Client Update
The Cybersecurity Information Sharing Act

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Max Shaul
mshaul@debevoise.com

WASHINGTON, D.C.

David A. O'Neil
daoneil@debevoise.com

Significant new cybersecurity legislation was signed into law by President Obama over the holidays. The Cybersecurity Information Sharing Act, or CISA ("SEE-sa") for short, is a revised version of a bill that passed the Senate last fall. Notably, CISA provides a safe harbor from liability to companies for the voluntary sharing of "cyber threat indicators" and "defense mechanisms" with the federal government. CISA is not industry-specific and thus has implications for a wide range of companies.

BASICS OF THE BILL

The premise of CISA is that we are all generally better off when companies engage in robust monitoring of cyberthreats and robust sharing of threat information. If Company A shares what it knows, the argument goes, then Company B (and Companies C, and D . . .) can use that information to improve their own defenses. Sharing also may help law enforcement and other public-sector players to take action against the threat. Yet there is a perception that concerns such as confidentiality, trade secrets and privacy historically may have made companies reluctant to monitor and share.

CISA aims to break down that reluctance. Specifically, the new statute:

- Requires that the Department of Homeland Security ("DHS") establish a portal for collection of threat information, and a system for dissemination of the information to private- and public-sector entities.
- Provides that a private entity may, for cybersecurity purposes, monitor (i) information systems of its own; (ii) information systems of other private entities (upon receiving authorization and written consent); (iii) information systems of the U.S. government (upon receiving authorization and written consent); and (iv) information that is stored on, processed by, or transmitted via an information system monitored by such private entity.

- Provides that private entities may establish certain cyberdefenses, such as firewalls or other intrusion prevention systems, provided the measures do not "destroy[], render[] unusable, provide[] unauthorized access to, or substantially harm[]" an information system of another (or information stored thereon) without prior consent.
- Protects private entities from liability from causes of action based on the monitoring of an information system or the sharing or receipt of threat information. CISA also guarantees the prompt dismissal of any such causes of action. To receive protection, the monitoring, sharing or receipt, must be conducted in accordance with all other requirements of CISA.

CISA includes belt-and-suspenders privacy safeguards: A private entity must remove personally identifying information about individuals before sharing with DHS, and DHS must confirm removal of all such information before making any subsequent disclosure. Information shared in accordance with CISA is exempt from Freedom of Information Act requests. CISA expressly creates no "duty to share a cyber threat indicator or defensive measure," and no "duty to warn or act based on the receipt" of the same.

Important details remain to be filled in. Within 60 days after enactment, the Director of National Intelligence, in consultation with the heads of the appropriate federal agencies, must submit to Congress procedures for facilitating and promoting the sharing of information by the federal government. DHS and the Department of Justice ("DOJ") must within 60 days of enactment jointly develop (i) interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the federal government and (ii) interim guidelines relating to privacy and civil liberties; each of these must be finalized within 180 days of enactment. Within 90 days after enactment, DHS, in coordination with other relevant agencies, must develop and implement the portal for accepting cyber threat indicators and defensive measures.

CONSIDERATIONS FOR COMPANIES

Over time, CISA likely will have many implications for organizations of all kinds. Here are a few initial thoughts on its practical effects.

Adjustments to Policies and Procedures

Companies likely will want to build at least three new mechanisms into their cybersecurity policies and procedures: (i) a mechanism for considering when to report a threat to the DHS portal; the statute provides no specific guidance on what constitutes a reportable event; (ii) a mechanism for actually submitting

information to the portal with care - the safe harbor does not apply if, for example, a company fails to strip out personally identifiable information; (iii) and a mechanism for acting on threat information that DHS shares. CISA itself imposes no substantive standards for cybersecurity, and (as noted) imposes no duty to act on information shared by DHS. But neither does it bar courts, regulators and enforcement agencies from seeking to impose liability on companies for their cybersecurity failings. The CISA safe harbor applies only to the acts of monitoring and sharing.

Disclosure Issues

Longstanding SEC guidance calls for public companies to disclose "cybersecurity risks and cyber incidents," as well as the costs and other consequences of those risks and incidents, to their investors to the extent such disclosure would be material. No specific level of detail is mandated, but the SEC cautions that "generic 'boilerplate' disclosure" is to be avoided. Companies will want to keep an eye on any evolving interplay between this disclosure obligation and their CISA disclosures. Depending upon the particular facts and circumstances, disclosure of a risk to the DHS portal could be seen as an indicator of materiality necessitating disclosure of the same risk to the market.

Vendor Relationships

Companies also will want to monitor how CISA affects their relationships with key vendors. For example, companies that outsource the storage of sensitive information might inquire with vendors about their own CISA compliance practices. In some cases, it might be appropriate to contractually mandate that vendors participate in CISA information sharing, or that the same information a vendor shares with DHS must also be shared with the contract counterparty.

Privacy

Companies should pay particular attention to the DOJ/DHS privacy procedures as they are developed and promulgated, and should consider taking advantage of any opportunity that is provided to comment on such procedures.

* * *

We are available to discuss any questions that our clients and friends may have about CISA.