OFFICE OF THE CHAIRWOMAN

Media Contact:
MediaRelations@fcc.gov

For Immediate Release

FCC CHAIRWOMAN PROPOSES INTERNET ROUTING SECURITY REPORTING REQUIREMENTS

Broadband Providers Would Need BGP Security Plans and Largest Providers Would File Quarterly Reports

WASHINGTON, May 15, 2024—FCC Chairwoman Jessica Rosenworcel today proposed requiring the largest broadband providers to file confidential reports on Border Gateway Protocol (BGP) security so the FCC and its national security partners can for the first time collect more up-to-date information about this critical internet routing intersection. BGP is the technology used for routing information through the physical and digital infrastructure of the internet.

National security experts have raised concerns that, by accessing vulnerabilities in BGP, bad actors can disrupt critical services that rely on the internet and result in misdirection, interception, inspection, or manipulation of data. A bad network actor may deliberately falsify BGP reachability information to redirect traffic. Russian network operators have been suspected of exploiting BGP's vulnerability for hijacking in the past. "BGP hijacks" can expose Americans' personal information, enable theft, extortion, state-level espionage, and disrupt otherwise-secure transactions.

"It is vital that communication over the internet remains secure," **said Chairwoman Rosenworcel**. "Although there have been efforts to help mitigate BGP's security risks since its original design, more work needs to be done. With this proposal, we would require broadband providers to report to the FCC on their efforts to implement industry standards and best practices that address BGP security."

The proposal aims to increase the security of the information routed across the internet by proposing certain reporting obligations on broadband internet access service (BIAS) providers on their progress towards secure internet routing. The proposal looks to utilize the Resource Public Key Infrastructure (RPKI) as a critical component of BGP security. It proposes to require that all broadband providers develop plans for implementing BGP security measures, and that a select number of the largest broadband providers would file those plans with the Commission as well as file quarterly data reports.

The Notice of Proposed Rulemaking would, if adopted by a vote of the full Commission at its June Open Meeting, formally propose:

- BIAS providers develop BGP Routing Security Risk Management Plans (BGP Plans) that describe in detail their specific progress, and plans for, implementing BGP security measures that utilize the Resource Public Key Infrastructure.
- The nine largest service providers file their BGP Plans confidentially with the Commission as well as file publicly available quarterly data that would allow the Commission to measure progress in the implementation of RPKI-based security measures and assess the reasonableness of their BGP Plans.

- Seek comment on other measures related to implementing RPKI-based security.

Border Gateway Protocol is the global inter-domain routing protocol that is used to exchange reachability information amongst the various networks that comprise the internet. This technology is essential to the internet and has been referred to as the "glue" that enables modern connectivity. This essential technology, however, was designed decades ago and provides no intrinsic means by which to verify a "route origination" – that the internet address that you are requesting to access is in fact a valid address.

Today's proposal looks to use origin validation and Resource Public Key Infrastructure to increase BGP security. Origin validation verifies that a network is authorized to originate a route advertisement to a specific IP address. The RPKI allows validation of a route's origin by enabling cryptographically verifiable associations between specific IP address blocks, or autonomous system numbers (ASNs), and the "holders" of those internet number resources.

The FCC formally launched a proceeding on BGP with a Notice of Inquiry adopted in February 2022. Building on this record and the FCC Public Safety and Homeland Security Bureau's 2023 workshop featuring remarks from FCC Chairwoman Jessica Rosenworcel and CISA Director Jen Easterly, today's proposal seeks to further federal efforts to ensure BGP continues to efficiently serve our economic and communications needs while ensuring the security of U.S. networks.

###

Office of the Chairwoman: (202) 418-2400 / www.fcc.gov/jessica-rosenworcel