CONGRESSIONAL TESTIMONY

Salt Typhoon: Securing America's Telecommunications from State-Sponsored Cyber Attacks

Testimony before the
Committee on Oversight and Government Reform

Subcommittee on Cybersecurity, Information Technology, and Government Innovation

U.S. House of Representatives

April 2, 2025

Cory Simpson, J.D., L.L.M.
Chief Executive Officer
The Institute for Critical Infrastructure Technology (ICIT)

1701 Pennsylvania Ave Suite 200 | Washington, D.C. 20006

Subject: Standing with You to Secure America's Telecommunications from State-Sponsored Cyber Threats

Dear Chairwoman Mace, Ranking Member Brown, and Members of the Subcommittee,

Your April 2, 2025, hearing, *Salt Typhoon: Securing America's Telecommunications from State-Sponsored Cyber Attacks*, could not come at a more critical moment. On behalf of the Institute for Critical Infrastructure Technology (ICIT) and the broader community we serve, I would like to thank you for drawing national attention to a threat that is both urgent and strategically significant.

The Institute for Critical Infrastructure Technology (ICIT) is a nonprofit, nonpartisan, 501(c)3 think tank with the mission of modernizing, securing, and making resilient critical infrastructure that provides for people's foundational needs. ICIT does not take institutional positions on policy matters. Rather than advocate, ICIT is dedicated to being a resource for the organizations and communities that share our mission.

Telecommunications is one of ICIT's core focus areas, alongside energy, water, wastewater, and transportation. The threat posed by foreign adversaries to U.S. telecom networks goes to the heart of our mission—and the heart of national security.

Salt Typhoon, attributed to the People's Republic of China (PRC) and believed to operate on behalf of the Chinese Ministry of State Security, represents a calculated evolution in cyber operations targeting the homeland. According to the Congressional Research Service, Salt Typhoon has conducted long-term cyber intrusions into U.S. telecommunications and internet service providers to surveil, exfiltrate sensitive information, and pre-position for future disruption. The group's use of legitimate credentials and native tools enables it to operate undetected for extended periods.

As recently reported by CyberScoop, Salt Typhoon's latest campaign stood out for its "indiscriminate targeting" of U.S. telecom providers, indicating not just reconnaissance but also systemic infiltration.

The PRC has been stealing Americans' data for years. But this is different. Today, they are gaining direct access to U.S. critical infrastructure with the intention of disrupting it. The **2025 Annual Threat Assessment** underscores this concern, stating that "China is using complex, whole-of-government campaigns featuring coercive military, economic, and influence operations short of war to assert its positions and strength against others." They appear to be preparing to deliver effects at a time and in a manner of their choosing. This is not a distant or abstract risk. It is deliberate, ongoing, and increasingly sophisticated. We should be alarmed—and we must be prepared for what's next.

This hearing represents a vital step in acknowledging the scope and intent of these state-sponsored cyber operations. But recognition must lead to action. Congress has the authority—and the responsibility—to ensure our telecommunications infrastructure is not only defended but resilient under real-world stress. That begins with setting clear national priorities, aligning

resources accordingly, and driving persistent coordination across federal departments, state and local governments, and the private sector. Success will depend on sustained engagement and shared situational awareness—not only in Washington, but across the entire American infrastructure ecosystem. Strategic, focused, and collective action is what will position us to meet this moment.

ICIT stands ready to support your work in this endeavor. We are a nonpartisan resource to help translate emerging threats into meaningful insight and convene communities across the public and private sectors in service of national cybersecurity.

Thank you again for your leadership and for your commitment to safeguarding American telecommunications from state-sponsored cyber aggression.

Yours in service,

Cory Simpson

Cory Simpson, J.D., LL.M.
Chief Executive Officer
Institute for Critical Infrastructure Technology (ICIT)
Website: https://www.icitech.org/