wiley

ALERT

Congress Authorizes Cybersecurity Information Sharing and Other Cybersecurity Measures

December 21, 2015

On December 18, 2015, Congress passed, and the President signed, a year-end omnibus spending package which includes the Cybersecurity Act of 2015. After years of debate and failed attempts to pass legislation in both the U.S. House of Representatives and U.S. Senate, the Cybersecurity Act includes, among other things, long-sought procedures and protections to facilitate the sharing of information about cyber threats between the federal government and private entities. In addition, the Act clarifies private entities' authority to monitor their networks and to engage in limited "defensive measures." The Act reiterates the voluntary nature of covered activities, and disavows any intent to create new regulatory authorities.

Supporters of the Cybersecurity Act believe that increased, voluntary sharing of cyber threat information and other cooperative activity will allow both government and the private sector to respond more quickly to either mitigate or prevent ongoing cyberattacks.

The Cybersecurity Act has been heralded as a key element of a national effort to improve cybersecurity, against a backdrop of vigorous Executive branch activity on cybersecurity. This law's provisions will help General Counsels, Chief Information Security Officers, and others in the private sector increase their organization's cybersecurity. It will be important to carefully study the requirements of the Cybersecurity Act and the limits of each grant of authority, but a brief summary of the Cybersecurity Act and some of its key changes follows.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

The Cybersecurity Act's approach should be considered in the context of other recent federal efforts on cybersecurity, such as Executive Order 13636 on Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013), the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST), and the Cybersecurity Enhancement Act of 2014, in which Congress emphasized the role of non-regulatory agencies like NIST, and voluntary collaborative activities.

Regulators are considering their roles and authorities, with increased interest in assurances and reporting on private sector cyber readiness. The Cybersecurity Act of 2015 confirms that federal policy on cybersecurity generally has been based on voluntary action, collaboration and private sector leadership.

* * *

The Cybersecurity Act is comprised of four titles. The first, and most anticipated, governs real-time, automated information-sharing, including liability protection for the private sector. Title II focuses on other federal efforts, including federal network security. Title III aims to improve the nation's cyber workforce. Title IV addresses some discrete issues, like mobile device security in the federal government.

Title I: Cybersecurity Information Sharing Act of 2015 (CISA)

Title I's goal is to facilitate voluntary information-sharing between the private sector and the federal government, by removing certain obstacles and providing protection from liability. It also authorizes certain protective activities, and confirms its provisions are purely voluntary.

CISA Promotes Information Sharing. CISA directs the federal government, with the U.S. Department of Homeland Security (DHS) taking the lead, to develop the capability "to share cyber threat indicators and defensive measures in real time consistent with the protection of classified information." §§ 103, 105. The statute contemplates automated sharing of threat indicators between federal agencies and the private sector. The provisions balance competing interests in creating incentives for the private sector to share.

CISA Provides Immunity for Participating in Covered Sharing. In order to encourage private entities to participate, the Act provides a grant of immunity. Specifically, CISA provides that no cause of action will lie against a private entity that shares or receives cyber threat indicators or defensive measures pursuant to the Act. § 106. The Act also establishes that there is no liability for choosing not to engage in voluntary sharing. § 108(i). Finally, the Act provides an antitrust exemption for certain cybersecurity activities, clarifying that the exemption does not permit price-fixing or certain other anti-competitive behaviors. §§ 104(e), 108(e).

CISA Addresses Privacy Concerns about Shared Information. In response to privacy concerns, CISA aims to prevent private entities from knowingly disclosing personal information to the government as part of exchanging cyber threat information. Private entities sharing cyber threat indicators must manually review and remove, or use a technical capability configured to automatically review and remove, any information not directly related to a cybersecurity threat that the private entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual. § 104. Companies will need to make certain that their organization is compliant with this restriction in order to take advantage of the

Act's grant of immunity.

CISA Limits the Disclosure & Use of Shared Information. As a further incentive to share, the Act aims to limit potentially adverse uses of shared information, and restricts the federal government's ability to use the cyber threat information it obtains from private entities. These include provisions specifying that cyber threat indicators and defensive measures shared with the federal government will:

- be considered the commercial, financial, and proprietary information of the sharing entity;
- be deemed exempt from disclosure under the Freedom of Information Act and any State, tribal, or local provision of law requiring disclosure of information or records;
- be used by the federal government only for investigating and prosecuting certain enumerated crimes such as terrorism, crimes involving a serious risk of bodily injury, and computer hacking crimes;
- be retained, used, and disseminated by the federal government in a manner consistent with privacy laws;
- not be considered an *ex parte* communication;
- not be used by any federal, State, tribal, or local government to initiate an enforcement action against the sharing entity, subject to certain exceptions.

The statute further provides that the act of sharing cyber threat indicators and defensive measures does not constitute a waiver of privilege or of trade secret protection.

CISA Authorizes Some Network Monitoring. In addition to directing the government to create a real-time sharing program, the Act authorizes private entities to engage in network monitoring for "cybersecurity purposes." § 104. This includes the monitoring of an organization's own information systems as well as information that is stored on, processed by, or transits the organization's network, or the information systems of another party, with appropriate authorization and consent of the other entity. These authorizations clarify the ability of private entities to engage in activities that otherwise might have implicated prohibitions in the Electronic Communications Privacy Act or the Wiretap Act.

CISA Authorizes Limited Defensive Measures. The Act also authorizes private entities to engage in limited defensive measures to protect against intrusion. Like the provisions authorizing limited network monitoring, defensive measures are generally limited to operating on an organization's own information systems as well as information that is stored on, processed by, or transits the organization's network, or the information systems of another party, with appropriate authorization and consent of the other entity. § 104. The Act expressly excludes measures that provide unauthorized access to or substantially harms the data or information systems of another entity. § 102. Countermeasures have been controversial, and can risk transgressing the Computer Fraud and Abuse Act, which proscribes unauthorized access to protected computers and networks. Organizations seeking to rely on CISA's authorization for defensive measures should ensure that they are reviewed appropriately, and that such review takes into account the technical capabilities of any defensive measures to ensure they come within the terms of the Act.

CISA Follows a Voluntary, Non-Regulatory Approach. Title I makes plain that the activities contemplated are voluntary in nature, and are not to be used as a basis for obligations on the private sector. *See* § 108(h) (anti-tasking restriction prevents federal entities from requiring information-sharing or conditioning cooperation or the aware of any grant or contract on information-sharing by the private entity); § 108(i) (making clear that the Act is not to be "construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized in this title"). The Act expressly preempts the role of states in regulating activity authorized by the Act. § 108(k). And it expressly disavows any intent that the Act be used as a basis for regulatory activity. § 108(l).

Title II – National Cybersecurity Advancement (NCA)

The NCA is comprised of two subtitles. Subtitle A, the National Cybersecurity Protection Advancement Act of 2015, amends the functions and composition of the National Cybersecurity and Communications Integration Center (NCCIC). § 203. Among other things, Subtitle A directs NCCIC to develop capabilities in support of the automated information sharing program envisioned by the Act, § 203(g), and establishes procedures for NCCIC to enter into information sharing agreements with private entities, § 203(h).

Subtitle A also amends the statute authorizing DHS's Protected Critical Infrastructure Information (PCII) Program, 6 U.S.C. § 133, to expressly include information pertaining to "cybersecurity risks and incidents." § 204. Under the existing PCII program, private sector entities may voluntarily submit proprietary information about security practices and perceived areas of vulnerability to critical infrastructure, and DHS will protect that information subject to certain limitations.

Subtitle A also clarifies that it does not grant DHS any new authority to "to promulgate regulations or set standards relating to the cybersecurity" of private entities. § 210. Finally, Subtitle A amends or creates several reporting obligations of DHS. §§ 205-209, 211.

Subtitle B, the Federal Cybersecurity Enhancement Act of 2015, is designed to improve federal network security by authorizing DHS to employ "advanced internal defenses" "to continuously diagnose and mitigate cybersecurity risks." §§ 223, 224. The subtitle also requires federal agencies to implement network information security requirements to protect "sensitive and mission critical data." § 225. These requirements include, access control, encryption, identity management, and trusted sign-on. *Id.* The subtitle also imposes assessment and reporting obligations on federal agencies, including reporting to Congress. §§ 226, 228.

Title III – Federal Cybersecurity Workforce Assessment Act of 2015 (FCWAA)

The FCWAA requires the head of each federal agency to identify all positions within the agency that require the performance of cyber-related functions, and to assign a corresponding "employment code"—to be developed by the Office of Personnel Management in coordination with NIST—under the National Initiative for Cybersecurity Education. § 303. The information gathered from this process will be reported to Congress and form a "baseline" from which to measure future personnel needs. §§ 303, 304.

Title IV – Other Miscellaneous Matters

Title IV addresses seven relatively discrete cybersecurity issues. Notable among them is mobile device security. Section 401 commissions DHS, in consultation with NIST, to complete a study on threats relating to the security of the mobile devices of the federal government and to submit a report to Congress. The study is to "assess the evolution of mobile security techniques from a desktop-centric approach," the adequacy of such techniques, and effect cybersecurity threats may have to non-defense and intelligence federal systems. § 401 (b). The report will develop recommendations for addressing threats; identify "deficiencies" in DHS's authorities; and "develop a plan for accelerated adoption of secure mobile device technology by the department of Homeland Security." *Id.* This study could impact federal information technology strategy or procurement efforts.

Other sections of Title IV relate to the U.S. Department of State's international cyberspace policy, the apprehension and prosecution of international cyber criminals, enhancement of emergency services, improving cybersecurity in the healthcare industry, federal computer security, and stopping the fraudulent sale of financial information of people of the United States. §§ 402-407.

* * *

The Cybersecurity Act is an important legislative contribution to improving the nation's cyber readiness and response. As with any new legislation, it will be subject to interpretation and implementation. But the private sector has at its disposal several new tools and another concrete indication of the federal government's continued commitment to voluntary collaboration in the area of cybersecurity. It remains to be seen how the administrative state approaches cyber and the desire in some quarters to promote public assurances and accountability, notwithstanding the repeated emphasis by Congress on truly voluntary measures that promote collaboration and cooperation, rather than regulation.