9

# Homeland Security

**Remaining vigilant to threats against the commercial facilities sector is crucial for ensuring the safety and security of employees, customers, and assets. Potential perils from cyberattacks, terrorism, and transnational criminal activity continue to be a focus for RER's homeland security efforts. Intelligence gathering, law enforcement, community engagement, and information sharing partnerships are critical to preventing, disrupting, and prosecuting physical and cyber threats.**

**Additionally, there are growing concerns about AI having the potential to create new risks. Key concerns include the risk of cyberattacks that exploit AI vulnerabilities, leading to unauthorized access to facilities or sensitive data.**

## Cyber and Physical Threats to U.S. Real Estate

As the threat landscape facing the commercial facilities sector—including commercial real estate—grows increasingly complex, RER continues to lead efforts that enhance industry preparedness and promote stronger coordination with federal law enforcement and intelligence agencies.

According to the ODNI's 2025 Annual Threat Assessment, a diverse set of foreign actors are targeting U.S. health and safety, critical infrastructure, industries, wealth, and government. State adversaries and their proxies are also trying to weaken and displace U.S. economic and military power in their regions and across the globe. Russia, China, Iran, and North Korea—individually and collectively—are challenging U.S. interests in the world by attacking or threatening others in their regions, with both asymmetric and conventional hard power tactics, and promoting alternative systems to compete with the U.S., primarily in trade, finance, and security. A range of cyber and intelligence actors are targeting our wealth, critical infrastructure, telecom, and media.

In this environment, protecting critical infrastructure—both physical and digital—is paramount. Through our Homeland Security Task Force and the Real Estate Information Sharing and Analysis Center (RE-ISAC), RER remains a trusted partner to law enforcement and intelligence agencies in preparing for and responding to security threats. These efforts ensure that owners and operators of real estate assets are informed, coordinated, and engaged in safeguarding against key threats.

The RE-ISAC plays a central role in sharing real-time threat intelligence between real estate owners and federal partners. Through a Cybersecurity Information Sharing and Collaboration Agreement with DHS's Cybersecurity and Infrastructure Security Agency (CISA), the RE-ISAC engages in operational efforts to better coordinate activities supporting the detection, prevention, and mitigation of cybersecurity, communications reliability, and related data threats to critical infrastructure.

In 2024, the White House advanced key objectives in its National Cybersecurity Strategy, including the development of scenario-based cyberattack exercises to help critical infrastructure owners prepare for potential threats.

Even as the nation makes progress on putting the right protections in place, RER has emphasized that it is vital to advance security measures without imposing overly burdensome regulations on real estate. In July 2024, RER was part of a coalition of national real estate organizations that wrote to CISA to express concerns about a proposed reporting rule that carried an estimated compliance cost of over $1.4 billion—seen as disproportionate to the rule's benefits.

Alongside our work with our Homeland Security Task Force and RE-ISAC, RER will continue to promote measures that businesses can take—such as creating resilient infrastructure that is resistant to physical damage and cyber breaches—to better prepare for possible threats.