Section by Section

CYBERSECURITY INFORMATION SHARING LEGISLATION

Sec. 101. Purpose.

This section states that the purpose of the legislation is to codify mechanisms for enabling cybersecurity information sharing between private and government entities, as well as among private entities, to better protect information systems and more effectively respond to cybersecurity incidents.

Sec. 102. Definitions.

This section sets forth relevant definitions, including "cyber threat," "Federal entity," "malicious cyber command and control," "malicious reconnaissance," "operational control," "technical control," and "technical vulnerability," among others.

The proposal defines "cyber threat indicator" as "information—

(A) that is necessary to indicate, describe or identify —

(i) malicious reconnaissance, including communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cyber threat;
(ii) a method of defeating a technical or operational control;
(iii) a technical vulnerability;
(iv) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system inadvertently to enable the defeat of a technical control or an operational control;
(v) malicious cyber command and control;
(vi) any combination of (i)-(v).

(B) from which reasonable efforts have been made to remove information that can be used to identify specific persons reasonably believed to be unrelated to the cyber threat."

Sec. 103. Authorization to Provide Cyber Threat Indicators.

Section 103 authorizes any private entity to disclose lawfully obtained cyber threat indicators, notwithstanding any other provision of law, to private information sharing and analysis organizations and to the Department of Homeland Security's National Cybersecurity and Communications Integration Center.

This section also states that any entity may disclose lawfully obtained cyber threat indicators to a Federal entity for investigative purposes consistent with its lawful authorities.

This section also states that private entities that disclose or receive cyber threat indicators under this section may only use, retain, or further disclose cyber threat indicators for the purpose of protecting an information system from cyber threats, identifying or mitigating such threats, or for reporting a crime. It also requires private entities to take reasonable efforts to minimize

information that can be used to identify specific persons and is reasonably believed to be unrelated to a cyber threat, to safeguard information that can identify a specific person from unauthorized disclosure, and to comply with reasonable restrictions that another private entity places on further disclosure of a cyber threat indicator to a third-party private entity.

Sec. 104. Private Information Sharing and Analysis Organizations.

Section 104 requires the Secretary of Homeland Security, in consultation with the Secretary of Commerce, the Attorney General, the Director of the Office of Management and Budget, the heads of sector-specific agencies and other appropriate Federal agencies, to select through an open and competitive process, a private entity to identify, or develop if necessary, a common set of best practices for the creation and operation of private information sharing and analysis organizations.

Sec. 105. Civilian Cyber Threat Indicator Portal.

This section directs the Secretary of Homeland Security to designate the National Cybersecurity and Communications Integration Center (NCCIC) to receive and distribute cyber threat indicators in as close to real time as practicable, consistent with, and in accordance with the purposes of, the Act.

This section also requires the Secretary of Homeland Security, in coordination with the Attorney General, and in consultation with other Federal agencies, to ensure that cyber threat indicators are shared with other Federal entities in as close to real time as practicable.

Sec. 106. Limitation of Liability.

This section provides that no civil or criminal cause of action shall lie or be maintained in any Federal or State court for the voluntary disclosure or receipt of a lawfully obtained cyber threat indicator consistent with the requirements of the Act, and that the entity was not otherwise required to disclose, to or from the NCCIC or a private information sharing and analysis organization, if such organization maintains a publicly-available self-certification that it has adopted the best practices described in Section 104.

This section also ensures that cyber threat indicators shared with the NCCIC, pursuant to the legislation, will be protected from disclosure under the Freedom of Information Act and State laws requiring disclosure and may not be used as evidence in a regulatory enforcement action against the entity that disclosed such cyber threat indicator.

Sec. 107. Privacy Protections.

Section 107 requires the Attorney General, in coordination with the Secretary of Homeland Security, and in consultation with the Chief Privacy and Civil Liberties Officers at DHS and DOJ and the Privacy and Civil Liberties Oversight Board, among other Federal agencies, to develop and periodically review policies and procedures that govern the receipt, retention, use, and disclosure of cyber threat indicators by Federal entities.

The procedures will require the government to: (1) reasonably limit the acquisition, interception, retention, use and disclosure of cyber threat indicators reasonably likely to identify specific

persons, consistent with the need to carry out the responsibilities of the Act; (2) establish a process for timely destruction of information known not to be directly related to a cyber threat; (3) establish a process to anonymize and safeguard information; and (4) protect the confidentiality of proprietary information, among other things.

This section also directs the Attorney General to develop guidelines to permit law enforcement use of cyber threat indicators only for computer crimes; threats of death or serious bodily harm; serious threats to a minor, including sexual exploitation and threats to physical safety; or attempts or conspiracies to commit those offenses.

Sec. 108. Construction and Federal Preemption.

Section 108 provides that nothing in the bill may be construed to limit an entity's authority to share information about potential criminal activity or investigations with law enforcement or interfere with existing sharing relationships between private entities and the government. In addition, the section provides that nothing shall be construed to permit price-fixing or market allocation between competitors.

Additionally, this section provides that this Act preempts any law or requirement of a State or political subdivision of a State that restricts or otherwise expressly regulates the retention, use, or disclosure of cyber threat indicators by private entities to the extent such law contains requirements inconsistent with the bill, but preserves all other state laws or requirements.