ALSTON&BIRD

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTONPRIVACY.COM MARCH 17, 2015

An Evolving Path Forward: Recent Developments in Cybersecurity Information Sharing

By Kim Peretti and Jason Wool

On March 12, 2015, the Senate Intelligence Committee passed, by a vote of 14-1, a revised version of last year's Cybersecurity Information Sharing Act (CISA). While the strong bipartisan support for the bill is encouraging, in the past Congress has been unable to pass legislation that President Obama would be willing to sign.[1] This Congress may be different, however, as the President has made it an obvious priority to communicate his preferences for an information sharing bill up front and has otherwise taken executive action to spur increased sharing in the meantime. Indeed, the President's efforts may already be making an impact, as early reports of the CISA markup last week indicate that certain amendments have moved the bill towards some of the White House's stated policy preferences.[2]

Specifically, on February 13, 2015, President Obama signed an executive order intended to spur increased cybersecurity information sharing between the private sector and the federal government. Around the same time, the White House also announced the creation of a new Cyber Threat Intelligence Integration Center (CTIIC), held a summit on cybersecurity and consumer protection at Stanford University and circulated a series of legislative proposals on cyber-related topics, including threat indicator sharing. These actions followed the President's historic statement in the January State of the Union address that "[n]o foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids."

The White House's flurry of activity is just the latest in a series of governmental attempts to encourage and incentivize private entities to share cyber threat indicators with the federal government and specialized information sharing organizations. Despite significant focus on information sharing by the government and media alike, however, many observers have voiced confusion about the impacts of the

---

1 In the last Congress, several committees circulated information sharing bills, including, most notably, CISA in the Senate and the Cyber Intelligence Sharing and Protection Act (CISPA) in the House. *See* Cybersecurity Information Sharing Act of 2014, S. 2588, 113th Cong. (2014); Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013). In the current Congress, one cyber information sharing bill has already been introduced, with more certain to follow. *See* Cyber Threat Sharing Act of 2015, S. 456, 114th Cong. (2015). The 2015 version of CISA has not yet been released to the public.

2 Charlie Mitchell, "Feinstein Hopes Third Time's a Charm for Cybersecurity Legislation," *Inside Cybersecurity*, March 13, 2015 ("The changes would seem to move the Intelligence panel's work closer to the Obama administration's info-sharing proposal.").

White House's actions. For additional background on cybersecurity information sharing, including types of information shared, methods of sharing and concerns with information sharing, see Kim Peretti"s "Cyber Threat Intelligence: To Share or Not to Share—What Are the Real Concerns?" in the Bloomberg BNA *Privacy and Security Law Report*.

Executive Order

Recognizing the importance of organizations that facilitate cybersecurity information sharing, the executive order seeks to "encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis." Specifically, the President directs the Secretary of Homeland Security to "strongly encourage" the formation of so-called information sharing and analysis organizations (ISAOs) and to enter into an agreement with a nongovernmental organization to develop a set of "voluntary standards or guidelines for the creation and functioning of ISAOs...."ISAOs could be formed by nonprofit or for-profit entities from the private or public sectors and could be based on sector, region or any other relationship or commonality. The order also designates the National Cybersecurity and Communications Integration Center (NCCIC) as a critical infrastructure protection program and delegates to it "authority to enter into voluntary agreements with ISAOs in order to promote critical infrastructure security with respect to cybersecurity."

The President's focus on ISAOs in the executive order initially raised eyebrows in some communities for appearing to eschew the existing ecosystem of sector-based information sharing and analysis centers (ISACs). These organizations developed largely in response to the September 11 terrorist attacks to streamline the collection, analysis and dissemination of threat intelligence within a given sector (or, in some cases, across several sectors that share a particular technology, such as industrial control systems).[3] Although ISACs are, in some cases, already highly mature, it is likely that the White House did not wish to limit the universe of information sharing organizations while also desiring to apply the same set of operational guidelines to all entities that facilitate cyber threat sharing. For instance, there are a number of for-profit companies that provide information sharing services, and the administration may want to encourage competition in this space in order to spur innovation. Indeed, the Department of Justice issued a business review letter in October 2014 advising a private entity that its cyber threat sharing program did not raise antitrust concerns, an act that may have signaled the administration's support for such organizations, or at least its agnostic stance on threat sharing facilitators.[4]

Moreover, ISAOs were already part of an existing statutory information sharing framework, which the President may want to leverage. The Critical Infrastructure Information Act of 2002, a subtitle of the Homeland Security Act of 2002, created what is now known as the Protected Critical Infrastructure Information (PCII) program and specifically defined the term "information sharing and analysis

---

3 Kimberly Peretti, "Cyber Threat Intelligence: To Share or Not to Share—What Are the Real Concerns?," *BNA Privacy and Security Law Report*, September 1, 2014, at 2-3.

4 U.S. Dep't of Justice, Letter from William J. Baer, Assistant Attorney General, to Steven A. Bowers, Fish & Richardson P.C. at 1 (Oct. 2, 2014).

organization." Information submitted pursuant to the requirements of the PCII law and regulations receives a number of legal protections, including exemption from disclosure under the Freedom of Information Act, protection from use in any civil action without consent from the submitting entity and preservation of any applicable legal privilege or other protection provided by law, such as trade secret protection. Under the statute, the President is entitled to delegate authority to a critical infrastructure protection program, which now includes the NCCIC, "to enter into a voluntary agreement to promote critical infrastructure security, including with any [ISAO]…."

By aligning the executive order with the PCII program, the President may also wish to remind the private sector of the existing statutory liability protections for information sharing provided under the PCII program in the absence of new legislation. Liability concerns are often cited among the foremost hurdles to private sector information sharing, and most attempts at federal legislation on this subject include substantial protections for entities that share.[5] For instance, CISA attempted to authorize entities to monitor networks and operate countermeasures under certain circumstances, provide a qualified antitrust exemption, prohibit lawsuits based on network monitoring and the sharing or receipt of cyber threat indicators, preserve any applicable privilege or other legal protection to information shared with the federal government and prohibit any government recipient of shared threat indicators from directly using the information to regulate the lawful activities of an entity.

Because no recent cybersecurity information sharing bills have become law despite Congress's repeated efforts, the President may want to remind the private sector that some of these protections are already available under certain circumstances. The executive order's attempt to create a uniform system of "middle man" organizations is likely also, in part, an attempt to make organizations more comfortable with information sharing. At the same time, the President's own legislative proposal on information sharing[6] would also leverage ISAOs and would require them to maintain "a publicly-available self-certification that it has adopted the best practices" identified or developed by the standards organization referenced in another section of the proposal. The use of ISAOs in the executive order is thus also viewed as laying the groundwork for the White House's legislative proposal.

The executive order should not, therefore, be regarded as seeking to re-invent the wheel with regard to ISACs. Numerous ISACs will likely form ISAOs under the guidelines eventually produced by the standards organization selected by the Secretary of Homeland Security.

It is important to note, however, that PCII protections are only available to critical infrastructure information (CII) as defined in the statute. As a result, information shared with the federal government that does not qualify as CII is ineligible for liability protection, even if shared with an ISAO. In addition, the liability protections provided under the PCII program are somewhat limited in comparison to those most

---

5 Peretti, *supra*, at 4-7.

6 The proposal is available at http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-information-sharing-legislative-proposal.pdf.

sought by the private sector.[7] For instance, PCII does not address antitrust liability or criminal liability under statutes such as the Stored Communications Act. It is not immediately apparent what legal benefits, if any, the executive order provides to entities that are not in critical infrastructure sectors or that wish to share information unrelated to critical infrastructure. By sharing information with an ISAO, however, entities may be able to ensure that the data is anonymized prior to submission to the government, similar to methods offered under existing ISACs' structures.

Moreover, without an explicit assurance that threat information shared with an ISAO or the federal government is itself a privileged communication, entities may not be willing to share information obtained as a direct result of an intrusion unless that information happens to already be subject to a legal privilege. One focus of much of the litigation concerning data breaches at the state level is when the breached organization discovered the incident, and information sharing communications with an ISAO or the federal government may be discoverable evidence in this inquiry. Although the PCII statute protects an *existing* privilege, it likely would not create a new privilege when technical threat data is conveyed to an appropriate entity as part of the program. Thus, if no privilege exists with regard to a specific threat indicator, it could be discoverable if conveyed to an ISAO or the government.[8] This is likely a major disincentive to sharing threat information.

Cyber Threat Intelligence Integration Center

In creating the Cyber Threat Intelligence Integration Center (CTIIC), the President followed through on a commitment in his last State of the Union address to make "sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism." The CTIIC, which will be modeled on the National Counterterrorism Center, will be responsible for analyzing and integrating cyber threat intelligence collected by other government agencies for use in producing and disseminating coordinated cyber threat assessments to "Cyber Centers and other elements within the government."[9] The CTIIC, which the Director of National Intelligence will direct, will not itself collect intelligence but rather will focus on rapid information analysis and sharing. In addition to intra-government sharing, the administration will not "bottle up our intelligence—if we have information about a significant threat to a business, we're going to do our utmost to share it."[10] The CTIIC will also integrate intelligence provided by the private sector.

---

7 *Id.*

8 In addition, it is not entirely clear from the statute if, when an ISAO conveys threat information to the federal government on behalf of an entity, the privilege protection is maintained. The statute states that CII that is voluntarily submitted *to the government* under the program does not constitute a waiver of any applicable privilege. Although the definition of the term "voluntary" states that submittal of information to the government "may be accomplished by a single entity or an [ISAO] on behalf of itself or its members," one could read the statute such that privilege protection only applies when an entity submits threat information directly to the government.

9 Lisa O. Monaco, Strengthening our Nation's Cyber Defenses (Feb. 10, 2015).

10 *Id.*

White House Summit on Cybersecurity and Consumer Protection

On February 13, 2015, the White House hosted a summit at Stanford University on cybersecurity and consumer protection. The summit touched on a number of cybersecurity topics, ranging from consumer-oriented data protection and issues facing payment technologies (including the President's BuySecure Initiative announced last October) to international law enforcement and information sharing. With regard to the latter, the summit featured a panel on cybersecurity information sharing moderated by Michael Daniel of the National Security Council featuring several CEOs, high ranking government officials and the director of civil liberties at Stanford.

The President also delivered a policy-oriented speech at the summit in which, among other things, he set forth four guiding principles for cybersecurity. These policy pillars are shared responsibility between the public and private sectors, intelligent use of the respective strengths of the public and private sectors, rapid, flexible evolution in defensive tactics and protection of privacy and civil liberties.

White House Legislative Framework for Information Sharing

On January 13, 2015, President Obama announced a legislative proposal on cybersecurity information sharing intended to address the White House's own criticisms of previous legislative proposals such as CISA and CISPA, including those associated with privacy. The proposal defines a cyber threat indicator to primarily encompass technical information, though content-based information is not entirely out of scope. By definition, a cyber threat indicator must also have been subject to "reasonable efforts... to remove information that can be used to identify specific persons reasonably believed to be unrelated to the cyber threat." The proposal authorizes the sharing of "lawfully obtained cyber threat indicators" to an ISAO, the NCCIC or a federal law enforcement agency. It would also provide a number of liability limitations on the sharing or receipt of cyber threat indicators.

Most notably, the proposal would require the development of policies and procedures governing the receipt, retention, disposal, use and disclosure of cyber threat indicators by the federal government under the proposed act. It would also require the development of guidelines governing law enforcement's use of received cyber threat indicators, which would limit their use to the investigation, prosecution, disruption or response to a computer crime, a threat of death or serious bodily harm, a serious threat to a minor or an attempt or conspiracy to commit one of these offenses. At the same time, the proposal would require the NCCIC to share received cyber threat indicators with "other Federal entities in as close to real time as practicable," which would presumably include intelligence agencies such as the National Security Agency.

While the White House proposal may not be likely to pass, it will likely prove useful to Congress in determining whether other information sharing proposals will be likely to gain the President's approval, especially with regard to the protection of privacy and civil liberties.

Conclusion

It is clear from the President's recent actions that the administration is serious about promoting cybersecurity information sharing and that it will use all available tools to further this goal. While the executive order may help in the near term, the President's ultimate goal is to sign legislation that will facilitate more effective and robust cyber threat indicator sharing from the private sector. By taking action early in this Congress, the President may help to ensure that such a bill can become law this year. Moreover, companies that wish to take advantage of information sharing within their industry or with the federal government should stay abreast of the evolving options for doing so while minimizing any potential risk to the organization.

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

Security Incident Management & 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