Secure American Communications Act

Chinese hackers have breached American telecom infrastructure, reportedly targeting President-elect Trump, Vice President-elect Vance, people affiliated with Vice President Harris's presidential campaign and other political figures, national-security officials and staffers. These spies have successfully stolen customer call records data, intercepted private communications, gathered information about the targets of U.S. surveillance and, reportedly, have been able to listen in on audio calls in real time.

These attacks are a direct result of the U.S. government's failure to fully implement telecom security requirements already required by federal law. In 1994, Congress required telecom providers to design their systems to permit the government to obtain communications and call-identifying information with a court order or other lawful authorization. Congress otherwise required providers to secure their systems from unauthorized interceptions, and gave the FCC the authority to issue regulations to implement this requirement. However, in the years since, the FCC has not fully implemented this provision.

The Secure American Communications Act would require the FCC to finally prescribe appropriate rules to fully implement the law requiring telecom systems security, including requiring telecom carriers to:

- Implement specific cybersecurity requirements as designed by the FCC, in consultation with the Director of CISA and the Director of National Intelligence, to prevent unauthorized interceptions by any person or entity, including by an advanced persistent threat (APT)
- Conduct annual testing to evaluate whether their systems are susceptible to unauthorized interceptions by any person or entity, including by an advanced persistent threat; take such corrective measures as indicated by the test; and document the findings and all corrective measures taken in response
- Contract with an independent auditor to conduct an annual assessment of compliance with FCC cybersecurity rules; and document the audit findings, including areas of noncompliance
- Submit annually to the FCC:
    - the documentation from annual tests and audits
    - a written statement signed by the CEO and CISO (or equivalent) stating that the telecom carrier is in compliance with FCC cybersecurity rules