EINPRESSWIRE

As Congress Meets Cyber Experts in Silicon Valley, Centraleyes Delivers a Platform for Efficiency and Collaboration

At Stanford, lawmakers and tech leaders weigh upstream accountability, smarter compliance, and the future of cyber threat sharing.

NEW YORK, NY, UNITED STATES, May 28, 2025 /EINPresswire.com/ -- On May 28, the House Homeland Security Committee will hold a field hearing at Stanford University's Hoover Institution, bringing together lawmakers and leading voices from companies like Google Cloud and Palo Alto Networks to examine the future of U.S. cybersecurity. One key question on the table: how can we "flip the economic model" of cybersecurity?

That phrase, now circulating in D.C. and industry circles, reflects a growing call to rethink how responsibility is shared. The idea is to shift more responsibility upstream to those who build and deploy digital infrastructure. In legacy models, end users absorb the bulk of the operational and financial risk. But that imbalance is drawing fresh scrutiny. And it's not just about who pays for security. It's about how information flows and how responsibility is distributed across the cybersecurity lifecycle.

> While policy shifts are debated in Washington and beyond, we see organizations already moving toward smarter and more connected risk management."
>
> *Yair Solow*

Which is why this hearing couldn't come at a more pivotal moment. Congress is also considering whether to renew the Cybersecurity Information Sharing Act (CISA), a 2015 law that allows private companies and government agencies to share cyber threat intelligence without legal risk. Without it, that flow of information could dry up right when we need it most.

The hearing's bipartisan panel includes Chair Mark Green (R-TN) and Rep. Bennie Thompson (D-MS). Experts from Google Cloud, Palo Alto Networks, and Stanford will be in the conversation as well. Expected themes include stronger alignment between regulators and innovators, regulatory streamlining, and secure modernization of public systems.

The Centraleyes AI-powered GRC platform reflects this market evolution. It enables public and private organizations to:

- Map and track regulatory frameworks in real-time.
- Identify and quantify risks using autonomous AI-driven registers.
- Automate remediation workflows across internal teams and external vendors
- Share risk insights and evidence across frameworks, regions, and reporting bodies

A shift is underway in how cybersecurity is being governed, implemented, and understood. No longer confined to IT departments or regulatory checklists, cybersecurity is becoming a matter of national resilience. As regulatory expectations evolve and cyber threats grow more complex, both government and industry are being challenged to rethink the foundations of collaboration.

About Centraleyes

Centraleyes provides the underlying infrastructure organizations need to manage cybersecurity risk and compliance in a more connected, accountable ecosystem. As the focus shifts toward upstream responsibility and smarter regulation, the platform supports this transition with tools for real-time risk visibility, regulatory tracking, and cross-team coordination. It's used by public and private sector teams to keep pace with evolving standards and to build security programs that are both agile and auditable.

The company's approach reflects a broader industry trend: less complexity, more automation, and better collaboration between the systems and people responsible for security.

Jacob Zakay
Centraleyes
email us here