

STATEMENT OF COMMISSIONER NATHAN SIMINGTON

Re: Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program, ET Docket No. 21-232; Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program, EA Docket No. 21-233.

The Notice of Proposed Rulemaking and Notice of Inquiry we adopt today ask exactly the right questions. These items will assist us in working out a precise and carefully tailored extension of the present legal and regulatory framework, thus further reducing security threats to the nation's communication networks. The information we seek today ensures that our evolving framework permits the Commission to eliminate more security threats without disrupting, or placing unnecessary burdens upon, the communications supply chain and equipment industry. It's straightforward: neither communications equipment, nor financial support for auction applicants, should be funded by any entity that the Commission has designated as a danger to our country's national security. There is a broad social consensus that we must take action. And so, I support taking a close look at how the Commission can expand the scope of these defensive measures beyond our universal service programs.

I also thank the Acting Chairwoman and my fellow commissioners for supporting my suggestion that, as part of the Notice of Inquiry, we take a close look at how radiofrequency (or RF) fingerprinting technology can play a central role in interdiction and enforcement of hacking and cyber-crime. RF fingerprinting uniquely identifies an individual wireless device, similar to the unique identification enabled by a human fingerprint. If we can identify specific devices involved in malfeasance, we can protect the security and privacy of wireless communications in an era of ever-increasing threats. Adopting an RF identification approach can also help manufacturers wishing to compete on the basis of superior security. The use of techniques such as RF fingerprinting could, for example, serve to demonstrate that a given manufacturer has taken action to mitigate security risks. Implementations of these technologies have matured significantly since the Commission last considered them and they are due for another look.

I'm pleased to vote to support this item and express my gratitude to the Commission staff for all of their diligent work.