

Homeland Security

The recent conflict in Iran has intensified concerns about cyberattacks on critical infrastructure, violent extremist radicalization, and attacks on religious or government targets by Iran-linked actors, alongside pre-existing risks from other nation-state and non-state threats. To support the protection of our nation's infrastructure, RER has focused on strengthening public-private information sharing and helping members prepare for a more complex threat environment.

RE-ISAC and Homeland Security Task Force Activities

As cyber and physical threats evolve, timely information sharing between the public and private sectors remains essential for safeguarding commercial properties and the businesses and people they serve. Direct coordination with government partners helps the industry improve preparedness, respond more quickly to incidents, and better protect assets that are part of the nation's critical infrastructure.



RER's Actions:

Continued to operate the RER Homeland Security Task Force and the Real Estate Information Sharing and Analysis Center (RE-ISAC), the industry's core platforms for sharing cyber and physical threat information with key law enforcement and intelligence agencies.

Supported RE-ISAC's ongoing operational coordination with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), helping strengthen the detection, prevention, and mitigation of cyber and related data threats.

At the January 2026 State of the Industry meeting, connected members with federal law enforcement leaders to discuss emerging risks and elevated data center security as a policy priority.



RER's Impact:

Helped ensure that members have a consistent channel for information sharing as the security environment becomes more volatile.

Strengthened public-private coordination between the commercial real estate industry and federal homeland security partners.

Elevated AI risks and data center security as an emerging priority within RER's broader homeland security agenda.

Sen. Bill Hagerty (R-TN) (Committees: Appropriations; Banking, Housing and Urban Affairs; and Foreign Relations) discussed national security.



CISA 2015 Reauthorization and Updates

The Cybersecurity Information Sharing Act of 2015 provides legal protections that encourage private companies to share cyber threat information with the government. Congress temporarily extended the law through Sept. 30, 2026, and lawmakers are considering legislation to reauthorize and modernize it for AI and supply-chain risks.



RER's Actions:

Supported the *Widespread Information Management for the Welfare of Infrastructure and Government (WIMWIG) Act*, led by House Homeland Security Committee Chairman Andrew Garbarino (R-NY), to reauthorize CISA 2015 for 10 years and update it to address AI and supply-chain threats.

Continued to emphasize the importance of preserving the liability and privacy protections that support voluntary cyber threat information sharing between the private sector and government.

Encouraged policymakers to advance cybersecurity measures that strengthen resilience without creating duplicative or inconsistent requirements for critical infrastructure owners and operators.



What's Next:

RER continues engaging lawmakers to advance the *WIMWIG Act* ahead of CISA 2015's expiration.



Rep. Andrew Garbarino (R-NY) (Chairman, House Homeland Security Committee; Vice Chairman, House Financial Services Subcommittee on Capital Markets) briefed members on terrorism risk insurance (TRIA) reauthorization, ahead of its 2027 expiration.

Looking Ahead

In addition to supporting existing information sharing platforms and the *WIMWIG Act*, RER promotes practical measures businesses can take to better prepare for evolving threats, including stronger cyber defenses and resilient infrastructure that withstands physical damage and cyber breaches. As the threat environment shifts, RER will continue to back policies and partnerships that improve preparedness and operational resilience across the industry.