ALSTON&BIRD

CYBER ALERT

A Publication of the Cybersecurity Preparedness & Response Team

WWW.ALSTONPRIVACY.COM DECEMBER 23, 2015

The Cybersecurity Information Sharing Act Is Now Law

After years of vigorous debate and numerous bills aimed at incentivizing cyber threat intelligence sharing having failed to become law, on December 18, 2015, President Obama signed an omnibus spending bill containing the Cybersecurity Information Sharing Act of 2015 (CISA).[1] Passage of CISA is a major victory for cybersecurity proponents in Congress and the private sector, many of whom have called for information sharing legislation for years. It also constitutes the culmination of a year filled with cybersecurity policy developments, including a number of initiatives specifically aimed at information sharing.[2] Although CISA raises some significant privacy concerns, the final text contains a number of provisions aimed at minimizing the impact on privacy of cyber threat sharing both among private entities and with (and within) the federal government.

Passage of CISA is particularly important given the private sector's long-recognized reluctance to share cyber threat information due to legal concerns.[3] These include concerns regarding compliance with applicable privacy and antitrust laws, that shared information could be discoverable through a Freedom of Information Act (FOIA) request, that applicable legal privileges could be waived by sharing information and that sharing information could lead to regulatory action or civil liability. CISA largely addresses these concerns and is expected to lead to a significant increase in cyber threat sharing. At the same time, it requires entities that share information to take certain basic precautions—for instance, with regard to the removal of personal information from shared information—and generally requires that sharing activities be for cybersecurity purposes in order to take advantage of many of the legal protections offered.

Overview

Among other things, CISA generally authorizes (1) private entities to monitor their information systems (and those they are authorized to monitor)[4] and to operate defensive measures on the same for cybersecurity purposes;[5] (2) non-federal entities to share with, as well as receive from, other non-federal entities or the federal government

---

1 Consolidated Appropriations Act, 2016, H.R. 2029, 114th Cong., Division N, Title I (2015).

2 *See, e.g.*, Kim Peretti and Jason R. Wool, "An Evolving Path Forward: Recent Developments in Cybersecurity Information Sharing," *Alston & Bird Cyber Alert* (Mar. 17, 2015) (discussing passage of CISA by the Senate Intelligence Committee, as well as President Obama's February 2015 executive order on information sharing, the creation of the Cyber Threat Intelligence Integration Center, the White House's Summit on Cybersecurity and Consumer Protection, and the White House Legislative Framework for Information Sharing).

3 *See, e.g.*, Kim Peretti and Lou Dennig, *Cyber Threat Intelligence: To Share or Not to Share – What Are the Real Concerns?*, Bloomberg BNA Privacy & Security Law Report (Sept. 1, 2014).

4 *See* CISA at § 104(a).

5 *See id.* at § 104(b).

cyber threat indicators or defensive measures;[6] and (3) entities that receive cyber threat indicators or defensive measures to use them for cybersecurity purposes.[7] The statute also directs representatives of the federal government to develop and issue procedures to facilitate and promote the sharing of cyber threat indicators and defensive measures of varying levels of classification amongst various categories of federal and non-federal entities.[8] The term "cyber threat indicator" is defined with specificity and refers to information necessary to describe or identify a host of security-related activities.[9]

The statute also provides liability protections for private entities that (1) monitor information systems or (2) share or receive cyber threat indicators or defensive measures, provided that these activities are conducted "in accordance with" the Act.[10] Specifically, the statute provides that no cause of action shall lie or be maintained in any court against such entities. In order to receive liability protections for sharing with the federal government via email, electronic media, an interactive form on a website or a real time, automated process between information systems ("electronic means"), private entities must generally share the information with the Department of Homeland Security (DHS) through the process to be established by it, subject two exceptions.[11] CISA further provides that it should not be construed to create a duty to share cyber threat indicators or defensive measures or a duty to warn based on the receipt thereof.[12]

Cyber threat indicators and defensive measures shared with the federal government via electronic means must generally be submitted to DHS pursuant to a "capability and process" to be developed by the secretary of DHS within 90 days of enactment.[13] DHS must then send the cyber threat indicators and defensive measures to "appropriate federal entities"—defined as the Departments of Commerce, Defense, Energy, Homeland Security, Justice and Treasury and the Office of the Director of National Intelligence—in an automated manner and in near real time. Cyber threat indicators and defensive measures may then be disclosed to and used by federal agencies or departments for cybersecurity purposes and (1) to identify cybersecurity threats or security vulnerabilities; (2) to respond to or otherwise prevent or mitigate a specific threat of death, serious bodily harm or serious economic harm; (3) to respond to a serious threat to a minor, including sexual exploitation and threats to physical safety; or (4) to prevent, investigate, disrupt or prosecute certain specific crimes related to fraud, identity theft, espionage and trade secrets.[14] This provision is notable in that it makes clear the federal government is not limited

---

6 *See id*. at § 104(c).

7 *See id*. at § 104(d)(3).

8 *See id*. at § 103(a).

9 *See id*. at § 102(6).

10 *See* CISA at § 106(a), (b).

11 To gain liability protections, such sharing must be "in accordance with" Section 105(c)(1)(B), which generally requires sharing with the government through electronic means to be via DHS. However, that section also allows (1) "communications between a Federal entity and a non-Federal entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such a threat indicator" or (2) "communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat." The Senate Intelligence Committee's report on CISA also notes that the "sharing of cyber threat indicators and defensive measures in other formats where there is less privacy risk, such as a telephone call, letter, or in-person meeting, receives liability protection regardless of whether it is first sent through the DHS portal." S. Rep. No. 114-32, at 10 (2015).

12 *See* CISA at § 106(c).

13 *See id*. at § 105(c).

14 *See id*. at § 105(d)(5).

to using shared information for cybersecurity purposes. Policies and procedures to be developed jointly by DHS and the U.S. attorney general must provide for the existence of audit capabilities and appropriate sanctions for officers, employees or agents of federal entities that knowingly or willfully "conduct activities under this title in an unauthorized manner."[15]

Privacy and Civil Liberties Issues

CISA also includes a number of provisions intended to safeguard the privacy and civil liberties of individuals whose personal information may be shared pursuant to the statute. For instance, federal entities that share cyber threat indicators will be required to review the shared information prior to sharing it. They must then assess whether it contains any information not directly related to a cybersecurity threat that the entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual, and remove that information. This can be achieved through the use of a "technical capability."[16] The federal government is also required to notify individuals whose personal information is shared by a federal entity in violation of the statute.[17]

Non-federal entities that share cyber threat indicators must take similar precautions prior to sharing such information.[18] Each entity must review the indicators to assess whether they contain any information not directly related to a cybersecurity threat that the entity knows at the time of sharing to be personal (or identifying) information of a specific individual and remove it. Alternatively, the entity may employ a technical capability configured to remove such information. Regardless of which option private entities adopt, it will likely be important to establish a documented process and controls for this step of information sharing, as it could be the subject of debate in a lawsuit.

In addition, within 60 days of enactment, CISA directs the attorney general and the secretary of DHS to issue publicly available guidance on sharing cyber threat information with the federal government.[19] This guidance must, among other things, identify types of cyber threat indicators that would be unlikely to include information not directly related to cybersecurity threats and personal or otherwise identifying information of specific individuals. Further, the guidance must identify types of information that are protected under otherwise applicable privacy laws and that are unlikely to be directly related to a cybersecurity threat (e.g., protected health information).

CISA also directs the attorney general and secretary of DHS to jointly develop, submit to Congress and make publicly available guidelines for the program relating to privacy and civil liberties.[20] These guidelines will govern the federal government's receipt, retention, use and dissemination of cyber threat indicators, and must generally limit the effect on privacy and civil liberties caused by the government's activities under CISA consistent with the need to protect information systems from cybersecurity threats and to mitigate cybersecurity threats. CISA specifies a number of specific requirements aimed at achieving this goal, including the timely destruction of

---

15 *See id*. at § 105(a)(3)(C).

16 *See id*. at § 103(b)(1)(E).

17 *See id*. at § 103(b)(1)(F).

18 *See* CISA at § 104(d)(2).

19 *See id*. at § 105(a)(4).

20 *See id*. at § 105(b).

information containing personal information that is known not to directly relate to an authorized use under the statute, as well as safeguarding and protecting the confidentiality of threat indicators that are authorized but nonetheless contain personal information.

Other Key Features

By sharing information with the federal government, applicable privileges or other legal protections (such as trade secret protection) will not be waived.[21] The information is also exempted from disclosure under state, tribal, local and federal FOIA laws.[22] Subject to a limited exception, shared cyber threat indicators and defensive measures may not be used by any state, local, tribal or federal regulator to regulate the "lawful activities of any non-Federal entity," including via an enforcement action, pursuant to mandatory standards.[23]

Consistent with the policy statement on antitrust and cybersecurity information sharing issued by the Federal Trade Commission and Department of Justice (DOJ) in 2014, CISA also contains an antitrust exemption.[24] This provision provides that "it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator or defensive measure" for cybersecurity purposes under CISA.[25] The exemption applies only to information exchanged or assistance provided for specified cybersecurity purposes.

Finally, it is important to note that CISA's authorization to use defensive measures[26] does not authorize "hacking back" or other "offensive defenses," consistent with previous guidance issued by the DOJ warning against that practice.[27] CISA defines a defensive measure, in pertinent part, as an "an action, device, procedure, signature, technique, or other measure … that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability."[28] It specifically excludes from the definition a "measure that destroys, renders unusable, provides unauthorized access to, or substantially harms" an information system or data stored on one. Finally, in authorizing the use of defensive measures, the statute states that it "shall not be construed … to authorize the use of a defensive measure other than as provided in this subsection."[29]

---

21 *See id*. at § 105(d)(1).

22 *See id*. at § 105(d)(3).

23 *See id*. at § 105(d)(5)(D).

24 Maki DePalo, "DOJ and FTC Issue Antitrust Policy Statement on Cybersecurity Information Sharing," *Alston & Bird Privacy & Data Security Blog* (Apr. 11, 2014).

25 *See* CISA at § 104(e).

26 *See id*. at § 104(b).

27 *See* Jason R. Wool, "DOJ Issues Data Breach Guidance," *Alston & Bird Privacy & Data Security Blog* (Apr. 29, 2015).

28 *See* CISA at § 102(7).

29 *See id*. at § 104(b).

If you have any questions or would like additional information, please contact Kimberly Peretti, Jim Harvey or Jason Wool.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: **@AlstonPrivacy | www.AlstonPrivacy.com**