Shumaker

OCTOBER 10, 2025 | PUBLICATION

Client Alert: Government Shutdown Creates a "Perfect Storm" for U.S. Cybersecurity

As Washington barrels through another government funding crisis, the most significant impact on the technology and security landscape isn't happening in a committee room—it's the effective shuttering of our nation's frontline cyber defense agency.

INDUSTRY SECTOR

Public Sector
Technology

SERVICE LINE

Public Policy & Government Affairs
Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Chris Salemme

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

The first blow is to the Cybersecurity and Infrastructure Security Agency (CISA), the lead federal body responsible for protecting critical infrastructure like our electric grid, water systems, and financial networks. CISA has been forced to furlough the vast majority of its staff and is now operating with a skeleton crew of just 889 employees—a mere 35 percent of its workforce. This dramatically reduces the government's ability to detect, analyze, and respond to sophisticated cyber threats.

Compounding this problem, the shutdown coincided with the expiration of a critical legal framework on September 30th. Key privacy and liability protections under the Cybersecurity Information Sharing Act of 2015 have now lapsed. These protections were pivotal, creating a legal safe harbor that encouraged private companies to share cyber threat data with each other and with government agencies like CISA. The simultaneous loss of CISA's operational capacity and this legal framework leaves the private sector isolated as it faces a surge in sophisticated hacks from China and persistent ransomware attacks.

https://thehill.com/homenews/5529647-cyberthreat-sharing-law-expires-as-government-shuts-down/

Shumaker