**STATEMENT OF**
**COMMISSIONER GEOFFREY STARKS**

Re: *Reporting on Border Gateway Protocol Risk Mitigation Progress*, Notice of Proposed Rulemaking, PS Docket No. 24-146; *Secure Internet Routing*, PS Docket No. 22-90.

Border Gateway Protocol is the mechanism that enables our Internet service providers (ISPs) to route traffic throughout the variety of networks that, when combined, make up the Internet. I've been focused on this since 2022, when I sat down with a group of the largest ISPs in America to discuss the challenges surrounding Internet routing. So, trust me when I tell you that it is vitally important that BGP is secure and we get it right.

As with most of the underlying protocols that make the Internet work, it was unfortunately not designed with security in mind. Accidental or malicious actions that send erroneous routing traffic information can make networks unavailable, or worse, can be used to redirect traffic to allow for cyberattacks, data theft, or espionage. For example, in 2008, YouTube was rendered inaccessible for much of the world after Pakistan attempted to block access to it within its borders by modifying YouTube's BGP routes. Russia took advantage of BGP vulnerabilities to limit access to Twitter as part of its invasion of Ukraine. And China Telecom misdirected 15% of the world's Internet traffic, and routed domestic United States Internet traffic through China, by hijacking BGP.

The good news is experts have developed tools and strategies to enhance BGP security. A group of ISPs working together at the Mutually Agreed Norms for Routing Security, or "MANRS," created one such tool, Routing Public Key Infrastructure (RPKI), which is a public database of authenticated BGP routes and the gold standard of protecting Internet routing.

That's where our *Notice* comes in. In proposing that ISPs providing broadband Internet access service create BGP security risk management plans, ISPs that otherwise have not yet begun the process to deploy BGP mitigations will do so. In proposing to measure RPKI deployment, we will help inform both the private and public sectors about what more needs to be done to secure our networks. Our actions are part of a multi-pronged approach throughout the government. It is also consistent with Initiative 4.1.5 of the National Cybersecurity Strategy Implementation Plan, which tasks the Office of the National Cyber Director, along with stakeholders and government agencies, to develop a roadmap to increase adoption of secure Internet routing techniques including BGP security.

I thank the Chairwoman for her ongoing leadership in securing Internet routing, and for accepting my edits to make sure we ask questions about how our efforts can promote accountability among stakeholders, support the development of open standards setting solutions, such as RPKI, understand how network architecture plays into BGP security and RPKI deployment, and ensure that our efforts promote risk-based routing security among ISPs.

I look forward to continuing to engage with stakeholders and following the record closely. Protecting routing security will require an all-hands-on-deck approach from all stakeholders. Thank you to the Commission staff working on this complicated proceeding. I approve.