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

Analysis of President Obama's Information Sharing Legislation

Article By:

David N. Fagan

On Tuesday, President Obama announced his proposal for legislation that would encourage sharing of cyber threat information between the public and private sector by shielding private entities from liability for sharing information on cyber threats. The White House has since released the text of the proposed bill, which includes limitations on liability for private entities along with a mandate to develop policies and procedures to address privacy concerns. In comparison with previous failed attempts to enact similar legislation, the current White House proposal offers increased privacy protections and more narrowly defined exemptions from liability, but it remains to be seen whether this proposal can succeed where others have failed.

The proposed bill provides for the voluntary sharing of "cyber threat indicators," which the bill defines to include information necessary to indicate, describe, or identify the following:

- malicious reconnaissance, including communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cyber threat;
- a method of defeating a technical or operational control;
- a technical vulnerability;
- 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;
- malicious cyber command and control; or
- any combination of the above.

Prior to sharing any cyber threat indicators, an entity must make reasonable efforts to remove information that can be used to identify specific persons unrelated to the threat.

The proposed bill designates the National Cybersecurity and Communications Integration Center

(NCCIC), recently codified under the *National Cybersecurity Protection Act of 2014*, as the entity that will receive cyber threat information and distribute it to federal agencies and other recipients "in as close to real time as practicable." Any private entity can disclose lawfully obtained cyber threat indicators to the NCCIC or to "private information sharing and analysis organizations." Private entities can also disclose cyber threat information to federal entities for investigative purposes. For private entities that receive cyber threat information from the NCCIC or others under these provisions, the bill would limit how they can use, retain, or disclose that information.

Under the proposed bill, private entities would be exempt from civil or criminal liability for the voluntary disclosure of lawfully obtained cyber threat information to the NCCIC, or the receipt of such information from the NCCIC, unless the entity was separately required to disclose such information. The bill would exempt cyber threat indicators shared with the NCCIC from disclosure under FOIA and comparable state laws, and regulators would be unable to use such information as evidence in regulatory proceedings against the entity that disclosed it.

The bill also extends this liability protection to sharing of cyber threat indicators with private information sharing and analysis organizations if the organization maintains a publicly available self-certification that it has adopted the best practices for such organizations that will be developed under this bill. The Secretary of Homeland Security, in consultation with other federal agencies, will lead a process to select a private entity to identify or, if necessary, develop a common set of best practices for the creation and operation of private information sharing and analysis organizations.

In addition, the bill addresses the privacy concerns inherent in the sharing of cyber threat information between the public and private sectors by directing the Attorney General, in consultation with other federal officials, to develop and periodically review policies and procedures for the federal government's receipt, retention, use, and disclosure of cyber threat indicators. According to the proposed bill, these policies and procedures should reasonably limit the government's acquisition, use, and disclosure of information that is reasonably likely to identify specific individuals. In addition, the policies and procedures should protect the confidentiality of proprietary information and establish a process for anonymization and timely destruction of information when appropriate. Finally, the bill would direct the Attorney General to develop guidelines that would limit law enforcement use of cyber threat information to investigations of computer crimes, threats of death or serious bodily harm, or serious threats to a minor.

The current bill follows a multi-year effort by both parties to overcome privacy concerns and pass legislation that would shield private entities sharing cyber threat information with the federal government from liability. In May 2011, President Obama proposed a bill that included immunity from suit for private entities that voluntarily shared cyber threat information with the Department of Homeland Security, but the measure failed to pass Congress, in part due to privacy concerns. President Obama opposed a subsequent measure, the Cyber Intelligence Sharing and Protection Act (CISPA), which failed to pass the Senate in 2013. The Cybersecurity Information Sharing Act of 2014, which would have provided for real-time sharing of cyber threat information between the federal government and private entities, stalled in the Senate.

Although the White House's most recent proposal contains many of the same elements as these previous bills, there are several key differences between the proposed bill and CISPA. Most importantly, the current bill requires the development of policies and procedures to curtail the use and sharing of information that would identify specific individuals, as well as policies that would restrict law enforcement use of the shared information. The proposed bill also requires entities to remove information that would identify specific individuals prior to sharing cyber threat information, while a

similar provision was offered as an amendment to CISPA but not adopted. In addition, the proposed bill contains a narrower exemption from liability than CISPA, which would have exempted private entities from liability for using cybersecurity systems to identify cyber threat information, for sharing such information, and for decisions based in good faith upon such information. However, the current bill does not include a CISPA provision that would have provided a cause of action against the federal government for violations of information sharing restrictions. These differences from previous information sharing proposals may determine whether President Obama's proposed bill will usher in an era of increased sharing of cyber threat information between the private sector and the federal government.

National Law Review, Volume V, Number 15