STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Reporting on Border Gateway Protocol Risk Mitigation Progress*, PS Docket No. 24-146; *Secure Internet Routing*, PS Docket No. 22-90, Notice of Proposed Rulemaking (June 6, 2024).

A few months ago I hosted a conversation with Vint Cerf, one half of the team that developed the protocol that allows computers to talk to one another. For this he is often described as the "Father of the Internet." We had a joyous back-and-forth about the origins and open architecture of the internet. So I asked him to reflect for a moment. What was it that he wished he had known back then when it all started? He responded without skipping a beat. He told me he wished he had known that the internet would need more security.

Amen. We have come to rely on the internet for nearly everything in our lives. Ensuring that internet traffic is secure is essential.

That is where Border Gateway Protocol comes in. BGP manages how packets of data get transmitted between networks. It is central to the global routing system of the internet because it is the protocol that allows independently managed networks to send traffic to one another.

That means we all rely on BGP. Every one of us, every day. That is true if you are running a small business and using connections to engage with customers and suppliers, banking online, having a telemedicine session with a healthcare provider, helping the kids with their digital age schoolwork, staying in touch with family, or keeping up to date on the news. BGP is in the background, helping connect our critical infrastructure, support emergency services, keep the financial sector running, shore up manufacturing, and more.

You might be surprised to learn that something so critical in the modern economy has pretty humble origins. This history is why BGP is sometimes called the "three napkin protocol." As the story goes, back in 1989, the internet, then a novelty for computer scientists like Vint Cerf, was expanding—fast. But the internet's basic protocols at the time could not handle this growth. So on their lunch break from an Internet Engineering Task Force meeting in Austin, Texas, a pair of engineers sketched out the ideas for BGP on three ketchup-stained paper napkins. What was meant to be a short-term solution developed on the sidelines of an internet engineering conference is still with us today.

While BGP has allowed network operators to grow and evolve the modern internet, it was not designed with explicit security features to ensure trust in exchanged information. That means bad actors can use this protocol to maliciously misdirect and exploit internet traffic. I want to thank the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security for working with my office and jointly holding a BGP public forum to discuss this problem. I also want to thank the Department of Defense and Department of Justice for publicly disclosing in our record that China Telecom used BGP vulnerabilities to misroute United States internet traffic on at least six occasions. These "BGP hijacks" can expose personal information, enable theft, extortion, and state-level espionage. They can also disrupt sensitive transactions that require security, like those in the financial sector.

For all of these reasons, today we begin a rulemaking to help make our internet routing more secure. We propose that all providers of broadband internet access service prepare and update confidential BGP security risk management plans. These plans would describe and attest to their efforts to follow existing best practices with respect to Route Origin Authorizations and Route Origin Validation using the Resource Public Key Infrastructure. In addition, we propose quarterly reporting for the largest providers to ensure we are making progress addressing this well-known vulnerability.

Thank you to my colleagues for working with me on this essential issue for network security. Thank you also to the staff behind this rulemaking, including Debra Jordan, Jim Schlichting, Nicole McGinnis, Austin Randazzo, Kenneth Carlberg, Sonja Rodriguez, Maureen Bizhko, James Wiley, Drew Morin, George Donato, Padma Krishnaswamy, Jim Zigouris, Bradley Rosen, Leah Calvo, and Haille Laws from the Public Safety and Homeland Security Bureau; Adam Copeland, Elizabeth Drogula, and Callie Coker from the Wireline Competition Bureau; Emily Talaga, Cher Li, Susan Lee, and Patrick Sun from the Office of Economics and Analytics; Tom Tran, Kamran Etemad, Jennifer Salhus, Saurbh Chhabra, Justin Park, and Barbara Esbin from the Wireless Telecommunications Bureau; Ryan McDonald and Victoria Randazzo from the Enforcement Bureau; Michele Ellison, Erika Olsen, Douglas Klein, William Huber, Jeffrey Steinberg, Anjali Singh, Chin Yoo, Wade Lindsay, Joel Rabinovitz, and Keith McCrickard from the Office of General Counsel; and Joy Ragsdale and Chana Wilkerson from the Office of Communications Business Opportunities.