SULLIVAN & CROMWELL LLP

December 22, 2015

The Cybersecurity Act of 2015

Congress Passes and President Signs Long-Anticipated Measure Setting Framework for Sharing Cyber Threat Information with Federal Government and Private Sector

SUMMARY

On December 18, 2015, President Obama signed into law the Cybersecurity Act of 2015. The Act, arguably the most significant piece of federal cyber-related legislation enacted to date, establishes a mechanism for cybersecurity information sharing among private-sector and federal government entities. It also provides safe harbors from liability for private entities that share cybersecurity information in accordance with certain procedures, and it authorizes various entities, including outside the federal government, to monitor certain information systems and operate defensive measures for cybersecurity purposes. The Act also contains provisions designed to bolster cybersecurity protections at federal agencies, assess the federal government's cybersecurity workforce, and implement a range of measures intended to improve the cybersecurity preparedness of critical information systems and networks.

BACKGROUND

For nearly two decades, information relating to potential cyber threats has been shared through industry-specific Information Sharing and Analysis Centers ("ISACs"), established in 1998 under the auspices of Presidential Decision Directive 63. Despite the growth and importance of ISACs, participants and commentators have expressed concern that perceived risks associated with information sharing—including potential civil liability, antitrust issues, and the protection of intellectual property and other proprietary business information—have limited the effectiveness of ISACs and other information-sharing efforts.

On February 13, 2015, President Obama signed Executive Order 13691 "to encourage and promote sharing of cybersecurity threat information within the private sector and between the private sector and government." The Order encouraged the development of Information Sharing and Analysis Organizations ("ISAOs") and of a common set of voluntary standards for ISAOs, including privacy protections. It also clarified the authority and operational framework of the National Cybersecurity and Communications Integration Center ("NCCIC"), a civilian agency in the Department of Homeland Security ("DHS") tasked with coordinating the sharing of information within the federal government and with entities outside the government. Finally, it added DHS to the list of federal agencies that approve classified information-sharing arrangements to streamline private companies' ability to access classified cybersecurity threat information.

Building on Executive Order 13691, in April 2015, the House of Representatives passed two bills—one reported by the House Permanent Select Committee on Intelligence and the other by the House Committee on Homeland Security—intended to encourage information sharing within the private sector and between the private sector and the government. In October 2015, the Senate passed a separate cybersecurity information-sharing bill, which was reported by the Senate Select Committee on Intelligence. While the three bills were similar in many ways and would all have encouraged the voluntary sharing of cybersecurity threat information, they differed in important respects. Significantly, the House Committee on Homeland Security's bill and the Senate bill would have vested oversight of the information-sharing apparatus in DHS, while the House Intelligence Committee's bill would instead have placed that responsibility with the intelligence community. Title I of the Cybersecurity Act of 2015, which is called the Cybersecurity Information Sharing Act of 2015 ("CISA"), is the product of intense negotiations to reconcile the three bills.

POINTS OF EMPHASIS

The Cybersecurity Act of 2015—and particularly the information-sharing mechanism it implements through CISA—is expected to set the parameters for how federal departments and agencies, as well as private entities and state, tribal, and local government agencies (collectively, "Non-Federal Entities"), share and receive cybersecurity-related information. The legislation is the product of years of discussions, numerous bill drafts, and extended debates about the privacy and liability risks associated with information sharing. Privacy advocates and civil liberties groups continue to express concern about some of the Act's provisions.[1] On the other hand, industry groups such as the U.S. Chamber of

[1] *See, e.g.*, Jenna McLaughlin, *Last-Minute Budget Bill Allows New Privacy-Invading Surveillance in the Name of Cybersecurity*, THE INTERCEPT (Dec. 18, 2015), https://theintercept.com/2015/12/18/last-minute-budget-bill-allows-new-privacy-invading-surveillance-in-the-name-of-cybersecurity/; Mark Jaycox, *EFF Opposes Cybersecurity Bill Added to Congressional End of Year Budget Package*, EFF (Dec. 18, 2015), https://www.eff.org/deeplinks/2015/12/statement-finalized-congressional-cybersecurity-bill.

Commerce and the Financial Services Roundtable have lauded the Act as a crucial step forward in protecting Americans' data and intellectual property from devastating cyberattacks.[2]

The following are a few key points regarding the legislation, which is reviewed in detail below:

- **Sharing centralized in DHS.** After a long tug-of-war between DHS and the intelligence community, DHS—and specifically NCCIC—has been selected as the primary gateway for cybersecurity information sharing between the private sector and the federal government. DHS is required to set up an automated system to forward information it receives to many other federal entities, including the Department of Defense and the Office of the Director of National Intelligence, in real-time or as quickly as operationally practicable. The president, through a report and certification to Congress, may also designate an additional information-sharing portal within another federal entity, such as the Office of the Director of National Intelligence or the Federal Bureau of Investigation.
- **Liability protections require sharing "in accordance" with CISA.** To benefit from CISA's safe harbor from civil liability, private entities' sharing activity must be "conducted in accordance" with CISA's provisions. Though some privacy advocates had called for imposing an intent-based requirement that companies comply with CISA in "good faith"—thereby opening the door to legal liability in the event of bad faith, yet technically proper, information sharing—Congress appears to have opted for an objective compliance test grounded in the technical requirements of CISA. Entities that share information should keep clear records evidencing their compliance with CISA to ensure they can benefit from its liability protections.
- **Broad safe harbors from liability.** Once triggered, CISA's safe harbors from liability are broad. Private entities sharing information are generally shielded from civil, regulatory, and antitrust liability based on their sharing. Unlike all three information-sharing bills the House and Senate passed earlier this year, CISA does not expressly exclude instances of either gross negligence or willful misconduct from its liability protections. Sharing cyber threat indicators and defensive measures with the federal government will also not constitute a waiver of any privilege or protection provided by law, and shared information is exempt from disclosure under freedom of information laws. Information shared with the federal government will remain the commercial, financial, or proprietary information of the originating Non-Federal Entity only if that entity so designates it.
- **Requirement to remove information known to be unrelated personal information.** One of CISA's requirements is that Non-Federal Entities review information to be shared, or utilize a technical capability, to remove any information that the Non-Federal Entity "knows at the time of sharing" to be personal or personally identifying information not directly related to a cybersecurity threat. DHS will release guidelines to assist in identifying information that should not be shared due to privacy concerns but, from a risk-of-liability perspective, CISA's actual knowledge requirement should provide private entities sharing information with some comfort, particularly as compared to the heightened standards based on "reasonable belief" included in the two House bills.
- **Communications with regulatory authorities permitted.** Though the availability of liability protection turns on using the DHS process, regulated entities can continue to communicate directly with their respective federal regulatory authorities regarding cybersecurity threats without losing CISA's liability protections.

---

[2] *See* Press Release, U.S. Chamber of Commerce, *U.S. Chamber President Comments on Omnibus Spending Bill* (Dec. 16, 2015), https://www.uschamber.com/press-release/us-chamber-president-comments-omnibus-spending-bill; Press Release, Fin. Serv. Roundtable, *Spending Bill Inclusion of Cybersecurity Information Sharing Legislation is Victory for Strengthening Defenses Against Cyber Attacks* (Dec. 15, 2015), http://fsroundtable.org/spending-bill-inclusion-of-cybersecurity-information-sharing-legislation-is-victory-for-strengthening-defenses-against-cyber-attacks/.

- **Limited use of shared information by federal and state governments.** The permissible purposes for which shared information may be used by federal and state governments are circumscribed, though these limits are less restrictive than those contained in the two House bills. Privacy and civil liberty advocates have raised concerns in particular regarding the potential breadth of CISA's authorization for governments to use shared information to respond to, prevent, mitigate, investigate, or prosecute a specific (though not necessarily imminent) "threat of serious economic harm."
- **No duty to share.** CISA does not create any duty to share cyber threat indicators or defensive measures and expressly prohibits the federal government from attempting to coerce sharing by withholding cybersecurity information or other benefits such as government contracts, addressing concerns some privacy advocates had expressed that companies could be forced to turn over large swaths of user data to the government.
- **No creation of a duty to warn or act.** CISA does not impose a duty to warn or act based on the receipt of shared information, but it does not expressly shield entities from liability in the event of a good-faith failure to act. An entity that receives information about a cybersecurity threat to its networks may remain subject to claims premised on common law causes of action such as negligence if it fails to respond diligently.
- **Authorization to use defensive measures.** CISA also authorizes private entities to use defensive measures for cybersecurity purposes on an entity's own information systems and on the information systems of other consenting entities. Excluded from the definition of "defensive measures" are those that destroy, render unusable, provide unauthorized access to, or substantially harm third-party information systems. As such, CISA does not authorize "hacking back," which generally remains illegal pursuant to the Computer Fraud and Abuse Act and guidance published by the Department of Justice.

Entities engaged in or contemplating information sharing are advised to review the Cybersecurity Act of 2015 closely and may wish to consult counsel to better understand the requirements of the Act and the legal protections from which they may be able to benefit.

OVERVIEW OF THE ACT

The Cybersecurity Act of 2015 contains four titles:

- Title I, which will be of greatest interest to most private-sector entities, establishes a centralized mechanism for cybersecurity information sharing.
- Title II instructs DHS to take measures designed to strengthen cybersecurity in the federal government and at federal agencies, as well as to facilitate the implementation of Title I.
- Title III calls for a cybersecurity-focused assessment of the federal workforce.
- Title IV provides for other measures intended to identify and address threats to critical information systems and networks.

A. TITLE I – CYBERSECURITY INFORMATION SHARING ACT OF 2015

Title I of the Act, CISA, establishes mechanisms by which (a) federal departments and agencies can share cybersecurity information with one another and with Non-Federal Entities; and (b) Non-Federal Entities can share cybersecurity information with one another and with federal departments and agencies. It also provides several safe harbors from liability for private entities that share cybersecurity information in accordance with its procedures and the processes that DHS is to promulgate, and it authorizes

Non-Federal Entities to monitor certain information systems and operate defensive measures for cybersecurity purposes. Finally, it establishes reporting mechanisms designed to keep Congress apprised of the implementation of information-sharing measures; compliance with information-sharing policies, procedures and guidelines; the protection of personal privacy through removal of personal data from shared information; and the general state of cybersecurity threats directed against the United States. CISA also includes a preemption clause and a ten-year sunset provision.

Sharing by Federal Departments and Agencies

CISA requires key federal agencies to develop and issue a series of procedures to facilitate information sharing by federal departments and agencies with other federal entities, Non-Federal Entities, and the public. The procedures, which are to be developed jointly by the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, must be issued within 60 days of the law's enactment.

The procedures are to be designed to facilitate the timely sharing of both classified and unclassified cyber threat indicators and defensive measures with persons who have appropriate security clearances, including by declassifying information as appropriate, and to permit the sharing of unclassified information directly with the public. The procedures also are to encourage timely sharing of information about cybersecurity threats with entities that are the subjects of those threats, as well as the periodic sharing, through publications and targeted outreach, of cybersecurity best practices, with particular attention to accessibility and implementation challenges faced by small businesses.

The information-sharing procedures should also:

- Ensure that cyber threat indicators and defensive measures are shared by federal departments and agencies in real time or as quickly as operationally practicable;
- Incorporate, to the greatest extent practicable, existing processes, roles and responsibilities (including sector-specific ISACs);
- Include procedures for notifying entities that receive erroneous information or information shared in contravention of CISA;
- Require federal departments and agencies sharing cyber threat indicators and defensive measures to utilize controls to protect against unauthorized access to or acquisition of such information;
- Require federal departments and agencies to scrub cyber threat indicators they share for any information not directly related to a cybersecurity threat that the federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual, which may be accomplished by either reviewing the threat indicators or using a technical means configured to remove personal information; and
- Include rules for notifying, in a timely manner, any U.S. person whose personal information is known or determined to have been shared by a federal entity in violation of CISA.

Sharing by Non-Federal Entities

CISA authorizes Non-Federal Entities to share cyber threat indicators and defensive measures with, and receive such information from, both federal entities and Non-Federal Entities for cybersecurity purposes. In so doing, Non-Federal Entities must protect classified information from improper disclosure and comply with any lawful use or sharing restrictions placed on information they receive.

Importantly, as with federal departments and agencies, prior to sharing cyber threat indicators, Non-Federal Entities must scrub them for any information not directly related to a cybersecurity threat that the Non-Federal Entity knows at the time of sharing is personal or personally identifying information. Non-Federal Entities are permitted to employ technical means configured to remove such information.

CISA also streamlines the process by which the federal government generally receives cyber threat indicators and defensive measures from Non-Federal Entities. Within 90 days of CISA's enactment, DHS is directed to develop and implement a capability and process to (a) accept, in real-time, cyber threat indicators and defensive measures on behalf of the federal government from Non-Federal Entities, and (b) share such information automatically with various other federal entities, including the Departments of Commerce, Defense, Energy, Justice, and the Treasury, and the Office of the Director of National Intelligence (collectively with DHS, "Appropriate Federal Entities"). The Secretary of Homeland Security is also directed to consult with these federal entities in developing the capability and process, and to certify to Congress within 90 days of the enactment of CISA whether the capability and process is fully operational.

While the DHS information-sharing process is to be the primary means by which the federal government receives cybersecurity information from Non-Federal Entities, CISA directs that the DHS process is not to limit or prohibit otherwise lawful disclosures of cybersecurity information by Non-Federal Entities to federal entities, including reporting of suspected criminal activity, participation in federal investigations, or the provision of cyber threat indicators or defensive measures as part of a statutory or contractual requirement. Moreover, certain communications between federal entities and Non-Federal Entities are specifically excepted from the process. Specifically, certain communications concerning previously shared cyber threat indicators need not flow through DHS, and regulated Non-Federal Entities can continue to communicate directly with their respective federal regulatory authorities regarding cybersecurity threats.

Within 60 days of CISA's enactment, the Attorney General and the Secretary of Homeland Security are directed to develop a number policies, procedures and guidelines to govern the information-sharing process:

- **Interim policies and procedures relating to the receipt of cybersecurity information by the federal government.** These policies and procedures are to ensure that cyber threat indicators and defensive measures shared with the federal government by Non-Federal Entities are shared in real

time, in an automated, uniform, and simultaneous manner, or as quickly as operationally practicable, with all Appropriate Federal Entities. Final policies and procedures must be submitted to Congress within 180 days of CISA's enactment.

- **Guidelines to assist with and promote the sharing of cyber threat indicators with federal entities.** Among other things, these guidelines are to provide guidance concerning what types of information qualify as cyber threat information and are unlikely to contain unrelated personal or personally identifying information, and what types of information are unlikely to be directly related to a cybersecurity threat and are protected under otherwise applicable privacy laws.
- **Interim guidelines relating to privacy and civil liberties.** These guidelines will govern the receipt, retention, use, and dissemination of cyber threat indicators by federal departments and agencies. Among other things, they are to limit the effect on privacy and civil liberties of the federal government's activities under CISA; maintain the security, safeguard the confidentiality, and limit the receipt, retention, use and dissemination of cyber threat indicators containing personal or personally identifying information; and include a procedure to notify entities that share information when that information is known or determined by a federal entity not to constitute a cyber threat indicator. Final guidelines are to be issued within 180 days of CISA's enactment and must thereafter be reviewed at least every two years.

Possible Parallel Designation

Although CISA vests the federal government's information-sharing capability and process in DHS, it also permits the president to designate a second federal entity to develop and implement a parallel information-sharing capability and process. The agency designated to create this parallel process may not be the National Security Agency or any other part of the Department of Defense. To make such a designation, the president must explain and certify to Congress that such a designation is necessary to ensure the full, effective, and secure operation of the information-sharing mechanism; that the mechanism will be conducted in compliance with policies, procedures, and guidelines developed under CISA; and that its implementation is consistent with the mission of the designated federal entity.

Limitations on Federal Use

CISA also limits what the federal government and state, tribal, and local governments may do with information provided to them pursuant to CISA. Specifically, such information may be disclosed, retained, or used only for: (a) a cybersecurity purpose; (b) identifying cybersecurity threats or security vulnerabilities; (c) responding to, preventing or mitigating a specific threat of death, or serious bodily or economic harm, including a terrorist act; or (d) responding to, investigating, prosecuting, preventing, or mitigating a serious threat to a minor, including sexual exploitation and threats to physical safety, any offense arising out of a threat described in (c), or certain offenses relating to fraud, identity theft, espionage, censorship, or the protection of trade secrets.

Monitoring and Operation of Defensive Measures

CISA authorizes private entities, for cybersecurity purposes, to monitor and apply defensive measures to their own information systems and those of other entities that have provided written consent. Private entities can also monitor information stored on, processed by, or transiting through such information systems. Measures that destroy, render unusable, provide unauthorized access to, or substantially harm

an information system or information not owned by either the private entity operating the measure or a consenting entity are, however, excluded from the definition of "defensive measures" and are therefore not authorized by CISA.

Safe Harbors

CISA establishes a number of safe harbors from liability for private entities that share cyber threat indicators or defensive measures, so long as sharing is conducted in accordance with CISA's requirements:

- **No civil liability for information sharing.** No cause of action can be maintained against any private entity for sharing or receiving cyber threat indicators or defensive measures if such sharing or receipt is conducted in accordance with CISA and, for information shared with the federal government, if it is shared via the capability and process within DHS (or any parallel mechanism designated by the president).
- **Limitation on regulatory liability based on shared information.** Cyber threat indicators and defensive measures that Non-Federal Entities share with a federal entity or with a state, tribal or local government pursuant to CISA may not be used to regulate, including in an enforcement action, the lawful activity of any Non-Federal Entity or any activity taken by a Non-Federal Entity pursuant to mandatory standards. Such shared information may, however, inform the development or implementation of regulations of information systems consistent with a regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems.
- **No antitrust liability for information sharing or providing cybersecurity assistance.** It will not be considered a violation of antitrust laws for two or more private entities to exchange cyber threat indicators or defensive measures, or to provide assistance relating to the prevention, investigation or mitigation of a cybersecurity threat, for cybersecurity purposes. CISA makes clear, however, that it does not permit anti-competitive conduct, such as price-fixing or market allocation between competitors.
- **No waiver of privileges or protections as a result of sharing.** Sharing of cyber threat information with the federal government will not constitute a waiver of any applicable privilege or protection provided by law, including trade-secret protection, and shared cyber threat indicators and defensive measures are exempted from disclosure under the Freedom of Information Act and other federal, state, and local freedom of information laws. Shared information will also be considered the commercial, financial, or proprietary information of the originating Non-Federal Entity if that entity so designates it.
- **No duty to share or act, and no liability for not sharing.** CISA states that it does not create a duty to share cybersecurity information or a duty to warn or act based on the receipt of such information, and does not impose liability on entities choosing not to engage in the voluntary activities authorized by CISA. It also does not compel the creation of new information-sharing relationships for any Non-Federal Entity and does not require Non-Federal Entities to provide information to any other entity or use the capability and process within DHS. A federal entity may not condition the sharing of cyber threat indicators with a Non-Federal Entity on such entity's reciprocal sharing of indicators and may not condition the award of any federal grant, contract or purchase on the provision of cyber threat indicators.
- **No liability for monitoring.** CISA explicitly shields private entities from any liability for monitoring activities conducted consistent with CISA's requirements.

B. TITLE II – NATIONAL CYBERSECURITY ADVANCEMENT

Title II contains two subtitles: Subtitle A, the National Cybersecurity Protection Advancement Act of 2015 ("NCPAA"); and Subtitle B, the Federal Cybersecurity Enhancement Act of 2015 ("FCEA").

The NCPAA amends the Homeland Security Act of 2002 to charge NCCIC with the implementation of the information-sharing mechanism set forth in CISA. Among other things, the NCPAA also:

- Sets out the procedures by which NCCIC may enter into and terminate voluntary information-sharing relationships with Non-Federal Entities and the types of agreements that may govern such relationships;
- Instructs DHS, within 60 days of the NCPAA's enactment, to enhance outreach to critical infrastructure owners and operators for purposes of sharing cybersecurity information and to disseminate to the public information about how to voluntarily share cyber threat indicators and defensive measures with NCCIC;
- Tasks NCCIC with a number of other new functions, including engaging with international partners on cybersecurity and participating, as appropriate, in national exercises run by DHS;
- Amends the composition of NCCIC by explicitly adding ISACs and private entities to the list of groups that may represent Non-Federal Entities on NCCIC, and adding entities that collaborate with state and local governments on cybersecurity and share information with NCCIC to the list of groups that compose NCCIC; and
- Requires DHS to report to the House and Senate Homeland Security Committees on a number of issues, including: (a) efforts to bolster cooperation on cybersecurity with international partners; (b) the feasibility of reducing cybersecurity risks in DHS data centers; (c) the feasibility of producing a risk-informed plan to address the risk of multiple simultaneous cyber incidents affecting critical infrastructure; and (d) the cybersecurity of the ten U.S. ports that DHS determines are at the greatest risk of a cybersecurity incident.

The FCEA aims to secure the information systems of the federal government by requiring DHS to deploy and make available to federal agencies a system to detect and prevent cybersecurity risks in network traffic transiting or traveling to or from an agency information system. The system must be deployed within a year of the FCEA's enactment. This requirement applies to federal agencies and systems other than the Department of Defense, intelligence community components, and national security systems,[3] and is required to be used for all information travelling between their information systems and information systems not belonging to a federal agency. In developing the cybersecurity system, DHS and private entities retained by DHS are authorized to access information transiting or traveling through or from federal agency information systems, but the FCEA sets out a number of principles limiting permissible access to and use of such information.

[3] A national security system is defined as "a telecommunications or information system operated by the federal government, the function, operation, or use of which . . . involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or . . . is critical to the direct fulfillment of military or intelligence missions, . . . [other than] a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications)." 40 U.S.C. § 11103(a).

Within one year of the FCEA's enactment, the head of each federal agency and system other than the Department of Defense, intelligence community components, and national security systems must also conduct certain cybersecurity assessments and implement certain cybersecurity measures specified in the FCEA, unless doing so would be excessively burdensome and is not necessary to secure the agency's information system.

The FCEA grants DHS a central role in ensuring that the federal government as a whole has the appropriate tools in place to protect its systems from cybersecurity threats. Beyond tasking DHS with developing the aforementioned cybersecurity system, the FCEA provides that:

- DHS must implement a plan, developed by the Office of Management and Budget ("OMB"), to ensure that each federal agency utilizes appropriate advanced network security tools to detect and mitigate intrusions and anomalous activity;
- DHS will assist OMB in ensuring federal agencies timely adopt and comply with federal cybersecurity policies and standards to secure their information systems;
- In coordination with OMB, DHS will develop and implement an intrusion assessment plan to proactively and routinely detect, identify and remove intruders in the information systems of federal agencies other than the Department of Defense, intelligence community components, and national security systems; and
- In response to a known or reasonably suspected threat, vulnerability or incident that represents a substantial threat to an agency's information security, DHS may issue emergency directives to the head of the relevant federal agency to take any lawful action with respect to the operation of the information system in question.

The FCEA also instructs the Comptroller General to conduct a study and publish a report within three years of the FCEA's enactment on the effectiveness of the federal government's strategy and approach to securing agency information systems and puts into place various reporting requirements to ensure Congress is kept apprised of relevant developments.

C. TITLE III – FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT ACT OF 2015

Title III of the Act is the Federal Cybersecurity Workforce Assessment Act of 2015 ("FCWAA"). The FCWAA contemplates a wide-ranging assessment of the federal workforce, both civilian and non-civilian, to identify positions that require the performance of cybersecurity or other cyber-related functions. The assessment is expected to be completed approximately three years after enactment of the FCWAA. One year after the first assessment, and annually thereafter, the head of each federal agency will be required to identify roles of critical need in the areas of information technology, cybersecurity or other cyber-related work.

D. TITLE IV – CHANGES TO ACCESS DEVICE LIABILITY OUTSIDE OF THE UNITED STATES AND OTHER CYBER MATTERS

Title IV of the Act includes miscellaneous provisions intended to address cybersecurity threats. One of these measures is a change to the U.S. Code provision criminalizing access device fraud, which includes

credit card fraud, 18 U.S.C. § 1029. This change will eliminate one of the two jurisdictional requirements for application of the statute to persons outside the United States. Prior to the amendment, persons outside the territorial jurisdiction of the United States who engaged in one of the prohibited acts would only be covered by the statute if there was a physical territorial connection to the United States, such as the transportation or storage in the United States of any article used to assist in the commission of the offense or of the proceeds of the offense.[4] With the elimination of that requirement, a person outside the territorial jurisdiction of the United States will be covered by the statute so long as he or she meets the remaining requirement that the offense involve an access device (such as a credit card, debit card, or account number) issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States, or of any state, the District of Columbia, or any other territory of the United States. The amendment also narrows the scope of entities protected by 18 U.S.C. § 1029, since they must now be organized under U.S. law, instead of merely being within the jurisdiction of the United States.

Title IV also calls on the Secretary of State to take actions in the international sphere to protect U.S. systems. Among other measures, the Secretary of State must produce a comprehensive strategy relating to U.S. international policy with regard to cyberspace. This strategy is to include the development of norms of responsible international behavior in cyberspace and a review of alternative concepts with regard to international norms in cyberspace offered by countries such as Brazil, China, India, and Russia.

---

[4] The text of 18 USC § 1029(h), prior to its amendment by the Cybersecurity Act of 2015, provided that:

> (h) Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under subsection (a) or (b) of this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if—
>
> (1) the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity within the jurisdiction of the United States; and
>
> (2) the person transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the United States, any article used to assist in the commission of the offense or the proceeds of such offense or property derived therefrom.

As amended, it reads as follows:

> (h) Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under subsection (a) or (b) of this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States, or any State, the District of Columbia, or other territory of the United States.

The other measures contemplated by Title IV include a study on the security of federal mobile devices, initiatives to ensure that international cybercriminals who are not extradited to the United States are apprehended and prosecuted in other countries, enhancement of emergency services, measures to improve cybersecurity in the healthcare industry (including creation of a healthcare cybersecurity task force), and reports on access security of U.S. national security systems and U.S. systems that provide access to personally identifiable information.

* * *

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 800 lawyers on four continents, with four offices in the United States, including its headquarters in New York, three offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future related publications from Stefanie S. Trilling (+1-212-558-4752; trillings@sullcrom.com) in our New York office.

CONTACTS

New York		
Jay Clayton	+1-212-558-3445	claytonwj@sullcrom.com
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Scott D. Miller	+1-212-558-3109	millersc@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Eric J. Kadel Jr.	+1-202-956-7640	kadelej@sullcrom.com
Brent J. McIntosh	+1-202-956-6930	mcintoshb@sullcrom.com
Stephen H. Meyer	+1-202-956-7605	meyerst@sullcrom.com
Jennifer L. Sutton	+1-202-956-7060	suttonj@sullcrom.com
Samuel R. Woodall III	+1-202-956-7584	woodalls@sullcrom.com
Palo Alto		
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com