REMARKS OF
FCC CHAIRWOMAN JESSICA ROSENWORCEL
BORDER GATEWAY PROTOCOL SECURITY WORKSHOP
WASHINGTON, DC
JULY 31, 2023

Good morning. Border Gateway Protocol or BGP, may not be a common household term, but as those of you in this room—or watching online—know, few technologies are more important for the internet. BGP manages how packets of data get transmitted between networks. It's central to the internet's global routing system. It's the protocol that allows independently managed networks on the internet to send traffic to one another.

Whether or not you've heard of it, we *all* rely on BGP every day when using the internet. 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, and shore up manufacturing.

You might be surprised to learn that something so critical in the modern economy came from such 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, was growing and expanding. The internet's basic protocols at the time couldn't 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 the BGP on three ketchup-stained paper napkins. What was meant to be a short-term solution developed on the sidelines of an IETF meeting is still with us today. And while BGP has allowed network operators to grow and evolve the modern internet, it was not designed with security in mind.

It's time to address that. Because it is vital to our Nation's economy that communication over the internet is secure. BGP's initial design, which remains widely deployed today, does not include explicit security features to ensure trust in exchanged information. As a result, an adversary may deliberately falsify BGP reachability information to redirect traffic. In fact, state-level actors have been suspected over the years of exploiting BGP's vulnerability to hijacking. These "BGP hijacks" can expose personal information, enable theft, extortion, and state-level espionage, and disrupt security-critical transactions, including in the financial sector.

Again, this needs attention. Although there have been efforts to help mitigate BGP's security risks since its original design, more work needs to be done, including facilitating and encouraging the uptake of newer security measures. We also need to work together to develop and implement industry standards and best practices that address BGP security.

To move forward, we need the full range of stakeholders together at the table. And today we are doing that, quite literally. The broad representation at this forum, including from our federal partners at the Cybersecurity and Infrastructure Security Agency, Office of the National

Cyber Director, National Institute of Standards and Technology, Office of the Director of National Intelligence, Department of Justice, and National Telecommunications and Information Administration and underscores the importance of this issue. We also need a common understanding of what current activities are underway, what is planned, and how best to ensure that we all are moving rapidly to identify and deploy the safeguards necessary for secure internet routing.

Today's workshop promises to help move this effort forward examining mitigation approaches, including emerging BGP security advancements, and identifying steps that need to occur to reach our common objective. I believe that with education, collaboration, and our collective expertise, we can make our communications networks and critical infrastructure more secure. Everyone here has a role to play in this effort to make our internet secure. We stand ready to support the development of industry commitments to quickly adopt critical measures to make BGP more secure.

It is my pleasure to now introduce my colleague working alongside us in this effort, Director Jen Easterly of CISA.

###