STATEMENT OF
COMMISSIONER GEOFFREY STARKS

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)

As technology becomes more sophisticated and integral to public life, the risk and occurrence of cyber-attacks has also increased at an alarming rate. The threat of cyber-attacks has permeated through every industry with digital capabilities, including the domestic public warning system we use in the United States. Specifically, the Emergency Alert System (EAS) and the Wireless Emergency Alert (WEA) system are two significant components of the national public warning system. Both services exist to deliver urgent national public warnings from state, local, and federal authorities when there is emergency information necessary to protect people and property from danger, such as inclement weather, and AMBER alerts. Given the significance of these services, it is especially important for the Commission to emphasize the security of EAS and WEA.

Unfortunately, in the last decade, the Commission has been made aware of several incidents that raise concerns about the security of the EAS and WEA systems. EAS and WEA systems have become increasingly susceptible to malicious intrusions and cyber threats without sufficient security measures in place to protect them. According to data collected by the Public Safety and Homeland Security Bureau during the nationwide EAS test in August 2021, more than 5,000 EAS Participants were using outdated software or using equipment that no longer supported regular software updates. In the area of equipment operational readiness, the test also revealed that an appreciable number of EAS Participants were unable to participate in testing due to equipment failure. Most recently, on August 1, 2022, the Federal Emergency Management Agency (FEMA) issued an advisory on a potential vulnerability in certain EAS encoder/decoder devices that have not been updated to most recent software versions. FEMA observed that if EAS devices are not up to date, an unauthorized actor could issue false EAS alerts over the EAS Participant's infrastructure. The same week, the Commission released another Public Notice highlighting the need for EAS participants to secure their EAS equipment. We simply cannot leave our alerting systems unprotected.

The proposals in the NPRM would require EAS Participants and Commercial Mobile Service (CMS) providers that participate in WEA take several steps to increase the operational readiness of these systems and improve the Nation's cybersecurity posture, including by addressing cybersecurity vulnerabilities that could be exploited by malicious cyber actors. First, the item proposes that EAS participants report unauthorized access of their EAS equipment, communications systems, and services within 72 hours of when it knew or should have known that the incident occurred, with details of the incident. Second, it seeks comment on whether we should require the same for unauthorized access to WEA systems and equipment. This is an important step. Without notice, unauthorized access could continue unabetted and spread to other EAS and WEA systems.

I'm glad to see that the item has proposed to have the reporting period match the amount of time identified in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). I've consistently said that the Commission's actions must be within the larger whole-of-government approach to protect our nation's networks and infrastructure. I'm confident that this proposal will compliment other efforts at the Cybersecurity and Infrastructure Security Agency as it implements the broader CIRCIA reporting requirements, and as we work together to secure our networks.

The item also proposes to require EAS Participants and Participating CMS Providers to annually certify to creating, updating, and implementing a reasonably sufficient cybersecurity risk management

plan to ensure the confidentiality, integrity, and availability of their respective alerting systems. I strongly support this proposal. Consistent with my recent efforts to push for providers receiving Universal Service Fund support to have cybersecurity risk management plans, it is integral that our networks are protected and that providers take affirmative steps to do so as part of their normal operations. To the extent that the Commission asks to see a copy of a provider's cybersecurity risk management plan, I appreciate my colleagues agreeing to my edit to propose that these plans be presumptively confidential. It is important that providers view us a partner on national security. To be so, we need to ensure that we are doing our part to protect their networks when they share information with us.

I also want to thank my colleagues for agreeing to another edit. As part of our proposal to require EAS Participants to adopt cybersecurity risk management plans, we will now seek comment on whether we should require the plans to be structured to follow the NIST Risk Management Framework or the NIST Cybersecurity Framework. The importance to the safety of life and property regarding EAS alerts cautions that allowing a cybersecurity risk management plan that doesn't meet the structure of the NIST gold standards is likely to be ineffective. If, as Shakespeare once said, "what's past is prologue," we need to be vigilant to avoid a situation where so many EAS participants did not update their system. Our recent experience with those in the path of Hurricanes Fiona and Ian reiterated the importance of EAS and WEA alerts. We must ensure and safeguard EAS's operational readiness. We must increase the Commission's situational awareness of disruptions to EAS. And, we must further prevent instances of cyber-attacks on EAS and WEA.

It is fitting that we are adopting this item now, as October is Cybersecurity Awareness Month. I thank the Public Safety and Homeland Security Bureau, and all the Commission staff that worked diligently on this item. It has my support.