STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System,* PS Docket No. 15-94*; Wireless Emergency Alerts*, PS Docket No. 15-91; *Protecting the Nation's Communications Systems from Cybersecurity Threats*, PS Docket No. 22-329; Notice of Proposed Rulemaking (October 27, 2022)

October is Cybersecurity Awareness Month. It's an opportunity to recognize the importance of cybersecurity, take action to protect ourselves, and raise awareness about the steps we can take to stay safe online. This year's theme, "See Yourself in Cyber," emphasizes that cybersecurity is an issue for everyone, everywhere. That includes the Federal Communications Commission—where the work we are doing puts network security front and center.

We demonstrate that today with a rulemaking that would require Emergency Alert System and Wireless Emergency Alert participants to have a cybersecurity risk management plan in place and to ensure they have installed the most recent security patches. We then seek comment on other ways to improve the operational readiness of these systems, including reporting breaches to the agency. This effort will help ensure the function of these essential systems in emergencies and that the public can trust the warnings they receive. This is important because the Department of Homeland Security recently determined that some of this alerting infrastructure is susceptible to serious security vulnerabilities. While some patches have been released to fix these flaws, not everyone has installed them. We are committed to fixing that here and now.

This month—again, Cybersecurity Awareness Month—I also shared with my colleagues a proposal that would update our equipment authorization procedures to prohibit the sale of telecommunications and video surveillance equipment from five Chinese vendors that could pose a national security risk. Last week, I joined Deputy National Security Advisor Anne Neuberger at a White House workshop to advance cybersecurity for the Internet of Things. Last week I also announced a first-of-its-kind settlement against Truphone that will require the company to divest its unvetted Russian ownership, pay a civil penalty, and put in place new security procedures to vet any new ownership through the Office of Foreign Asset Control at the Treasury Department.

These efforts follow a series of other initiatives to keep our networks secure. We started by making our supply chains more transparent, by publishing the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Since then, we've updated that list to add equipment and services from five additional entities. We are removing insecure equipment from our universal service programs and from our networks through the Secure and Trusted Communications Networks Act Reimbursement Program. Working with our national security colleagues, we have revoked the Section 214 operating authorities of four Chinese state-owned carriers. We also have worked with the Department of State to update the 20-year-old process used for approving submarine cable licenses and with the Department of Justice to address related national security concerns. In addition, I have proposed stricter data breach reporting rules and launched inquiries on the security of internet routing and the security of the Internet of Things in order to reduce cyber risk. I also rechartered the Communications, Security, Reliability, and Interoperability Council and, for the first time, designated the Cybersecurity and Infrastructure Security Agency as a co-chair. And as today's rulemaking demonstrates, there's more to come.

Thank you to the Commission staff responsible for making all of this happen—and for ensuring that network security is now a priority for the agency. That is true during Cybersecurity Awareness Month and every month. A special thank you for today's rulemaking goes to

Debra Jordan, Nicole McGinnis, David Furth, Austin Randazzo, Rochelle Cohen, Ken Carlberg, James Wiley, Steven Carpenter, Minsoo Kim, Tara Shostek, Saswat Misra, Justin Cain, Shawn Cochran, John Evanoff, and David Sieradzki from the Public Safety and Homeland Security Bureau; Deborah Broderson and Douglas Klein from the Office of General Counsel; Aleks Yankelevich, Emily Talaga, Chuck Needy, and Cher Li from the Office of Economics and Analytics; Jeremy Marcus, Ashley Tyson, Janet Moran, Chris Sova, and Raphael Sznajder from the Enforcement Bureau; Charles Mathias and Ethan Jeans from the Wireless Telecommunications Bureau; Chana Wilkerson and Joy Ragsdale from the Office of Communications Business Opportunities; Zachary Ross from the Wireless Competition Bureau; and Sima Nilsson from the Media Bureau.