CRS Reports & Analysis

Legal Sidebar

Senate Passes Cybersecurity Information Sharing Bill – What's Next?

10/28/2015

After several years of legislative debate on how to reconfigure the legal framework for the collection, sharing, and use of cyber-threat information amongst the private sector and the government, on Tuesday October 27th, the Senate voted 74-21 to pass S. 754, the Cybersecurity Information Sharing Act of 2015 (CISA). CISA generally attempts to clarify the often-murky legal landscape that impacts cybersecurity information sharing, as current efforts are governed by a host of different laws, including tort, privacy, and antitrust laws, that proponents of CISA argue chill private entities' willingness to share cyber-threat information with each other and the government. While the passage of CISA marks the first time the upper chamber has passed a comprehensive bill respecting cybersecurity information, CISA now heads to a joint-conference committee where negotiations will reportedly occur over how to reconcile the Senate bill with two pieces of legislation – H.R. 1560 (Protecting Cyber Networks Act or PCNA) and H.R. 1731 (National Cybersecurity Protection Advancement Act OR NCPAA) – that were passed by the House of Representatives in April of this year.

So what are the major differences between the two House cybersecurity information bills and CISA? Here are **five areas** where the three bills differ and may be the center of negotiations in conference.

- **Liability protections:** As noted in this legal sidebar, recent cybersecurity information sharing legislation is not just about clarifying the legal framework respecting the *sharing* of information; bills like CISA, PCNA, and NCPAA are also concerned with encouraging the *collection* of cyber-threat indicators (CTIs) and the *use* of so-called defensive measures (DMs) to help combat known cyber-threats. To help clarify the laws governing the collection, sharing, and use of cybersecurity information, all three bills provide *some* civil and criminal *immunity* for entities complying with the new laws respecting the collection or sharing of cybersecurity information. The bills differ, however, with respect to the nature and scope of liability protections provided, including:
  - **Good faith provisions:** The two House bills contain a "good faith" provision that immunizes "good faith failure[s] to act" based on the sharing or receipt of CTIs or DMs in accordance with the Act. CISA does not contain a similar provision and merely immunizes causes of action based on the sharing or receipt of CTIs or DMs.
  - **Exceptions to liability protections:** While all three bills would exempt from immunity protections "willful misconduct" related to monitoring or information sharing, CISA also does not extend liability protections to "grossly negligent" acts.
  - **Evidentiary burdens:** The two bills that passed the House place a burden on a plaintiff to prove by "clear and convincing evidence" that a private entity engaged in willful misconduct. CISA does not contain a similar provision.
- **Privacy and civil liberty concerns:** One of the central issues in the debate over cybersecurity information legislation is the extent to which private entities in collecting and sharing cyber-intelligence are risking the unnecessary dissemination of personal identifying information (PII) with other private entities or the government. While all three bills have several provisions aimed at alleviating privacy concerns (including authorizing the creation of privacy "guidelines" with which the federal government must comply) , the bills vary in several respects, including:
  - **Removal of PII:** Both of the House bills require private entities to take "reasonable efforts" to remove or

exclude information that can be used to identify specific persons and is "reasonably believed" at the time of sharing to be unrelated to a cybersecurity risk or incident. In contrast, CISA does not contain the "reasonable efforts" or "reasonably believed" language. Instead, the Senate bill requires private entities to "remove" personal information of or identifying a specific person not directly related to a cybersecurity threat prior to the sharing of any information. Some privacy advocates have argued that the "reasonable efforts" language creates a needed benchmark for companies to adhere to before disseminating cyber-information. Others, however, have contended that the "reasonable efforts" language is meaningless and may be even more protective of PII, as CISA's requirement extends to even those entities that have made reasonable efforts, but nonetheless have failed to excise the necessary information.

- **Government use restrictions:** With respect to privacy and civil liberties, perhaps the biggest difference between all three bills is with regard to the "use" restrictions imposed on the federal government – that is, the ways the bills would restrict how the federal government can use cyber-intelligence shared by the private sector. The NCPAA, unlike the PCNA and CISA, has arguably the most stringent use restriction of the three bills, solely limiting the federal government's use of CTIs and DMs to "cybersecurity purposes." The PCNA and CISA, in contrast, allow the federal government to use shared cyber-intelligence not only for cybersecurity purposes, but also to respond to, investigate, prosecute, prevent, and mitigate several crimes unrelated to a cyberattack, such as a crime related to a serious threat to a minor. While somewhat scaled back by the recent manager's amendment, CISA, perhaps, has the broadest use restrictions, allowing the federal government to use shared cyber-intelligence with respect to acts that imminently threaten "serious economic harm."

- **Enforcement:** Another notable difference between the bills respects how violations of privacy and civil liberties norms can be enforced. Both of the House bills create a private cause of action, whereby a private entity harmed by the federal government's misuse of shared cyber-intelligence can sue the government for damages. When compared to the other two bills, the NCPAA's new cause of action is perhaps broadest in scope, creating a cause of action based upon intentional or willful violations of (1) the Act's provisions on information sharing; (2) the Act's privacy and civil liberties policies and procedures; or (3) the Act's "disclosure, retention, and use" restrictions for federal agents. In contrast, the federal government would risk liability under the PCNA only as a result of violating the privacy and civil liberties guidelines created by the Attorney General under that bill. CISA does not create a private right of action to enforce that bill's privacy and civil liberties provisions, relying instead on several mandated reports and studies to promote compliance with the bill's privacy standards.
- **Agency Roles:** Each bill takes a slightly different approach to what agency assumes the lead role as the interface between the private sector and the government on cyber-information sharing. The NCPAA amends the Homeland Security Act of 2002 and places the National Cybersecurity and Communications Integration Center (NCCIC) as the "lead Federal civilian interface" on information sharing, requiring participating private entities to enter formal agreements with the NCCIC on information sharing. The PCNA does not specify a particular agency to receive CTIs and DMs and instead merely excludes the Department of Defense (including the National Security Agency (NSA)) from being an agency that receives CTIs and DMs from the private sector. In contrast, CISA more generally contemplates the Department of Homeland Security developing and implementing the capability within DHS to accept CTIs/DMs in real time from any entity and share that information in an automated manner with other federal agencies.
- **Sunsets:** Finally, the bills differ with respect to their expiration dates. The two House bills contain an explicit sunset date of seven years. While a proposed amendment would have limited CISA's effective period to six years, the version of CISA that passed the Senate contains an expiration date of ten years.

Reports indicate that the reconciliation process should begin in the upcoming months, with a final vote on cybersecurity legislation in each chamber by early next year. For background on these and other issues, please see R43941, *Cybersecurity and Information Sharing: Legal Challenges and Solutions*.

Posted at 10/28/2015 03:25 PM