

Congress Moves Critical Infrastructure Cybersecurity Bill

Article By:

Privacy & Security Practice Group at Mintz Levin

On Wednesday, the **House Homeland Security Committee** passed a substitute bill for H.R. 3696, the **National Cybersecurity and Critical Infrastructure Protection Act of 2013**. The committee [substitute bill](#) was broadly supported by both parties. As it presently stands, H.R. 3696 delegates to the Department of Homeland Security the responsibility for civilian cybersecurity research and development, incident detection and response, and facilitating the exchange of cyberthreat information between government and the private sector. It calls for the establishment of industry sector coordinating councils under a so-called public-private partnership model. In response to requests from industry, it expands the tort liability immunity provisions of the SAFETY Act by adding cybersecurity technologies to the anti-terrorism technologies covered by that statute.

Of concern to privacy advocates is the inclusion of a provision that appears to immunize private electronic communications services from liability for selling information about their customers' communications to the government. Under the bill, DHS is authorized to enter into contracts or other agreements to obtain "the assistance of private entities that provide electronic communication services, remote computing services, or cybersecurity services to acquire, intercept, retain, use, and disclose communications and other system traffic No cause of action shall exist against private entities for assistance provided to the Secretary in accordance with this subsection."

©1994-2025 Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. All Rights Reserved.

National Law Review, Volume IV, Number 44

Source URL: <https://natlawreview.com/article/congress-moves-critical-infrastructure-cybersecurity-bill>