Published on *The National Law Review* https://natlawreview.com

Closer Look at CISA's Cybersecurity Information-Sharing Provisions

Article By:

David N. Fagan

Ashden Fein

David J. Bender

As we reported on October 27, the U.S. ***Senate*** passed the ***Cybersecurity Information Sharing Act*** ("***CISA***," S. 754). If enacted into law, CISA would, among other things, establish a voluntary framework for the sharing of cybersecurity threat information between and among the federal government and private entities. CISA must now be reconciled with two similar bills that the House passed in April before it can be sent to the President and enacted into law. According to CISA's co-sponsor Sen. Richard Burr (R-NC), a conference version of CISA will not be available for review until January 2016, at the earliest. Below is a deeper explanation of CISA's four Titles and how they purport to improve cybersecurity.

Title I: Cybersecurity Information Sharing Act of 2015

Title I establishes the core cybersecurity information sharing framework to include, among other issues, what information can be shared by the government and private entities, liability protections for entities that share, and government oversight of the programs the Act establishes. Outlined below are key sections of CISA.

Section 103 outlines how the federal government can share certain cybersecurity information with other entities—both private and public. Specifically, this section establishes that within 60 days of enactment, the Director of National Intelligence, the Secretaries of Homeland Security and Defense, and the Attorney General, in consultation with other heads of federal entities, "shall develop and promulgate procedures to facilitate and promote" sharing of the following:

- classified cyber threat indicators to appropriately cleared individuals (which would include individuals in the private sector who possess such clearances), and cyber threat indicators or other related information that are unclassified (including declassified or controlled unclassified information);

- information about cybersecurity threats to “prevent or mitigate adverse effects from such cybersecurity threats;” and

- “best practices that are developed based on ongoing analysis of cyber threat indications and information in possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns….”

The section also establishes the following requirements, limitations, and civil-liberty protections that must be considered in the development of the information-sharing procedures:

- the government must maintain “the capability to share cyber threat indicators in real time consistent with the protection of classified information;”

- the procedures must attempt to incorporate “existing processes and existing roles and responsibilities of Federal and non-Federal entities for information sharing by the Federal government[,]” which includes information sharing and analysis centers (“ISACs”);

- the government must notify entities if certain cyber threat indicators are shared with an entity “in error or in contravention of the requirements of this title or another provision of Federal law or policy…;”

- federal entities that share information must have security controls in place to protect against unauthorized access to the information;

- the procedures must include a process that requires, before sharing information, the government to: (i) review information to assesses whether it “contains any information that [the government] knows at the time of sharing to be personal information in information that identifies a specific person *not related to a cybersecurity threat* and remove such information;” or (ii) develop and use an automated process to remove personal information from the data “that identifies a specific person *not directly related to a cybersecurity threat*”; and

- the government must notify “any United States person whose personal information is known or determined to have been shared” by the government in violation of the Act.

Section 104 generally authorizes procedures for “preventing, detecting, analyzing, and mitigating cybersecurity threats.” The section specifically authorizes private entities to monitor or deploy “defensive measures” on their own systems for “cybersecurity purposes”—or, with written consent, a third-party’s system, including the federal government’s. It also authorizes private entities to share cyber threat indicators or defensive measures with other private entities or the federal government. Similar to the control required in Section 103, private entities must implement security controls for the information and remove information that the entity “knows at the time of sharing” to be personally identifiable. Section 104 also provides disclosure prohibitions for State, tribal, and regulatory authorities—such properly shared information is exempt from laws requiring disclosure of information or records and is prohibited from being used directly by “any State, tribal, or local government to regulate, including an enforcement action….”

This section also exempts the exchange of cyber threat indicators, “or assistance relating to the

prevention, investigation, or mitigation of a cybersecurity threat," from "any provision of *antitrust laws*." Specifically, this exemption applies to information that is shared or assistance provided with "facilitating the prevention, investigation, or mitigation of a cybersecurity threat" or "communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat." However, under Section 108(e), the antitrust exemption does not apply to "price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning."

Section 105 outlines how private and public entities can share certain cybersecurity information with the federal government through the Department of Homeland Security. Similar to the above sections, the Attorney General and Secretary of Homeland Security, in consultation with other heads of federal entities, must develop policies and procedures, subject to certain requirements, limitations, and civil-liberty protections. The following are examples of the specifications:

- the government must develop a real-time sharing (or as close to real-time sharing as possible) mechanism for both the private entities and intra-government sharing;
- information shared with the Department of Homeland Security will automatically forward to "appropriate Federal entities," defined as the Departments of Commerce, Defense, Energy, Justice, and the Treasury, as well as the Office of the Director of National Intelligence;
- the government must develop audit capabilities for "officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this title in an unauthorized manner;"
- the government may only use the information in a manner that it be "disclosed to, retained by, and used by" the federal government for "a cybersecurity purpose," with accompanying regulatory authority limited to "the prevention or mitigation of cybersecurity threats;"
- information shared with the government is exempt from the Freedom of Information Act;
- sharing of such information "shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection" and the information may be considered the "commercial, financial, and proprietary information" of a submitting entity, if so designated at time of submission; and
- shared information "shall not be directly used by any Federal, State, tribal, or local government to regulate, including enforcement action, the lawful activities of any entity, including activities relating to monitoring, operating defensive measures, or sharing cyber threat indicators" except if used to "inform the development or implementation of regulations relating to such information systems."

Section 106 establishes liability protections for certain monitoring and information sharing activities. Specifically, the section establishes that "[n]o cause of action shall lie or be maintained in any court against any private entity" for the monitoring and sharing of cyber threat indicators or defensive measures authorized by Section 104. The protection is limited, however, in that it does not apply to "gross negligence or willful misconduct," and does not "undermine or limit the availability of otherwise applicable common law or statutory defenses." In addition, the liability protections do not

apply to “any action that solely involves violation of a consumer term of service or a consumer licensing agreement,” which are excluded from the definition of “cybersecurity threat.”

Section 108 makes clear that CISA’s information-sharing framework is explicitly voluntary. The section outlines that the government cannot “require an entity to provide information” to the government or another third party and no liability exists “for choosing not to engage in the voluntary activities authorized in this title.”

Titles II-IV

Title II (*“Federal Cybersecurity Enhancement Act of 2015”*) establishes new cybersecurity-related requirements for the federal government or amends existing laws focused on cybersecurity, including improving federal network security, advancing internal defenses, and establishing specific reporting requirements.

Title III (*“Federal Cybersecurity Workforce Assessment Act of 2015”*) establishes new cybersecurity-related requirements for assessing the cyber-readiness of the federal workforce, including identifying certain cyber-related roles as being critical, requiring each federal agency to develop a process to account for its cybersecurity manpower needs, and require certain Government Accountability Office reports.

Title IV (*“Other Cyber Matters”*) contains an assortment of cybersecurity-related provisions. A number of these provisions impose requirements on the federal government relating to cybersecurity to include the following: authorizations for a government study on mobile device security, development of an international cyberspace policy strategy at the Department of State, coordination by the Department of State with other countries for the apprehension and prosecution of international cyber criminals, and reports to Congress on the state of federal computer security. The remaining provisions directly involve or affect the private sector to include the following: the development of voluntary cybersecurity best practices for emergency response providers and the healthcare industry, the development of mitigation strategies for cybersecurity incidents that effect critical infrastructure, and an amendment to the access device fraud statute, 18 U.S.C. § 1029, to allow for the prosecution of foreign individuals for access device fraud even if none of their assets are within the jurisdiction of the United States.

National Law Review, Volume V, Number 313