CARLTON FIELDS

Collaboration Key to Combating Cyber Threats: Federal Government Issues Final Guidance Clarifying Liability Protection for Private Entities that Share Cybersecurity Information

July 18, 2016

On June 15, the Department of Homeland Security (DHS) and the Department of Justice (DOJ) jointly issued final guidance on how the private sector and government will communicate cyber threat data and defensive measures under the Cybersecurity Information Sharing Act (CISA). Enacted at the end of 2015, CISA aims to identify and mitigate potential cyber incursions by encouraging, through liability protections and other incentives, the private sector to share cyber threat data and defensive measures. The Act provides liability protections to private entities that monitor information systems and employ defensive measures to address cyber threats to those systems. CISA also encourages the private sector to share with the federal government and among itself cyber threat indicators and defensive measures deployed in response to those threats. Specifically, CISA provides that no cause of action can be brought against private entities that conduct activities authorized by and in accordance with the Act. CISA's other incentives include the retention of legal privileges and protections for information shared with the federal government, including trade secret protections and exemptions from disclosure and antitrust laws. CISA directed the Executive Branch to develop guidelines and other procedures to implement the Act. On February 16, the DHS and DOJ issued preliminary instructions for sharing cyber threat indicators and defensive measures with DHS's National Cybersecurity and Communications Integration Center (NCCIC). The preliminary guidance

explained how NCCIC will share and use that information, and provided examples of what may and may not be shared. The guidance also outlined the four mechanisms available to private entities wishing to take advantage of CISA's liability protections: (1) DHS's Automated Indicator Sharing (AIS) system; (2) a fillable web form; (3) email to NCCIC; or (4) through Information Sharing and Analysis Centers or Information Sharing and Analysis Organizations. The guidance further explained how to identify certain types of personally identifiable information that must be scrubbed from any data prior to sharing with the government. The final guidance issued in June provides additional information to further assist private entities that elect to share cyber threat indicators and defensive measures. Specifically, the final guidance states that private entities also receive liability protection under the Act for sharing threat indicators and defensive measures with other private entities, not just the federal government, so long as it is shared in accordance with the Act. To meet those requirements, the only information that can be shared under CISA is information directly related to and necessary to identify or describe a cybersecurity threat, and all known personally identifiable information must be removed prior to sharing. Certain protections under the Act, such as federal and state disclosure law exemptions, would not apply to information shared among private entities. The final guidelines also identify other DHS programs, beyond the four mechanisms outlined above, through which cyber threat indicators and defensive measures may be shared with the government and receive liability protection. For example, DHS provides access to communities of interest, such as the industrial control systems owners and operators community, through a web-based portal that already allows indicator sharing within the portal. Stakeholders participating in DHS's Cyber Information Sharing and Collaboration Program may share cyber threat indicators or defensive measures within that program as well. Both of these existing programs now fall within CISA per the final guidelines. Even with these clarifications, however, it remains to be seen whether the protections afforded by CISA will encourage the private sector to share cyber threat information. As recently as June, industry experts testifying before the House Homeland Security Committee's Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee indicated that many companies remain hesitant to participate in cyber threat sharing due to concerns over potential backlash from regulators and the public. With the final guidance now available, companies can review the benefits available under CISA and determine their comfort level in participating in this information-sharing program.

Authored By

Erin J. Hoyle

Related Practices

Cybersecurity and Privacy