October 30, 2015

On October 27, the Cybersecurity Information Sharing Act (CISA) finally passed the Senate by a hefty margin of 74–21 **(read the text of the bill as passed)**. Despite an escalation of opposition and rhetoric over the past couple of weeks, particularly over privacy concerns, the bill passed. CISA (S.754) provides a framework by which technical indicators of compromise (what the bill calls "cyberthreat indicators") can be shared by private parties with the federal government or other private parties.

The Senate had a very difficult job—trying to provide for the protection of privacy and civil liberties while at the same time giving both the government and the private sector enough useful information to use in cybercrime investigations. To achieve this, they passed CISA in a form that permits limited use by the government of cyberthreat indicators that have been shared by the private sector. In return, the companies providing such cyberthreat indicators will receive some liability protection, including protection against civil suits.

Facing long odds, CISA overcame a number of attacks from various sides and numerous amendment attempts, and wound up striking a compromise between privacy and security that was acceptable to a majority vote. As Sen. Richard Burr stated on the Senate floor last Thursday, "[w]e have reached a very delicate balance. There have been bending and twisting and giving and taking, and we have done it not only within the Senate of the United States and within the committee, we have done it with stakeholders all around the country."

The balance consists of a number of privacy protections, including a requirement in Sec. 104(d)(2)(B) that anyone sharing a cyberthreat indicator "review such cyber threat indicator to assess whether such cyber threat indicator contains any information that the entity knows at the time of sharing to be personal information." If such personal information does exist, the entity must "remove any information contained within such indicator that the entity knows at the time of sharing to be personal information."

Further, for any cyberthreat indicators shared with the federal government, those cyberthreat indicators will be subject to (a) general policies and procedures (that still need to be developed) and (b) "guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity." In addition (and perhaps most significantly), CISA mandates that the Federal government may only use cyberthreat indicators for six limited purposes. Those are:

> (i) a cybersecurity purpose; (ii) the purpose of identifying a cybersecurity threat…; (iii) the purpose of identifying a cybersecurity threat involving the use of an information system by a foreign adversary or terrorist; (iv) the purpose of responding to, or otherwise preventing or mitigating, an imminent threat of death, serious bodily harm, or serious economic harm…; (v) the purpose of responding to, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or (vi) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat [involving identity theft, fraud, espionage, or theft of trade secrets].

Other than those six enumerated purposes in Sec. 105(d)(5)(A), "cyberthreat indicators and defensive measures provided to the Federal Government under this title shall not be disclosed to, retained by, or used by any Federal agency or department for any [other] use."

Balanced against these privacy protections, CISA protects entities that share cyberthreat indicators by stating that "[n]o cause of action shall lie or be maintained in any court against any entity, and such action shall be promptly dismissed, for the sharing or receipt of cyber threat indicators or defensive measures…if (1) such sharing or receipt is conducted in accordance with this title;

and (2) in a case in which a cyber threat indicator or defensive measure is shared with the Federal Government, the cyber threat indicator or defensive measure is shared in a manner that is consistent with [the privacy protection provisions in CISA]."

On the House side, two information sharing bills passed earlier in the year. While passing CISA in the Senate was clearly a major achievement, much work remains to resolve the House bills with CISA. Sen. Diane Feinstein, a clear supporter of CISA, remarked that there is still "a long road ahead" for actually passing an information sharing law by Congress and that specific timing for the conference negotiations between the House and Senate was not clear.

If CISA were to pass into law in a form similar to its current text, the perceived benefit would be that companies would now have certainty around two different aspects of information sharing. First, they presumably would be able to take comfort in knowing they will be protected from lawsuits if they do share cyberthreat indicators with the government. Second, companies would be able to gain intelligence from cyberthreat indicators that the government would be able to share with them. Opponents contend that both of these can already be done today, though perhaps not in such a centralized and controlled fashion. For some further detailed information about how CISA might affect companies in the healthcare space, see our **additional alert**.

Key Contacts

Matthew D. Brown San Francisco	brownmd@cooley.com +1 415 693 2188
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090
Vince Sampson Washington, DC	vsampson@cooley.com +1 202 728 7140