MINTZ

Happy New Year - Cybersecurity Information Sharing Act

January 04, 2016 | Blog | By **Christopher J. Harvie**, **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Just at the end of 2015, the Cybersecurity Information Sharing Act (CISA) was enacted into law as part of the omnibus spending measure passed by Congress and signed by President Obama at right before Christmas. The legislation combines elements from the versions of CISA that passed the House in April of 2015 and the Senate in October.

Enactment of CISA was driven by the goal of clearing away some of the legal uncertainty and liability risk concerns inhibiting sharing of cybersecurity threat information. Cyber criminals are technologically proficient and constantly innovating, which means that protecting American enterprise networks, industrial control systems, and electronic information systems requires continued vigilance and innovation. There is broad agreement that the nation's cyber defense posture could be greatly strengthened through more robust and timely sharing of cyber threat information both between the government and the private sector and between private companies themselves.

Federal statutes, however, such as the Wiretap Act, the Stored Communications Act (collectively knowns as the Electronic Communications Privacy Act (ECPA)), have created uncertainty regarding the permissibility of sharing of cyber threat information in certain circumstances. In addition, uncertainty regarding the breadth and application of ECPA, and certain other Federal and State laws, also can constrain monitoring of network traffic for cyber threats and operating countermeasures to combat a threat or attack. In the fluid and dynamic environment of an ongoing cyber incursion, the delay and deliberation involved in examining whether a piece of threat information can be shared or whether the most effective defensive measure can be deployed can mean the difference between successfully deterring or mitigating an attack and watching it grow or proliferate.

CISA is designed to bolster the nation's cyber defenses by mitigating liability risks that may be inhibiting companies from sharing cybersecurity threat information and taking other steps that can help detect and deter attacks on information systems and critical infrastructure. The aim of CISA is to promote *voluntary* information sharing, and the bill specifically states that it is not intended to subject any entity to liability for choosing not to participate in any of the voluntary activities authorized in the legislation.

Key elements of the bill include:

- Authorizing private entities, notwithstanding any other law and for cybersecurity purposes, to monitor their network for cybersecurity threats and to obtain and share threat information with other private entities and the Federal government;

- Authorizing private entities, notwithstanding any other law and for cybersecurity purposes, to operate defensive measures applied to their networks to protect those networks from cybersecurity attacks. The defensive measures authorization provision does not include measures that adversely impact third party networks or data.

- Establishing a process lead by the Department of Homeland Security for sharing and receipt of cybersecurity threat information by the Federal government – including real-time-sharing of cyber threat indicators and sharing of classified cyber threat intelligence with private entities with appropriate security clearances.

- Affording companies specific liability protection for monitoring their networks for cybersecurity purposes and for sharing or receiving information cyber threat information in accordance with the Act. Consistent with the Congressional establishment of a voluntary sharing framework, the bill legislation disclaims any intention of creating a duty to share cyber threat indicators or defensive measures or a duty to warn or act based on the receipt of such indicators or measures.

Companies engaged in information sharing must, prior to sharing cyber threat information, review and remove any information not directly related to a cybersecurity threat which is known at the time of sharing to be personal information of, or identifying, a specific individual, or must implement and utilize a technical capability to do the same.

Cyber threat information shared with the Federal government is considered proprietary information of the sharing entity, exempt from disclosure under the Freedom of Information Act, and generally prohibited from being used for regulatory purposes by Federal or State agencies. Cyber threat information shared with the Federal government may be used by agencies with specific authority to mitigate cyber threats to information system to “inform” the development or implementation of regulations relating to such information systems.

Along with CISA, the omnibus measure also includes provisions that enhance the functions of DHS’ existing National Cybersecurity and Communications Integration Center, enshrining it as the lead Federal civilian interface for multi-directional and cross-sector information exchange related cybersecurity risks, incidents, analysis and warnings. In addition, the bill authorizes NCCIC to enter into voluntary information sharing relationships with individual private companies for the sharing of cyber threat indicators, defensive measures, and information for cybersecurity purposes.

Authors

Christopher J. Harvie, Member

Christopher J. Harvie assists cable operators, broadband companies, and content providers with legal, policy, and legislative matters. He represents Mintz clients before federal and state agencies and on Capitol Hill. Chris's practice focuses on privacy, cybersecurity, and broadband policy.

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.