June 3, 2026

Chairman Andy Ogles
Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, DC 20515

Ranking Member Delia Ramirez
House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection
H2-117 Ford House Office Building
Washington, DC 20515

Dear Chairman Ogles and Ranking Member Ramirez:

On behalf of the members of the National Multifamily Housing Council (NMHC), the National Apartment Association (NAA), and the Real Estate Technology and Transformation Center (RETTC), we write ahead of your hearing entitled "The AI Security Landscape: How Frontier Models, Agentic AI, and AI Coding Tools Are Reshaping Cybersecurity and Critical Infrastructure Resilience." Thank you for the opportunity to share the views of rental housing providers and their technology partners as the Subcommittee examines the risks and opportunities of rapidly evolving AI technology.

As the Subcommittee considers AI policy, we urge you to support a balanced framework that safeguards innovation. Existing legal and regulatory frameworks provide an important foundation for cybersecurity and consumer protection, and any future policy efforts should build upon that foundation while preserving innovation.

Technological Transformation in Rental Housing

Rental housing increasingly relies on interconnected digital systems to operate rental housing communities, process payments, manage building access, communicate with residents, and maintain critical business functions. As AI capabilities advance, they are reshaping both the defensive and offensive sides of cybersecurity, making this discussion particularly important to the housing sector.

To improve housing affordability and better serve millions of residents, rental housing providers have increasingly adopted Artificial Intelligence (AI) and other emerging technologies. Today, AI-enabled tools support customer service interactions, maintenance workflows, fraud detection, cybersecurity monitoring, document processing, operational forecasting, software development, and administrative functions.

Along with its immense promise, AI also transforms the cyber risk landscape for rental housing and introduces new challenges. Cybercriminals are deploying this technology to execute more advanced attacks on businesses of all types. Rental housing is no exception. Disruptions to these systems can have real-world consequences for both residents and rental housing providers.

Importantly, as housing providers adopt more specialized technology solutions, cybersecurity resilience increasingly depends on the security practices of rental housing providers' third-party technology partners. Strengthening security across the broader technology ecosystem is therefore critical.

Core Commitment to Residents' Digital Security and Privacy

The core of rental housing is a focus on service to residents and a commitment to provide a safe and secure community for those who call rental housing home. That commitment extends to ensuring that information collected, used, or retained on residents is secure and privacy is safeguarded.

Residents increasingly interact with housing providers through digital platforms, mobile applications, smart building technologies, and AI-enabled services. Maintaining trust in these systems requires a strong commitment to cybersecurity resilience and responsible technology governance.

NMHC, NAA, and RETTC have undertaken efforts across the rental housing ecosystem to mitigate cybersecurity risks, promote good cyber hygiene, and encourage investments that strengthen cyber defenses. As part of our shared commitment to data protection and privacy, NMHC/RETTC is a member of the Real Estate Information Sharing and Analysis Center (RE-ISAC) and serves on the leadership committee. Timely information sharing between industry, government, and trusted cybersecurity partners remains an important component of identifying emerging threats and strengthening collective resilience.

Through RETTC and other industry-led collaborations, rental housing providers and technology partners are actively developing AI governance frameworks and cybersecurity educational resources to support responsible deployment of emerging technologies and strengthen cybersecurity resilience across the housing ecosystem.

AI is Changing the Cybersecurity Landscape

AI presents both significant opportunities and significant risks for rental housing providers and their technology partners. On the defensive side, AI-enabled cybersecurity tools can improve threat detection, identify anomalous activity, automate portions of incident response, and help organizations address vulnerabilities more efficiently.

At the same time, malicious actors are increasingly using AI to enhance phishing campaigns, automate reconnaissance activities, generate malicious code, exploit software vulnerabilities, and conduct social engineering attacks at unprecedented scale. These risks are particularly relevant in rental housing, where organizations often manage sensitive personal information, financial transactions, access-control systems, smart building technologies, and other operational technologies that support apartment communities. Importantly, smaller rental housing providers may face particular challenges in keeping pace with increasingly sophisticated cyber threats and rapidly evolving technologies.

Emerging frontier AI models, agentic AI systems, and AI coding tools may create new opportunities to improve productivity, software security, fraud detection, and cybersecurity outcomes. For rental housing providers and their technology partners, these tools may help identify vulnerabilities more quickly, improve operational resilience, and enhance defensive cybersecurity capabilities. However, these systems also introduce new governance, oversight, and risk-management considerations.

Housing Resilience Depends on Secure Technology Systems

The continued operation of rental housing communities depends on reliable and secure technology systems. Property management software, communications platforms, payment processing systems, access-control technologies, technology suppliers, and service providers all support daily housing operations. Apartment communities increasingly rely on these systems to support resident communications, building access, emergency notifications, maintenance coordination, and financial transactions. Maintaining the security and availability of these systems is essential to operational continuity and resident well-being.

Cyber incidents affecting these systems can disrupt essential functions relied upon by residents and housing providers alike. As AI-enabled threats continue to evolve, strengthening cybersecurity across the housing ecosystem should remain a priority.

This challenge is particularly important because many housing providers depend on a broad network of technology partners and service providers. Effective cybersecurity therefore requires collaboration across the entire housing technology ecosystem.

The Need for Clear and Consistent Data Governance Requirements

As the Subcommittee evaluates the current AI security landscape, we respectfully request that policymakers encourage risk-based, technology-neutral governance approaches that focus on outcomes rather than prescribing specific technologies. Such approaches can help organizations adapt to rapidly changing AI capabilities while maintaining appropriate security protections. The focus should be on strengthening resilience, encouraging adoption of effective security practices, and supporting innovation that improves defensive capabilities.

As organizations deploy increasingly sophisticated AI and cybersecurity tools, clear and consistent data governance requirements become even more important. Effective cybersecurity policy and data governance policy should work together. Organizations need clear, consistent rules governing the collection, protection, sharing, and notification requirements associated with sensitive information.

NMHC, NAA, and RETTC strongly believe that it is necessary to first establish a national data security, consumer privacy and breach notification standard that is reasonable, flexible and scalable. Importantly, a clear, federal preemption is essential to provide clarity for rental housing

firms that operate across state lines. The current patchwork of state laws creates a significant compliance burden for rental housing firms and leaves consumers vulnerable to compliance errors, inconsistencies, and unintended consequences. This is particularly true given the constantly evolving nature of state data privacy and security laws.

Conclusion

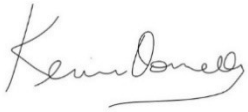
As AI capabilities continue to evolve, Congress has an opportunity to support policies that strengthen cybersecurity resilience without slowing innovation. A risk-based framework that promotes responsible AI adoption, supports cybersecurity investment, encourages information sharing, and establishes clear national standards for privacy and data security will help housing providers better serve residents, strengthen operational resilience, and protect critical systems and sensitive information.

We appreciate the Subcommittee's focus on fostering innovation while addressing emerging cybersecurity challenges. NMHC, NAA, and RETTC stand ready to work with the Subcommittee to support responsible AI adoption and technology innovation that strengthens security, improves operational efficiency, and expands housing opportunity and affordability.

Sincerely,

Sharon Wilson Géno
President
National Multifamily Housing Council

Bob Pinnegar
President and Chief Executive Officer
National Apartment Association



Kevin Donnelly
Executive Director and Chief Advocacy Officer
Real Estate Technology & Transformation Center