Clients&FriendsMemo

President Obama Signs Cybersecurity Act of 2015 to Encourage Cybersecurity Information Sharing

December 24, 2015

On December 18, 2015, President Obama signed into law a $1.1 trillion omnibus spending bill that contained the Cybersecurity Act of 2015 (the "Act"), a compromise bill based on competing cybersecurity information sharing bills that passed the House and Senate earlier this year. The Act creates a voluntary cybersecurity information sharing process designed to encourage public and private sector entities to share cyber threat information.[1]

Summary of Key Provisions

Although laws have long authorized the sharing of certain cybersecurity information, in practice there have been numerous obstacles impeding the effective exchange of information between and among the federal government and entities in the private sector. These include concerns about the possible public release through a public records request of data shared with the federal government, the privacy rights of individuals whose information may be included in information shared with the federal government, potential antitrust violations, and the use of shared information as evidence in regulatory enforcement actions against entities that have shared information with the federal government.[2]

The Cybersecurity Act of 2015 aims to address many of those concerns, creating a mechanism to facilitate and encourage information sharing between and among the federal government and

---

1 The Act also includes provisions to promote monitoring information systems and operating defensive measures for cybersecurity purposes, improve federal network and information system security, provide assessments on the federal cybersecurity workforce, and provide reporting and strategies on cybersecurity industry-related and criminal-related matters.

2 *See generally* Kimberly Peretti, *Cyber Threat Intelligence: To Share or Not to Share—What Are the Real Concerns?*, PRIVACY & SECURITY LAW REPORT (Sept. 2014); *Exchanging Cyber Threat Intelligence: There Has to Be a Better Way*, PONEMON INSTITUTE (Apr. 2014), *available at* http://content.internetidentity.com/acton/attachment/8504/f-001b/1/-/-/-/-/Ponemon%20Study.pdf; Andrew Nolan, *Cybersecurity and Information Sharing: Legal Challenges and Solutions*, CONG. RESEARCH SERV. (Mar. 16, 2015).

entities in the private sector.[3] Under the Act, the federal government is directed to create a process for sharing both classified and unclassified cyber threat indicators and defensive measures with the private sector, as well as information relating to certain cybersecurity threats and best practices.[4] Entities in the private sector, in turn, are afforded several protections when they share cybersecurity information in accordance with the Act. Under the Act's key information sharing provision, "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."[5]

The meaning of this provision hinges on how the key terms are defined. The following analysis clarifies the meaning of those terms to assess what information sharing will look like under the framework established by the Act.

What Information Can Be Shared?

The Cybersecurity Act of 2015 provides that "non-federal entit[ies]" – any person, private group, or state or local government – may share with the federal government both cyber threat indicators and defensive measures. A cyber threat indicator[6] includes information that is necessary to describe or identify attributes of a cybersecurity threat.[7] A defensive measure is broadly defined as "an action, device, procedure, signature, technique, or other measure" that "detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability."[8]

---

3 Specifically, the Act creates a framework for information sharing among the federal government and "non-Federal entit[ies]," which includes not only private entities but also non-federal government agencies or departments as well as state, tribal, and local governments. *See* Cybersecurity Act of 2015, § 102(14) [hereinafter Cybersecurity Act].

4 *See id.* at § 103.

5 Cybersecurity Act, § 104(c)(1).

6 *See id.* at § 102(6) ("The term 'cyber threat indicator' 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."). Many of these terms are further defined in the Act.

7 *See id.* at § 102(5) ("(A) In General.—Except as provided in subparagraph (B), the term 'cybersecurity threat' means an action, not protected by the First Amendment to the Constitution of the United States, 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. (B) Exclusion.—The term 'cybersecurity threat' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.").

8 Cybersecurity Act, § 102(7).

What Information Cannot Be Shared?

Under the Cybersecurity Act of 2015, the private sector may only share information that falls within the Act's definitions of cyber threat indicator or defensive measure. Prior to sharing a cyber threat indicator with the federal government, a private entity must remove certain personal information. Specifically, entities are required to remove information that the entity "knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual."[9]

With Whom Can Information Be Shared?

While the Department of Homeland Security is charged with developing the mechanism by which the federal government receives in real time cyber threat indicators and defensive measures shared by entities in the private sector,[10] that information is then shared "in an automated manner with all of the appropriate Federal entities," to include the Office of the Director of National Intelligence and the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury.[11] Moreover, the President may designate other federal entities in addition to the Department of Homeland Security, but not the Department of Defense, to develop and implement a similar capability and process for receiving in the first instance cyber threat indicators and defensive measures shared by entities in the private sector.[12]

What Can the Government Do With the Information?

The federal government is limited in its ability to disclose, retain, and use shared cybersecurity information. This information may be used solely for "a cybersecurity purpose,"[13] identifying cybersecurity threats or vulnerabilities, and in certain other law enforcement investigations related to a specific threat of death or serious bodily harm or a specific threat of serious economic harm, a serious threat to a minor, and certain specified offenses such as fraud and identity theft.[14] Federal agencies cannot release shared cybersecurity information, which the Act exempts from disclosure under the Freedom of Information Act.[15]

---

9 *Id.* at § 104(d)(2)(A).

10 *See id.* at § 105(c).

11 *Id.* at §§ 102(3), 105(a)(3)(A).

12 *Id.* at §105(c)(2)(B).

13 *Id.* at § 102(4) ("Cybersecurity purpose.—The term '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."). In addition, "[t]he term 'security vulnerability' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control." Cybersecurity Act, § 102(17).

14 *See* Cybersecurity Act, §105(d)(5).

15 *Id.* at § 105(d)(3).

How Does the Cybersecurity Act Promote Information Sharing?

Supporters of information sharing claim that increasing the flow of cybersecurity information between the federal government and private sector will improve the cybersecurity of all participants. While the prospect of a more secure cyberspace may be sufficient to motivate some private entities to share cyber threat indicators and defensive measures with the federal government, the Act provides certain assurances to entities in the private sector to encourage such sharing. In addition to the protection against public disclosure and the limitations on the federal government's use of shared information, the Act's principal incentive to encourage information sharing is liability protection for private entities that share information in accordance with the Act. Specifically, the Act provides that "[n]o 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 . . . [or] for the sharing or receipt of a cyber threat indicator or defensive measure."[16]

While the Cybersecurity Act of 2015 paves the way for entities to share cyber threat indicators with the federal government, details will be fleshed out in a series of implementing regulations and guidance intended to promote information sharing while protecting privacy and civil liberties, including publicly available guidance to be jointly developed by the Departments of Justice and Homeland Security.[17]

Reactions to the Legislation

Reaction to the Cybersecurity Act of 2015 has been decidedly mixed, with some privacy advocates characterizing it as a "thinly disguised surveillance provision . . . born of a climate of fear,"[18] while major business industry groups, such as the U.S. Chamber of Commerce, the Financial Services Roundtable, and the National Retail Federation expressed their support for its provisions.[19] Major tech companies, such as Apple, Twitter, and Yelp, as well as leading industry groups, such as the Computer and Communications Industry Association, had previously opposed the Senate's version

16 Cybersecurity Act, § 106(a)-(b).

17 *See id.* at § 105(a).

18 Jenna McLaughlin, *Hasty, Fearful Passage of Cybersecurity Bill Recalls Patriot Act*, THE INTERCEPT (Dec. 19, 2015, 11:05 AM), https://theintercept.com/2015/12/19/hasty-fearful-passage-of-cybersecurity-bill-recalls-patriot-act/.

19 *See, e.g.*, Press Release, National Retail Federation, Retailers Say Spending Plan Provides Broad Relief That Will Boost Economy (Dec. 18, 2015), *available at* https://nrf.com/media/press-releases/retailers-say-spending-plan-provides-broad-relief-will-boost-economy; Press Release, U.S. Chamber of Commerce, U.S. Chamber President Comments on Omnibus Spending Bill (Dec. 16, 2015), *available at* https://www.uschamber.com/press-release/us-chamber-president-comments-omnibus-spending-bill; Tim Starks, *Final Verdict on the Cybersecurity Bill*, POLITICO (Dec. 18, 2015, 10:00 AM), http://www.politico.com/tipsheets/morning-cybersecurity/2015/12/final-verdict-on-the-cybersecurity-bill-211837#ixzz3ugbTkYaf [hereinafter Starks, *Final Verdict on the Cybersecurity Bill*] (quoting Financial Services Roundtable Executive Vice President of Government Affairs Francis Creighton, who said, "It's as good a bill as Congress has passed this year" and described the Act as a "strong effort to make our systems a little bit safer").

of the bill, which passed in late October.[20] Even though some of these organizations' requested changes were incorporated into the final version of the bill, they ultimately did not support its passage, with some companies indicating that they will not participate in the sharing program.[21]

Implications and Takeaways

The Cybersecurity Act of 2015 – Congress's first major piece of cybersecurity legislation – has been years in the making. The Act's focus, however, is relatively modest, with one commentator calling information sharing "last decade's answer" to the cybersecurity problem.[22]

The law's provisions are voluntary in nature, and as such, businesses are under no obligation to share cyber threat indicators with the federal government or each other. The benefits of the bill's liability protection may also be somewhat overstated, at least with respect to information sharing among private entities. The recent proliferation of private sector information sharing organizations, such as Facebook's ThreatExchange, may suggest that companies are not especially concerned about potential liability arising from such sharing.[23] Indeed, the Act's antitrust liability protections probably are little more than a legislative formality, as the Department of Justice and Federal Trade Commission's joint Antitrust Policy Statement on Sharing of Cybersecurity Information made clear that the antitrust enforcement agencies "do not believe that antitrust is—or should be—a roadblock to legitimate cybersecurity information sharing" and provided guidelines on sharing such information without running afoul of the antitrust laws.[24] The Act's protection from liability for private entities when sharing cyber threat indicators or defensive measures with the federal government likely was unnecessary as well, as privacy experts and technologists have long argued that such indicators

---

20 *See* Cory Bennett, *Cybersecurity's Winners and Losers*, THE HILL (Dec. 19, 2015, 1:31 PM), http://thehill.com/policy/cybersecurity/263785-cybesecuritys-winners-and-losers [hereinafter Bennett, *Cybersecurity's Winners and Losers*]; Cory Bennett, *Major Tech Group Comes Out Against Cyber Bill*, THE HILL (Oct. 15, 2015, 12:34 PM), http://thehill.com/policy/cybersecurity/257029-major-tech-group-opposes-cyber-bill.

21 *See* Bennett, *Cybersecurity's Winners and Losers*, *supra* note 20.

22 Starks, *Final Verdict on the Cybersecurity Bill*, *supra* note 19.

23 *See* Steven Norton, *Facebook Says More Than 90 Companies Using Cybersecurity Information Sharing Platform*, CIO JOURNAL (Aug. 21, 2015, 6:16 PM), http://blogs.wsj.com/cio/2015/08/21/facebook-says-more-than-90-companies-using-cybersecurity-information-sharing-platform/.

24 For more information, see Jonathan Kanter, Kenneth Wainstein & Keith Gerver, *DOJ and FTC Release Joint Antitrust Policy Statement Regarding Sharing of Cybersecurity Information*, CADWALADER, WICKERSHAM & TAFT LLP (Apr. 15, 2014), http://www.cadwalader.com/resources/clients-friends-memos/doj-and-ftc-release-joint-antitrust-policy-statement-regarding-sharing-of-cybersecurity-information.

typically do not contain private data and are already being shared with the federal government in the case of a cyber attack.[25]

Although a limited measure, the Cybersecurity Act of 2015 should facilitate increased information sharing among private sector entities and between the private sector and the federal government, which will at least marginally improve the nation's cybersecurity. And while the Act provides for liability protection, private actors looking to share cyber threat indicators or other cyber-related information with each other or with the government should continue to consult counsel, especially when assessing how the Act's provisions interact with other federal and state laws and regulations regarding access to and use of proprietary or personally identifiable information.[26]

* * * *

If you have any questions, please contact any of the following attorneys or your Cadwalader contact:

Kenneth L. Wainstein	+1 202 862 2474	ken.wainstein@cwt.com
Keith M. Gerver	+1 202 862 2381	keith.gerver@cwt.com
Peter T. Carey	+1 202 862 2339	peter.carey@cwt.com

25 *See*, *e.g.*, Letter from Technologists to Sens. Richard Burr & Diane Feinstein & Reps. Adam Schiff, Devin Nunes, & Michael McCaul (Apr. 16, 2015), *available at* http://cyberlaw.stanford.edu/files/blogs/technologists_info_sharing_bills_letter_w_exhibit.pdf.

26 *See*, *e.g.*, Jennifer Granick, *OmniCISA Pits DHS Against the FCC and FTC on User Privacy*, JUST SECURITY (Dec. 16, 2016, 6:09 PM), https://www.justsecurity.org/28386/omnicisa-pits-government-against-self-privacy/.