Updates
June 24, 2024
FCC Proposes New Internet Routing Security Rules for Telecoms

Building on its renewed jurisdictional authority over broadband internet access service (BIAS) providers following the reinstatement of net neutrality, the Federal Communications Commission (FCC) has adopted proposed internet routing security rules in a notice of proposed rulemaking (NPRM) designed to prevent foreign manipulation of internet traffic.

If the proposed rules are adopted, FCC believes they will help secure internet traffic routing by addressing well-documented vulnerabilities in Border Gateway Protocol (the Protocol)—the global routing protocol on which connected critical infrastructure services depend. The Protocol was designed more than 30 years ago with a focus on efficiency—not security. As a result, bad actors can exploit vulnerabilities in the Protocol to redirect internet traffic, which may compromise personal information, enable extortion and theft, and threaten national security through state-level espionage and sabotage of critical infrastructure and communications.

The FCC's Intent To Strengthen Internet Security

The NPRM's proposals aim to mitigate internet routing vulnerabilities by requiring BIAS providers and nine of the largest U.S. telecommunications service providers, including Verizon and AT&T, to (1) develop and implement Protocol Routing Security Risk Management Plans (Plans); and (2) comply with reporting requirements based on the BIAS provider's corresponding telecom "tier." Plans would have to describe detailed provider efforts to secure their internet routing architecture using Resource Public Key Infrastructure-based security measures (Security Measures), which increase routing security by using digital certificates to verify the identity of each network to detect and prevent Protocol hijacks by rejecting false information from bad actors. Plans would also have to include (1) specific goals and timetables to implement Plans; and (2) any factors affecting a service provider's implementation or maintenance of Plans. These requirements are in line with the efforts of the U.S. Department of Commerce and other federal agencies in addressing Protocol routing security concerns as part of the National Cybersecurity Strategy. Additionally, the FCC seeks comments on alternative

methods to strengthen Protocol routing, including mandatory contractual security requirements and downstream security requirements for clients.

Data Collection and Reporting

The proposed Security Measures include monitoring and information collection about internet routing and adoption of security best practices and industry standards through Protocol reporting requirements. The requirements would be based on which telecom provider "tier" a BIAS provider falls into:

- Tier 1 BIAS providers are the largest providers that operate extensive global networks and can exchange data with other networks without payment.
- Tier 2 BIAS providers are regional providers with less extensive networks that rely on agreements with Tier 1 BIAS providers for global coverage.
- Tier 3 BIAS providers are local providers with small networks that rely on agreements with Tier 1 and Tier 2 BIAS providers to provide connectivity.

Tier 1 BIAS providers will be required to (1) confidentially file their Plans with the FCC; and (2) file publicly available quarterly data reports on Security Measure implementation progress with the FCC. Plans would have to be resubmitted annually, with a possible sunset of five years on annual reporting. However, BIAS providers that attest to maintaining Security Measures for 90% of the networks under their control would not have to file subsequent Plans annually, and the FCC is open to moving from quarterly reports to semiannually or annually to potentially no data reporting requirement instead for these BIAS providers. Tier 2 and Tier 3 BIAS providers would also have to develop Plans and provide them to the FCC upon request but would not have to file Plans or quarterly reports.

Takeaways and Next Steps

The NPRM reflects a step by the FCC towards increasing communication security over the internet as part of ongoing multistakeholder efforts to address and secure internet routing issues. However, some industry stakeholders contend that Protocol regulations would stunt progress on routing security development and impose barriers for small BIAS providers, in addition to concerns over the challenges of implementing the Security Measures. Yet the FCC may adopt stringent security requirements if it determines that the Plans filed by providers suggest a need for more comprehensive regulation.

The FCC's jurisdictional authority for the NPRM rests, at least in part, precariously on the recent reinstatement of net neutrality, which is currently under appeal. The FCC contends that the Communications for Law Enforcement Act (CALEA) provides an alternative legal basis for its authority to prescribe rules and requirements related to internet routing security, as CALEA requires telecom providers to secure their networks against unauthorized interception. Nevertheless, a cloud of uncertainty will likely shroud the potential reach of this rulemaking until the appeal of the net neutrality rules is fully resolved.

Authors

Explore more in

Technology Transactions & Privacy Law Privacy & Security Communications

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law