Akin Gump
STRAUSS HAUER & FELD LLP

Cybersecurity, Privacy & Data Protection Alert

December 22, 2015

If you read one thing...

- The omnibus appropriations package includes legislation that provides liability protection to companies who voluntarily engage in cybersecurity information sharing.
- The legislation seeks to increase the pace and volume of information sharing to help identify and defend against threats and limit the period of time and number of instances for which a particular attack can be repeated effectively.
- With many changes forthcoming, companies who share cybersecurity threat information already, and those who do not do so yet but may be interested in doing so, should follow developments across a number of fronts.

Cybersecurity Information Sharing Legislation Passes in Omnibus

On December 18, the House and Senate passed an omnibus appropriations package that not only funds the federal government through the remainder of fiscal year 2016, but also includes legislation that provides liability protection to companies that voluntarily engage in cybersecurity information sharing with one another or with the federal government, subject to privacy and other requirements. The legislation is designed to encourage greater and more timely sharing of cybersecurity threat information by reducing legal barriers to doing so, including the threat of litigation and increased regulatory action, while protecting private information.

The new law combines parts of three different cybersecurity information sharing bills previously passed by either the House or Senate in 2015 with strong bipartisan support and encouragement from President Obama. The business community, with some exceptions in the tech sector, has strongly supported the legislation, while privacy and civil liberties groups have opposed it. The legislation intends to foster more cybersecurity information sharing on a real-time or near-real-time basis, both among companies and between companies and the federal government by providing liability and certain confidentiality protections to businesses that share cybersecurity threat information stripped of sensitive privacy information. The idea is that businesses own much of the infrastructure and data being attacked, but the government also has relevant information, and that increasing the pace and volume of information sharing can (i) help identify and defend against threats and (ii) limit the period of time and number of instances for which a particular attack can be repeated and work effectively.

As interpretation and implementation of the new legislation proceeds, companies that can benefit from cybersecurity information sharing, which may be most, will want to learn and understand the requirements for preserving liability protection. It can also be expected that, over time, there increasingly may be private sector contract requirements that vendors participate in an information sharing organization.

Selected Key Information Sharing Provisions

- The legislation:
    - authorizes private entities expressly to monitor their information systems, share and receive cybersecurity threat and defense information and take defensive measures
    - requires all federal and non-federal entities that participate in cyber threat sharing to protect the data they collect, maintain and share from unauthorized access and disclosure
    - requires the scrubbing of personally identifiable information before a threat indicator is shared.
- The Department of Homeland Security (DHS) provides the "portal" through which cyber threat information will be shared by private companies with the federal government and later distributed to other agencies as necessary. DHS also has responsibilities to maintain personal privacy and civil liberties protections, and it must offer an automated sharing process. (The president can designate another point for sharing after taking certain steps, but not the Department of Defense, including the National Security Agency).
- To preserve liability protection, non-federal entities that share information with the federal government must do so through DHS and are required to remove from cyber threat indicators information that the entity "knows at the time of sharing" to be personally identifiable information.
- Private entities that receive or share threat information are not liable for failing to warn or act based on receiving or providing such information.
- Threat information shared with the federal government will not be used to regulate lawful activities, nor does it waive any privilege or protection. It may be deemed proprietary information by the sharing party and is exempt from certain disclosure laws.
- No cause of action shall be brought against a private entity for the monitoring of information systems or the sharing or receipt of cyber threat indicators, so long as those actions are conducted in accordance with the provisions of the Act.
- The Department of Justice (DOJ) and DHS must jointly develop interim policies for sharing of information with the federal government and private entities within 60 days, and full policies within 180 days of enactment. Within 60 days of enactment, DOJ and DHS are also required to develop guidelines for private entities sharing information with the federal government. Further, DOJ and DHS must develop privacy and civil liberty protection guidelines within 180 days of enactment (interim guidelines required within 60 days).

- The federal government cannot compel or coerce companies to participate and cannot condition other benefits or contracts on participation.
- Most provisions sunset after 10 years.

Additional Cybersecurity Titles

The omnibus bill contains three other titles related to cybersecurity. The first instructs DHS to develop procedures to facilitate voluntary, automated cyber threat sharing between non-federal entities and DHS's National Cybersecurity Communications and Information Center. It also contains the Federal Cybersecurity Enhancement Act, which amends the Homeland Security Act to require federal agencies, under DHS's lead, to strengthen their cybersecurity protection, detection and mitigation systems, as well as a liability shield for private entities that "provide assistance to the secretary [DHS]" in carrying out the provisions of the Act.

The second title contains the Federal Cybersecurity Workforce Assessment Act, which focuses on reviewing and improving the federal cybersecurity workforce by identifying agencies' cybersecurity workforce needs and reporting such needs to Congress.

The third title is a collection of other cybersecurity provisions, including Section 404, which would require DHS to establish, within 90 days of enactment, a process by which a "Statewide Interoperability Coordinator" may report data on any cybersecurity risk or incident involving any information system or network used by emergency responders. The provisions would require DHS to use that data to develop information and recommendations on security and resilience measures for any information system or network used by state emergency response providers within one year of enactment.

Section 405 of that title would require a report to Congress by the secretary of Health and Human Services (HHS) on the preparedness of HHS and health care industry stakeholders in responding to cybersecurity threats. Following a report by a health care industry task force to be created under this section, HHS would then be required to establish a common set of voluntary, industry-led guidelines that support voluntary adoption and implementation of safeguards to address cybersecurity threats. The section includes liability protection for health care industry stakeholders that choose not to engage with HHS during this process.

Conclusion

Cybersecurity information sharing legislation has been sought for years on a bipartisan basis across multiple Congresses. With passage, work now turns to implementation by DHS and other agencies on a relatively short timetable. While implementation of the legislation moves forward, there also is a separate ongoing effort by a standards organization already under contract with DHS pursuant to an executive order to develop additional standards and guidelines to facilitate cybersecurity information sharing. Thus, companies that share cybersecurity threat information already, and those that do not do so yet but may be interested in doing so, should follow developments across a number of fronts.

If not already understood thoroughly, businesses should review the personal data they collect, their IT security systems and how they may benefit from sharing or receiving cyber threat indicators with other businesses and with the federal government.

Contact Information

If you have any questions regarding this alert, please contact:

David S. Turetsky
Partner
dturetsky@akingump.com
+1 202.887.4074 | Washington, D.C.

Matthew Thomas
Senior Public Policy Specialist
mthomas@akingump.com
+1 212.872.1000 | Washington, D.C.

Francine E. Friedman
Senior Policy Counsel
ffriedman@akingump.com
+1 202.887.4143 | Washington, D.C.

Natasha G. Kohne
Partner
nkohne@akingump.com
+971 2.406.8520 | Abu Dhabi
+1 415.765.9500 | San Francisco*

Michelle A. Reed
Partner
mreed@akingump.com
+1 214.969.2713 | Dallas

Ed Pagano
Partner
epagano@akingump.com
+1 202.887.4255 | Washington, D.C.

Jo-Ellyn Sakowitz Klein
Senior Counsel
jsklein@akingump.com
+1 202.887.4220 | Washington, D.C.

*Licensed to practice for 15 years in New York. Practicing in California under the supervision of the partners of Akin Gump Strauss Hauer & Feld LLP. Application for admission to the California Bar pending.