or any other affinity, as well as in response to particular emerging threats or vulnerabilities.[84] Additionally, according to E.O. 13691, an ISAO member may be a member of the public or private sector, and may be formed as a for-profit or nonprofit entity.[85] E.O. 13691 directs the NCCIC to coordinate with ISAOs for sharing cybersecurity risks and incident information.[86]

E.O. 13691 directs the Secretary of Homeland Security and other federal entities to work with a nongovernmental organization to serve as the ISAO Standards Organization (SO).[87] The SO would identify a "common set of voluntary standards or guidelines for the creation and functioning of ISAOs."[88] The standards would "further the goal of creating robust information sharing related to cybersecurity risks and incidents with ISAOs and among ISAOs to create deeper and broader networks of information sharing nationally, and to foster the development and adoption of automated mechanisms for the sharing of information."[89] E.O. 13691 explains that the standards must address, but are not limited to, "contractual agreements, business processes, operating procedures, technical means, and privacy protections such as minimization for ISAO operation and ISAO member participation."[90] In accordance with E.O. 13691, DHS selected the University of Texas at San Antonio to

81. *See* 2015 Proposal, supra note 70.
82. *See supra* note 76.
83. Exec. Order No. 13,691, 80 Fed. Reg. 9,349 (Feb. 20, 2015).
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.* at 9,350.
88. *Id.*
89. *Id.*
90. *Id.*

serve the function of the SO with support from the Logistics Management Institute.[91]

G. Passage of CISA

Finally, on December 18, 2015, Congress enacted CISA as part of the Cybersecurity Act of 2015.[92] As enacted, CISA was not significantly different from the proposed 2014 bill, which facilitated private information sharing. CISA authorizes private entities to monitor their own information systems[93] and the information systems of other entities with the permission of the entity that owns the information system.[94] The statute also authorized private entities to use defensive measures to protect its own information system or information systems belonging to other entities with the permission of the other entity.[95] CISA further authorizes private entities to share cyber threat indicators[96] and defensive measures[97] with, or receive such information from, any other entity or the federal

91. Andy Ozment, *DHS Awards Grant for Creation of the Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)*, U.S. DEP'T OF HOMELAND SEC. BLOG (Sept. 3, 2015, 2:50 PM), https://www.dhs.gov/blog/2015/09/03/dhs-awards-grant-creation-information-sharing-and-analysis-organization-isao.

92. 6 U.S.C. §§ 1501–10 (2012).

93. Information system means "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, including industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers." 6 U.S.C. § 1501(9).

94. 6 U.S.C. § 1503(a) (2012).

95. 6 U.S.C. § 1503(b) (2012).

96. Cyber Threat Indicators means "information that is necessary to describe or identify: (A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability; (B) a method of defeating a security control or exploitation of a security vulnerability; (C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability; (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability; (E) malicious cyber command and control; (F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; (G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or (H) any combination thereof." 6 U.S.C. § 1501(6) (2012).

97. Defensive Measure means "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability." 6 U.S.C. § 1501(7) (2012).

government, so long as such sharing is for a cybersecurity purpose.[98]

However, CISA places certain requirements on entities that participate in the sharing of cyber threat indicators and defensive measures.[99] First, CISA requires that information sharing entities implement appropriate security controls to protect the cyber threat indicators and defensive measures that they share or receive from unauthorized access or acquisition.[100] Second, CISA requires that, prior to sharing any cyber threat indicator or defensive measure, participating entities must remove any personal information that is not directly related to a cybersecurity threat.[101] Third, CISA requires that participating entities that share cyber threat indicators or defensive measures with the federal government must do so using a DHS-certified sharing mechanism in order to benefit from the statute's liability protection.[102] While the statute shields private entities from liability for the purposes of sharing cyber threat information, it does not protect against all causes of action. Once an entity shares information through the DHS capability, however, other federal entities may then communicate with the non-federal entity regarding that specific information without losing liability protection.[103]

In addition to protection from liability for any cause of action arising from the monitoring of information systems and the sharing or receipt of cyber threat indicators, CISA also provides a number of other protections, including exemptions from: (1) federal antitrust laws; (2) federal and state disclosure laws; (3) use by any federal, state, tribal, or local government for the purpose of regulating a private entity; (4) waiver of any applicable privilege; and (5) the rules of any federal agency pertaining to ex parte communications.[104] CISA also permits participating entities to designate shared information as commercial, financial, and proprietary.[105]

---

98. Cybersecurity Purpose means "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability." 6 U.S.C. § 1501(4) (2012). A "cybersecurity threat" is "an action, not protected by the First Amendment . . . , on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system." 6 U.S.C. § 1501(5) (2012).

99. 6 U.S.C. § 1503(d) (2012).

100. 6 U.S.C. § 1503(d)(1) (2012).

101. 6 U.S.C. § 1503(d)(2) (2012).

102. 6 U.S.C. § 1505 (2012).

103. 6 U.S.C. § 1504 (2012).

104. 6 U.S.C. § 1503 (2012).

105. 6 U.S.C. § 1504(d)(2) (2012).

II. STRUCTURED THREAT INFORMATION EXPRESSION AND TRUSTED AUTOMATED EXCHANGE OF INDICATOR INFORMATION (STIX AND TAXII)

One of the seemingly intentional goals of the legislation was to increase automated information sharing, both by requiring DHS to build an "automated process" to share information with other agencies and to accept and share information in an automated manner, and requiring an automated privacy scrub of the information shared by the private sector.[106] Automation allowed entities to share and act upon an exponentially greater amount of threat information while compensating for the shortage of staff available to process the information. In order to ensure that automated processing of information could happen in real time, DHS needed to select a technical standard by which it would receive this information and share it through information sharing organizations. The standard DHS chose to define cyber threat information is called Structured Threat Information eXpression ("STIX"); its counterpart for exchanging information is known as Trusted Automated Exchange of Indicator Information ("TAXII").[107]

Prior to the development of STIX and TAXII, entities that shared cyber threat indicators generally shared this information from person to person, rather than machine to machine, and only shared a limited amount of information within specific communities or using specific technology.[108] Human-to-human sharing can be time consuming, involving manual sharing processes and requiring translation of threat information into a variety of formats.[109] Such sharing has also frequently involved the use of insecure transmission methods.[110] Where machine-to-machine sharing was being used, it was limited to relatively specific indicators, such as IP addresses, without sufficient context for an entity to take effective action.[111] STIX and TAXII grew out of a perceived need within the cybersecurity community for greater structure and uniformity around the sharing of cyber threat indicators to allow such sharing

106. 6 U.S.C. § 1504(d)(5)(C) (2012).

107. *Information Sharing Specifications for Cybersecurity*, U.S. COMPUT. EMERGENCY READINESS TEAM, https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity (last visited Apr. 9, 2017).

108. JULIE CONNOLLY ET AL., MITRE CORP., THE TRUSTED AUTOMATED EXCHANGE OF INDICATOR INFORMATION 10 (2012) https://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_November_2012.pdf [hereinafter TAXII TECHNICAL PAPER].

109. *Id.*

110. *Id.*

111. *Id.*

to include a broader set of information and to enable distribution across industry sectors and product boundaries.[112]

Beginning in 2012, DHS engaged the broader cybersecurity community through the Homeland Security Systems Engineering & Development Institute operated by the MITRE Corporation to develop the necessary tools to facilitate broader sharing of cyber threat indicators.[113] Out of this effort, DHS established STIX and TAXII for machine-to-machine communication and transmission of cyber threat information.[114] STIX is the structured language or format used to convey cyber threat information,[115] while TAXII is the standardized platform for the trusted exchange of such information.[116] In 2015, both STIX and TAXII were transitioned to OASIS, a nonprofit consortium that facilitates the development and adoption of open standards.[117] In this role, OASIS will continue to receive input from the cybersecurity community to further develop and refine the STIX and TAXII constructs.[118]

The development of STIX was guided by a set of principles, including: (1) expressivity; (2) integration; (3) flexibility; (4) extensibility; (5) automatability; and (6) readability.[119] Pursuant to these principles, DHS aimed to develop a language that would allow for the communication of a full range of cyber threat information; that would be both machine-readable to allow for automated sharing and human-readable so that security analysts could efficiently use the information; that integrated existing standards where possible;[120] and that allowed users to adopt only those portions of the language that they needed.[121] In short, DHS sought to

---

112. STIX/TAXII STANDARDS TRANSITION—FREQUENTLY ASKED QUESTIONS 1, https://stix-project.github.io/oasis-faq.pdf (last visited Apr. 9, 2017).

113. *See* TAXII TECHNICAL PAPER, *supra* note 108, at 1.

114. MITRE CORP., STANDARDIZING CYBER THREAT INTELLIGENCE INFORMATION WITH THE STRUCTURED INFORMATION EXPRESSION 1 (2012) https://www.mitre.org/sites/default/files/publications/stix.pdf [hereinafter STIX TECHNICAL PAPER].

115. *Id.*

116. *Id.*

117. STIX/TAXII STANDARDS TRANSITION—FREQUENTLY ASKED QUESTIONS, *supra* note 112, at 1.

118. *Id.*

119. *See* STIX TECHNICAL PAPER, *supra* note 114, at 8–10.

120. STIX incorporates Cyber Observable eXpression ("CybOX") to convey information about observables, it leverages Indicator Exchange eXpression ("IndEX") to convey information about indicators, and it incorporates Common Attack Pattern Enumeration and Classification ("CAPEC") and Malware Attribute Enumeration and Characterization ("MAEC") to convey information about tactics, techniques, and procedures. It also leverages existing standards for the communication of exploit targets, such as Common Vulnerabilities and Exposures ("CVE") and the Open Source Vulnerability Database ("OSVDB"). *Id.* at 11–14.

121. *Id.*

create a common language for relating a broad range of cyber threat information, such as cyber observables, indicators, incidents, tactics, techniques, and procedures, exploit targets, courses of action, campaigns, and cyber threat actors.[122]

TAXII defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organizations and product/service boundaries.[123] TAXII eliminates the need for custom sharing solutions with each sharing partner, and is designed to integrate into a variety of existing sharing models, including: (1) hub and spoke networks, (2) source/subscriber arrangements, and (3) peer-to-peer sharing.[124]

STIX/TAXII have seen broad adoption amongst businesses, ISAOs, and Information Sharing and Analysis Centers (ISAC).[125] Businesses, including BrightPoint Security, IBM, Microsoft, Intel, Lockheed Martin, Palo Alto Networks, Inc., RSA Security, Hewlett Packard, and Soltra, have already integrated STIX/TAXII into their products.[126] Similarly, many ISAOs and ISACs have begun using STIX/TAXII, including the Defense Industrial Base ISAO, the Industrial Control System ISAO, the National Health ISAC, and the Retail ISAC.[127]

III. AUTOMATED INDICATOR SHARING

CISA provides that "[n]o cause of action shall lie" with respect to the sharing of cyber threat information through a DHS-certified sharing mechanism or capability that is otherwise consistent with the statute (i.e., for a cybersecurity purpose and void of personally identifiable information not directly related to the threat).[128] Accordingly, pursuant to Section 105(c) of the Act, DHS developed and certified the operation of a public and private sector sharing process for cyber threat indicators and defensive measures via the following methods: the Automated Indicator Sharing (AIS) initiative, a web form, email, and other DHS information sharing programs that use these means of receiving cyber threat indicators

122. *Id.*

123. *See Information Sharing Specifications for Cybersecurity*, *supra* note 107.

124. MARK DAVIDSON & CHARLES SCHMIDT, MITRE CORP., TAXII OVERVIEW: 1.1 3–4 (2014), https://taxiiproject.github.io/releases/1.1/TAXII_Overview.pdf.

125. *See STIX/TAXII Supporters List (Archive)*, STIX PROJECT DOCUMENTATION, http://stix-project.github.io/supporters/ (last visited Apr. 9, 2017).

126. *Id.*

127. *Id.*

128. 6 U.S.C. § 1505 (2012).

or defensive measures.[129] Non-federal entities may also share cyber threat indicators and defensive measures with federal entities through ISACs or ISAOs, which may share them with federal entities through DHS on their behalf.[130] Sharing through any of these means is eligible for liability protection; however, this Article focuses on the use of the AIS system and STIX/TAXII framework as a means of securing liability protection in the cyber threat information sharing context.

Managed by the NCCIC, AIS enables the timely exchange of cyber threat intelligence information—i.e., cyber threat indicators and defensive measures—between the federal government and the private sector by leveraging the STIX/TAXII specifications for machine-to-machine communications.[131] In short, as soon as a private company or federal agency observes a cyber threat, AIS allows for the bidirectional sharing of the cyber threat information in real time with all AIS participants, including the private sector, state, local, tribal, territorial governments, and the federal government.[132] The ultimate goal of AIS is to commoditize cyber threat information such that cyber threat indicators and defensive measures are shared broadly among the public and private sector, enabling everyone to better protect against cyber attacks.[133]

In order to receive, analyze, process, and disseminate cyber threat information in real time, AIS uses the STIX/TAXII specifications for the format and exchange of information.[134] AIS enables participants to share cyber threat information in a secure, anonymous,[135] and automated manner.[136] Accordingly, in order to

---

129. U.S. DEP'T OF HOMELAND SEC. & U.S. DEP'T OF JUSTICE, 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 13–14 (2016), https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_(Sec%20105(a)).pdf [hereinafter GUIDANCE TO ASSIST NON-FEDERAL ENTITIES]

130. *Id.* at 14.

131. U.S. DEP'T OF HOMELAND SEC., *Automated Indicator Sharing (AIS)*, https://www.dhs.gov/ais (last updated June 21, 2016). DHS certified the deployment of its AIS capability for cyber threat information sharing on March 17, 2016. *DHS "Open for Business" to Receive Cyber Threat Indicators at Machine Speed*, U.S. DEP'T OF HOMELAND SEC. BLOG (Mar. 17, 2016, 5:15 PM), https://www.dhs.gov/blog/2016/03/17/dhs-open-business-receive-cyber-threat-indicators-machine-speed.

132. *Id.*

133. *Id.*

134. *Automated Indicator Sharing (AIS)*, U.S. DEP'T OF HOMELAND SEC., https://www.us-cert.gov/sites/default/files/ais_files/AIS_fact_sheet.pdf.

135. Participants who share indicators through AIS are not identified as the source of the information to other participants unless they affirmatively consent to the disclosure of their identity.

136. *See* GUIDANCE TO ASSIST NON-FEDERAL ENTITIES, *supra* note 129, at 14.

directly participate in the real-time sharing capability of AIS, participants need to acquire their own TAXII client to communicate with the DHS TAXII server and submit information in conformance with the AIS STIX Profile as discussed in detail below.[137]

AIS participants are also required to follow the AIS Terms of Use[138] and DHS submission guidance[139] that outlines the type of information that should and should not be provided when submitting cyber threat indicators or defensive measures through AIS.[140] Specifically, information provided must not contain any personally identifiable information (PII) unless it is directly related to the cybersecurity threat.[141] Accordingly, DHS uses the AIS STIX Profile[142] to standardize the indicator and defensive measure information and implement a series of automated and manual processes to ensure that PII is removed from the cyber threat indicator or defensive measure before it is disseminated, thereby minimizing privacy, civil liberty, and other concerns that may arise when PII and other sensitive information is submitted.[143]

The AIS STIX Profile limits the information that can be disclosed when sharing a cyber threat indicator or defensive measure by removing the STIX fields that could contain PII.[144] STIX includes more than 2,750 fields that can be used to convey information about cyber threat indicators; however, the AIS profile includes only 364 of these fields.[145] Limiting the number of available fields reduces the risk that PII will be disclosed and ensures a level of predictability in the AIS submission content, such that automated controls can be used to further screen the submission.[146]

Once the information is received, AIS performs a series of automated analyses to ensure that the information within the data fields

---

137. *Id.*

138. U.S. DEPARTMENT OF HOMELAND SECURITY AUTOMATED INDICATOR SHARING TERMS OF USE, U.S. DEP'T OF HOMELAND SEC., https://www.us-cert.gov/sites/default/files/ais_files/AIS_Terms_of_Use.pdf.

139. *See e.g.*, GUIDANCE TO ASSIST NON-FEDERAL ENTITIES, *supra* note 129, at 13–14.

140. *Id.*

141. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT STATEMENT FOR AUTOMATED INFORMATION SHARING (AIS) 2 (2016), https://www.us-cert.gov/sites/default/files/ais_files/PIA_NPPD-AIS.pdf [hereinafter AIS PRIVACY IMPACT STATEMENT].

142. *See generally AIS STIX Profile*, U.S. COMPUT. EMERGENCY READINESS TEAM (Dec. 30, 2016), https://www.us-cert.gov/sites/default/files/ais_files/AIS_Submission_Guidance_Appendix_A.pdf.

143. *See* AIS PRIVACY IMPACT STATEMENT, *supra* note 141, at 2.

144. *Id.* at 5 n.18.

145. *Id.*

146. *Id.* at 6.

meets certain predetermined criteria and does not contain unrelated PII.[147] These technical controls include, but are not limited to: schema restrictions, controlled vocabulary, regular expressions (i.e. pattern matching), known good values, and autogenerated text.[148] While the majority of AIS submissions are automatically processed, there are instances (e.g., an unrecognized value) where the particular field will be queued for human review.[149] In such cases, human analysts at the NCCIC review the information and determine the appropriate actions to be taken (e.g., verify there is no PII or manually delete identified PII).[150]

IV. CISA GUIDANCE

To facilitate the sharing of cyber threat indicators and defensive measures by private entities through AIS and other certified capabilities, CISA further required that the Attorney General and the Secretary of Homeland Security jointly develop guidelines for the sharing of such information with the federal government.[151] The statute required that the DOJ and DHS issue interim policies and procedures within sixty days of the statute's enactment and final guidelines within 180 days of enactment.[152] The DOJ and DHS issued their preliminary guidelines on February 16, 2016 and the final guidelines on June 15, 2016.[153] The guidelines included four documents: (1) the Operational Procedures,[154] (2) the Non-Federal Entity Sharing Guidance,[155] (3) the Federal Entity Sharing Guidance,[156] and (4) the Privacy and Civil Liberties Guidelines.[157] A

147. *Id.* at 5.
148. *Id.* at 6.
149. *Id.* at 7.
150. *Id.*
151. 6 U.S.C. § 1504 (2012).
152. 6 U.S.C. § 1504(a) (2012).
153. *Id.*
154. U.S. DEP'T OF HOMELAND SEC. & U.S. DEP'T OF JUSTICE, FINAL PROCEDURES RELATED TO THE RECEIPT OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT (2016), https://www.us-cert.gov/sites/default/files/ais_files/Operational_Procedures_%28105%28a%29%29.pdf.
155. GUIDANCE TO ASSIST NON-FEDERAL ENTITIES, *supra* note 129.
156. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE ET AL., SHARING CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 (2016), https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_%28103%29.pdf.
157. U.S. DEP'T OF HOMELAND SEC. & U.S. DEP'T OF JUSTICE, PRIVACY AND CIVIL LIBERTIES FINAL GUIDELINES: CYBERSECURITY INFORMATION SHARING ACT OF 2015 (2016), https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_%28Sec%20105%28b%29%29.pdf [hereinafter PRIVACY AND CIVIL LIBERTIES FINAL GUIDELINES].

significant public record has not yet developed regarding the reception of the guidelines by industry, however industry has spoken favorably about the guidelines.[158]

The Non-Federal Entity Sharing Guidance (Guidance) distinguishes the types of information that qualify as a cyber threat indicator under the Act and the types of information protected by otherwise applicable privacy laws.[159] The Guidance also explains how to identify and share cyber threat indicators and defensive measures with federal entities through the federal government capability and process operated by DHS.[160] The Guidance states that CISA promotes the sharing of cybersecurity information while protecting privacy by specifying the types of cyber threat indicators that can be shared and by limiting information sharing under the Act to only those circumstances in which the information is necessary to describe or identify threats to information and information systems.[161] The Guidance also provides a number of examples of information that would contain cyber threat indicators that a private entity could share with the federal government.[162] The Guidance further identifies a number of examples of defensive measures that a private entity could share under CISA,[163] as well as several types of information that are protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat, including protected health information, human resource information, and financial information, among others.[164] Finally, the Guidance explains how private entities must share cyber threat indicators and defensive measures with the federal government to take advantage of the liability protection made available by the statute.[165] Participation in AIS is not the only way for a private entity to be shielded from criminal and civil liability with respect to information sharing. However, the Guidance carefully avoids explaining the other ways to achieve liability protection beyond using AIS, presumably because DHS wants to promote AIS uptake.

---

158. *See* Notice of Public Workshop Regarding the Cybersecurity Information Sharing Act of 2015 Implementation, 81 Fed. Reg 32,340 (May 23, 2016).

159. GUIDANCE TO ASSIST NON-FEDERAL ENTITIES, *supra* note 129. The guidance provides several ways to share information. This paper is specifically focused on automated sharing.

160. *Id.* at 10.

161. *Id.* at 5.

162. *Id.* at 5–6.

163. *Id.* at 7.

164. *Id.* at 9–10.

165. *Id.* at 10.

The DOJ and DHS also issued guidelines pertaining to privacy and civil liberties (Guidelines) with respect to the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity.[166] The Guidelines state that cyber threat indicators provided to the federal government under CISA may be disclosed to, retained by, and used by any federal agency only for activities that have been authorized under the Act.[167] The Guidelines also provide that federal agencies must review cyber threat indicators before sharing them to determine whether the indicator contains any information that is not directly related to a cybersecurity threat and that the agency knows, or has reason to know, is personal information.[168] The Guidelines also apply the Fair Information Practice Principles to the sharing of cyber threat indicators with the federal government.[169] The Guidelines further address destruction requirements, notification procedures, use restrictions, safeguards, and the dissemination of such information, as required by statute.[170]

Although the Guidance and Guidelines pertain to the sharing of cyber threat indicators and defensive measures with the federal government, they also provide helpful guidance for the sharing of such information between private entities. Importantly, the Guidelines clarify that private entities can receive liability protection when sharing cyber threat indicators and defensive measures with other private entities if they would receive such protection under CISA for sharing the same information with the federal government.[171] Therefore, so long as an entity complies with the requirements under CISA for obtaining liability protection, that entity is not limited with respect to whom can receive such information.

The Guidelines also provide a framework for how private entities should structure any arrangement to share covered information under CISA. Specifically, to take advantage of the liability protection afforded under the statute, private entities should share threat indicators and defensive measures using the AIS STIX Profile and TAXII. In adopting this approach, private entities can conclude that they are meeting CISA's requirements without performing a time-consuming, manual review of each submission before sharing it with other parties. To benefit from CISA's liability protection, private entities must not only engage in the types of sharing that are covered by the statute, but they also must review any information

166. PRIVACY AND CIVIL LIBERTIES FINAL GUIDELINES, *supra* note 157.
167. *Id.* at 10.
168. *Id.* at 12.
169. *Id.* at 4.
170. *Id.* at 7–12.
171. GUIDANCE TO ASSIST NON-FEDERAL ENTITIES, *supra* note 129, at 10 n.11.

that will be shared with other entities before sharing it and remove any information that is not directly related to a cybersecurity threat that the private entity knows is PII.

Implementing this review process to benefit from the statute's liability protection could significantly increase the level of effort that companies must invest to be able to share cyber threat indicators and defensive measures with other private entities. Employing a manual process to review information before sharing it with other parties would be both time consuming and could lead to mistakes that would result in an entity losing liability protection.

To efficiently share covered information without incurring liability, private entities should use the AIS STIX Profile to structure the information that they provide, and they should use TAXII to structure the transmission. Using the AIS STIX Profile will be particularly helpful because it will only allow the submission of information that DHS has already determined meets the statute's requirements for liability protection. Following this process will enable private entities to share covered information efficiently and confidently, while limiting any risk associated with such sharing. Conversely, when a private entity does not use AIS limitations to share covered information, that entity may not be protected from liability, even though the entity used STIX/TAXII. Under the Guidance, using STIX/TAXII alone is insufficient for a private entity to be protected from liability.

CONCLUSION

In their guidance, DHS and DOJ have provided a clear pathway for companies to obtain liability protection by utilizing certain STIX fields, set forward in AIS, when automating information sharing with the federal government. Because DHS and DOJ have made clear that the steps that apply to the government sharing also apply to private sector sharing, organizations may take comfort in knowing that limiting sharing to the AIS STIX fields will afford them a greater degree of liability protection. Organizations that decide not to utilize STIX to automate sharing may still use the AIS STIX Profile to map fields to help ensure that they are protecting privacy as the law requires. Organizations that take this approach may want to work with DHS to assure themselves that the resulting profile closely tracks to the AIS profile in order effectively to take advantage of the liability protections in the law when using automated sharing.