

# Cyber Intelligence Sharing and Protection Act Set for Markup Session

April 09, 2013

The U.S. House of Representatives Intelligence panel will mark up the Cyber Intelligence Sharing and Protection Act (CISPA) this week. Last year, CISPA met strong opposition from privacy advocates and the public due to privacy concerns. The bill is intended to give companies the ability to receive and share threat intelligence from the government to defend against cyber attacks in real time. Leaders are expected to propose changes aimed at addressing privacy concerns to avoid repeating last year's veto threat from the White House, which came one day before the bill was to go to the House floor for a vote. The White House said its rapid response to the bill was due to the fact that it lacked sufficient privacy measures to prevent companies from sharing private customer information with the government and law enforcement. CISPA is one of many bills expected to emerge in the House in the next 60 days or so as part of a package of cyber security-related measures currently making their way through both houses of Congress. Privacy groups are already mobilizing to oppose the bill in whatever form it takes. They have been raising public awareness of the consequences of allowing private companies to share users' electronic communications with the federal government. In response to these concerns, Rep. Adam Schiff (D-Calif.) plans to introduce an amendment that would remove any personally identifiable information prior to any information sharing with the government or other companies. CISPA has been highly controversial and demonstrates how difficult it will be to pass comprehensive national cyber security laws. However, the imperative and well-documented need for a centrally organized cyber security defense strategy will likely result in the passage of some form of legislation very soon. Carlton Fields is closely monitoring CISPA and all cyber security-related federal legislative initiatives making their way through congress. We are prepared to help clients plan ahead and respond to the new rules as they arrive.

## Authored By



Dennis J. Olle

## Related Practices

[Business Transactions](#)

[Cybersecurity and Privacy](#)

[Health Care](#)

[Life, Annuity, and Retirement Litigation](#)

[Government Law & Consulting](#)

## Related Industries

[Health Care](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.