WILMERHALE

Congress Enacts Major Cybersecurity Legislation

JANUARY 7, 2016

On December 18, 2015, Congress passed, and the President signed, the Cybersecurity Act of 2015, which provides authorization and liability protection for cybersecurity monitoring and information-sharing and authorization for cyber defensive measures. The Act, which comes after four years of efforts to enact federal cybersecurity legislation, also creates a new regime to encourage federal agencies to share cyber intelligence with the private sector more rapidly.[1]

Key provisions include:

- **Authorization and Liability Protection for Cybersecurity Monitoring, Operation of Defensive Measures, and Sharing and Receiving Cyber Threat Information.** The Act authorizes private entities, "notwithstanding any other provision of law," (a) to monitor their own information systems, the information system of another entity with written consent, and information "stored on, processed by, or transiting" such an information system;[2] (b) to share and receive cyber threat indicators or "defensive measures"[3] from other entities, with no duty to warn or act based on information received;[4] and (c) to operate defensive measures on an entity's own information system or the information system of another entity with its written consent.[5] For monitoring and information-sharing, the Act also contains liability protection provisions requiring dismissal of claims based on activities undertaken in accordance with the Act's requirements.[6] These authorizations and liability protections preempt state and local laws that "restrict[] or otherwise expressly regulate[] an activity authorized under" the Act.[7]

- **Avenues for Sharing with the Government.** Under the Act, private entities may share cyber threat information with federal entities so long as the information is shared in a manner consistent with the Act, including a variety of provisions intended to protect personal information.[8] By February 16, 2016, the Attorney General and the Secretary of the Department of Homeland Security (DHS), in consultation with the heads of other federal agencies, must provide to Congress interim policies to govern the sharing of cyber threat indicators and defensive measures with the federal government.[9] Those policies, which must be finalized by June 15, 2016,[10] will include guidance on how information will be shared and protocols for federal government agencies to automatically circulate

information received from the private sector. The Act further requires DHS, by March 17, 2016, to establish a system for the federal government to receive cyber threat indicators from the private sector through online and other electronic means.[11] But it is important to note that the process created by DHS may not limit or prohibit the sharing with federal and non-federal entities of information associated with known or suspected criminal activity or the sharing of cyber threat indicators with federal entities either in support of law enforcement investigations or in order to fulfill contractual obligations.[12]

- **Requirement To Remove Personal Information.** The Act includes provisions designed to ensure that personal information is not shared with the government or other companies. Before sharing a cyber threat indicator, the sharing entity must (a) review it to assess whether it contains information not directly related to a cyber threat that the entity knows at the time of sharing is personal information of a specific individual or information identifying a specific individual, and remove that information, or (b) employ a technical capability configured to remove such information.[13] The Act requires the government to issue guidance to assist sharing entities with identifying this type of information.[14]

- **Protections for Information Shared with the Government.** Under the Act, information shared with the government shall (a) not constitute a waiver of privilege; (b) be protected from disclosure under the Freedom of Information Act (and state equivalents); (c) not be used to regulate, including in an enforcement action, the lawful activities of a non-federal entity or activities taken by such an entity pursuant to mandatory standards; and (d) be further disclosed, retained or used by a Federal agency only for (i) a cybersecurity purpose, (ii) identifying a cybersecurity threat or vulnerability, (iii) responding to, preventing, or mitigating a threat of death, serious bodily harm, serious economic harm, or a serious threat to a minor, or (iv) investigating, disrupting or prosecuting fraud, identity theft, espionage or offenses relating to trade secrets.[15]

- **Federal Government Sharing with the Private Sector.** The Act requires the government to develop procedures to promote the timely sharing with non-federal entities of classified, declassified and unclassified cyber threat indicators and defensive measures, as well as information relating to cyber threats and cybersecurity best practices.[16]

- **Authorization for DHS To Monitor the ".gov" Environment.** The Act authorizes (and directs) DHS to deploy, operate and maintain, and to make available for use by other agencies, a capability to detect cybersecurity risks in network traffic and to prevent network traffic associated with cyber risks from transiting or traveling to or from an agency information system. The Act authorizes using contractors for this effort, and provides limits on liability for such contractors.[17]

- **Healthcare Industry Task Force.** The Act requires the establishment of a healthcare industry cybersecurity task force, led by the Department of Health and Human Services (HHS) and the National Institute of Standards and Technology (NIST), and composed of

healthcare industry stakeholders and cybersecurity experts. The task force is directed to analyze how other industries address cyber risks, assess challenges and barriers to entities in the health sector securing themselves against cyber attacks, review challenges for securing networked medical devices and electronic health records, establish a plan for information-sharing between the government and industry stakeholders, and report to Congress. HHS and NIST are also directed to develop a set of voluntary, consensus-based, and industry-led best practices for the sector.[18]

- **International Cyberspace Strategy.** The Act requires the Secretary of State, within 90 days, to produce a "comprehensive strategy" regarding US international policy in cyberspace. The strategy is to include, among other things, a review of actions taken by the Secretary to support the goal of the President's May 2011 International Strategy for Cyberspace,[19] and a plan of action to guide diplomacy on the development of international cyber norms.[20]

- **Apprehension and Prosecution of International Cyber Criminals.** The Act directs the Secretary of State to consult with officials from countries from which extradition is not likely and in which international cyber criminals are physically present, to determine what actions those governments have taken to apprehend and prosecute those criminals and to prevent them from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.[21]

---

[1] The Cybersecurity Act of 2015 was enacted as Division N in the Fiscal Year 2016 omnibus spending bill. It is available here. The Act took effect on the date of its enactment (December 18, 2015). Title I of the Act, which includes the authorization and liability protections for cybersecurity monitoring, information sharing and use of defensive measures, will remain in effect with respect to any action authorized by or information obtained pursuant to it during the period ending on September 30, 2025. Section 111.

[2] Section 104(a).

[3] A "defensive measure" is a device, measure, etc. that "detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability." Section 102(7).

[4] Sections 104(c) and 106(c).

[5] Section 104(b).

[6] Sections 106.

[7] Section 108(k).

[8] Sections 104(c)-(d), 105, 106(b).

[9] Section 105(a)(1).

[10] Section 105(a)(2).

[11] Section 105(c).

[12] Section 105(c)(1)(E) (procedures established by Secretary of DHS may not limit or prohibit (i) reporting to law enforcement agencies known or suspected criminal activity, "including cyber threat

indicators or defensive measures shared with a Federal entity in furtherance of opening a Federal law enforcement investigation," (ii) legally compelled participation in a federal investigation; or (iii) providing cyber threat indicators or defensive measures to government agencies as part of a contractual requirement).

[13] Section 104(d)(2).

[14] Section 105(a)(4).

[15] Section 105(d).

[16] Section 103.

[17] Section 223(a)(6) (amending Subtitle C of title II of the Homeland Security Act of 2002 to add Section 230).

[18] Section 405.

[19] White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (May 2011), *available here*.

[20] Section 402.

[21] Section 403.

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195