

FACT SHEET: IMPLICATIONS OF SALT TYPHOON ATTACK AND FCC RESPONSE

Empowering Resilience Through Proactive Cybersecurity Measures

Overview

The Federal Communications Commission (FCC) is taking decisive steps to address vulnerabilities in U.S. telecommunications networks following the **Salt Typhoon cyberattack**, a sophisticated intrusion linked to foreign state-sponsored actors. These measures aim to safeguard critical communications infrastructure and ensure national security, public safety, and economic resilience in the future.

What Happened?

- **Salt Typhoon Attack:**
On December 4, 2024, a top U.S. security agency confirmed reports that foreign actors, state-sponsored by the People's Republic of China, infiltrated at least eight U.S. communications companies, compromising sensitive systems and exposing vulnerabilities in critical telecommunications infrastructure. This was part of a massive espionage campaign that has affected dozens of countries.
 - **Impact:**
The attack underscores the urgent need for robust cybersecurity frameworks to protect against escalating threats targeting the telecommunications sector.
-

How Is the FCC Responding?

- **Affirming Cybersecurity Obligations and Increasing Accountability:**
FCC Chairwoman Jessica Rosenworcel has proposed a Declaratory Ruling that would clarify that **Section 105 of the Communications Assistance for Law Enforcement Act (CALEA)** creates a legal obligation for telecommunications carriers to secure their networks against unlawful access and interception. The proposal clarifies that telecommunications carriers' duties extend not just to the equipment they use but how they manage their networks.
- **New Compliance Framework:**
Under a Notice of Proposed Rulemaking circulated today, the FCC proposed an **annual certification requirement** for communications service providers to:
 - Create, update, and implement **cybersecurity risk management plans**.
 - Certify compliance with these plans to the FCC to ensure accountability.
- **Seeking Broader Action:**
The proposed Notice of Rulemaking invites public comment on:
 - Expanding cybersecurity requirements across a range of communications providers.
 - Identifying additional ways to enhance cybersecurity defenses for communications systems.

Why Does This Matter?

- **National Security:**
Telecommunications networks are critical to the nation's defense, public safety, and economic systems. While the Commission's counterparts in the intelligence community are determining the scope and impact of the Salt Typhoon attack, the FCC can act now to strengthen cybersecurity safeguards and ensure resilience against future cyberattacks by adversaries.
 - **Adaptation to Evolving Threats:**
As technology evolves, so do the tactics of cyber adversaries. The Salt Typhoon attack highlights the need for proactive measures to stay ahead of emerging threats.
 - **Public Trust:**
A cyberattack in the communications sector can affect other sectors, including healthcare, manufacturing, energy, and transportation. Ensuring secure and reliable communications infrastructure builds confidence in the nation's ability to protect critical systems and also helps protect everyday Americans from cyberattacks.
-

Next Steps

These proposed measures have been made available to the five members of the Commission. They may choose to vote on them at any moment. If adopted, the Declaratory Ruling would take effect immediately. The Notice of Proposed Rulemaking, if adopted, would open for public comment the cybersecurity compliance framework, which is part of a broader effort to secure the nation's communications infrastructure.

###

Released: December 5, 2024

Media Contact: MediaRelations@fcc.gov

*This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action.
See MCI v. FCC, 515 F.2d 385 (D.C. Cir. 1974).*