Public Safety and Homeland Security Bureau, the Enforcement Bureau, the Media Bureau, the Wireline Competition Bureau, the Consumer & Governmental Affairs Bureau, the Office of Engineering and Technology and the Office of International Affairs Presentation to Commissioners

January 2025 Open Meeting

Panel 3: National Security, Public Safety, and Protecting Consumers

Presented by:

1. **Debra Jordan,** Chief, Public Safety and Homeland Security Bureau
2. **Peter Hyun,** Acting Chief, Enforcement Bureau
3. **Rosemary Harold,** Acting Chief, Media Bureau
4. **Alejandro Roark,** Chief, Consumer and Governmental Affairs Bureau
5. **Tom Sullivan,** Deputy Chief, Office of International Affairs

Joined at the Table by:

4. **Jodie Griffin,** Wireline Competition Bureau
5. **Jamie Coleman,** Office of Engineering and Technology

Slide 18: Introduction

Debra Jordan, Chief, Public Safety and Homeland Security Bureau

Good morning, Chairwoman and Commissioners.

I'm pleased to be here with Peter Hyun, Acting Chief of the Enforcement Bureau; Rosemary Harold, Acting Chief of the Media Bureau; Alejandro Roark, Chief of the Consumer and Governmental Affairs Bureau; Tom Sullivan, Deputy Chief of the Office of International Affairs; Jodie Griffin, Deputy Chief of the Wireline Competition Bureau; and Jamie Coleman, Associate Chief of the Office of Engineering and Technology.

As you know, the first sentence of the Communications Act lays out the FCC's national security and public safety mission. We are to make available rapid, efficient, and nation-wide communications service "for the purpose of the national defense" and "for the purpose of promoting safety of life and property." That mission has guided us over the past four years. Before I highlight some of our accomplishments, I want to stress that these represent the cooperative efforts of bureaus and offices from throughout the agency.

Slide 19: Promoting Network Security and Reliability

Supply Chain

To begin, the Commission took significant action in recent years to protect against national security threats to the communications supply chain of equipment and services in the U.S.

For example, the Commission launched the Secure and Trusted Communications Networks Reimbursement Program, more commonly known as Rip and Replace, to remove equipment and services

from Huawei and ZTE from communications networks. Thank you to the Wireline Competition Bureau for its work driving this critical initiative. Now that Congress has recently authorized the FCC to auction certain spectrum to fully fund the shortfall in the Rip and Replace Program, the agency has initiated a rulemaking to run the auction to support the new funding available for the removal, replacement, and disposal of covered communications equipment and services.

The Public Safety and Homeland Security Bureau published the first-ever Covered List of equipment and services that have been deemed to pose a threat to our national security.

And the Commission adopted new rules prohibiting communications equipment on this list from being authorized for importation or sale in the U.S. Thank you to the Office of Engineering and Technology for leading this work.

On another front, we worked closely with our partners at the Cybersecurity and Infrastructure Security Agency, other federal partners, and industry to bolster the integrity of the Border Gateway Protocol, which is central to the internet's global routing system, and proposed reporting requirements to improve internet routing security.

U.S. Cyber Trust Mark

The Commission also adopted the framework for a new voluntary cybersecurity labeling program for wireless consumer Internet of Things products. Qualifying consumer smart products that meet critical cybersecurity standards will bear a label—including a new "U.S Cyber Trust Mark"—that will help consumers make informed purchasing decisions, differentiate trustworthy products in the marketplace, and create incentives for manufacturers to meet higher cybersecurity standards. We are now standing up this comprehensive program, most recently selecting third party administrators to help run it.

Network Reliability and Disaster Response

The Commission took action to improve the reliability and resiliency of wireless networks. Our new Mandatory Disaster Response Initiative requires wireless providers to work together during disasters to reduce the impact of outages to the public. We activated it for the first time this hurricane season.

You are all familiar with our Disaster Information Reporting System, or "DIRS," where communications providers submit outage information to us during disasters. We analyze this data and issue daily communications status reports, which inform response efforts and keep the public apprised of restoration status.

The Commission launched a program to share this outage information in real time with state, federal, territorial, and Tribal nation agencies to help save lives. And the Commission expanded the scope and use of DIRS to close information gaps.

When hurricanes approached, we deployed staff to disaster areas to conduct pre- and post-landfall spectrum surveys. Through drive tests, often in challenging conditions, we determined the impact to radio and television and assessed capabilities for emergency services. We also analyzed the outage data submitted to us through DIRS and issued daily status reports–for Hurricanes Milton, Helene, Francine, Debby, Beryl, Lee, Idalia, Nicole, Ian, Fiona, Ida, and Nicholas, not to mention several tropical storms, wildfires in Hawaii and New Mexico, and other disasters.

We also stayed on top of sunny day outages, including issuing an investigative report detailing the cause and impact of a nationwide wireless service outage earlier last year, along with recommendations to help prevent similar outages in the future.

Slide 20: Strengthening 911

On the 911 front, the Commission required wireless providers to more precisely route wireless 911 calls and Real-Time Texts (RTT) to 911 call centers, which will result in faster response times and ultimately save lives.

The Commission established a national framework to accelerate the roll out of Next Generation 911 and support the deployment of advanced 911 capabilities—including video, text, and data—that will make the 911 system more resilient and help first responders save lives.

The Commission adopted rules to help end 911 fee diversion.

The Commission adopted rules to ensure that 911 call centers receive timely and useful notifications of network disruptions that affect 911 service. This will help call centers maintain emergency services and inform the public when to use alternative phone numbers to call them.

Similarly, the Commission adopted rules to ensure that the relevant officials receive timely information about 988 outages so that they can track trends and inform the public of alternate ways to contact the Suicide & Crisis Lifeline.

Slide 21: Improving Emergency Alerting

The Commission also strengthened emergency alerting in a host of ways, with some improvements underway now and others already up and running.

For example, the Commission is making Wireless Emergency Alerts, or WEA, more accessible by expanding multilingual alerting. In the future, participating wireless providers will support these life-saving messages in the 13 most commonly spoken languages in the U.S. as well as English and American Sign Language.

Participating wireless providers will also support the inclusion of maps in WEA messages that will show your location in relation to where the emergency is occurring.

The Commission established a new alert code to help save missing and endangered persons by delivering critical alert messages to the public over television, radio, and wireless phones. The new alert code will be especially beneficial to Tribal communities, where American Indians and Alaska Natives are at disproportionate risk of violence, murder, or vanishing. Thank you to our colleagues in the Consumer and Governmental Affairs Bureau for their great work on this.

The Commission adopted rules to make Emergency Alert System messages on television more clear and easier to understand and improved the way states plan for emergency alerts.

In addition, we joined with our partners at FEMA to run two nationwide tests of WEA and the Emergency Alert System. Also, for the first time ever, we entered into partnerships with dozens of state and local government agencies to assess the geographic accuracy of WEA through local tests. For *all* these tests, our analysis informed our policymaking and the public.

Slide 22: Helping First Responders Communicate

Last, but certainly not least, the Commission modernized and streamlined our rules for priority service programs, which help first responders and other emergency personnel communicate during disasters.

The Commission completed the 800 MHz rebanding, which eliminated a major interference threat to public safety radio systems and freed up additional spectrum capacity for public safety in the band.

And the Commission established a nationwide framework to solidify the 4.9 GHz band's status as public safety spectrum, while enabling the integration of technologies such as 5G.

Conclusion

These are just some of the actions taken in the past four years to enhance public safety and national security. (If I were to cover all our accomplishments, we'd be here much, much longer!) I want to thank the dedicated and talented staff of the Public Safety and Homeland Security Bureau. Through many late nights, weekends, and sometimes difficult conditions, the team has consistently delivered on its mission to help protect and serve the American people. Thank you also to the other bureaus and offices for their contributions.

Now over to Peter Hyun, Acting Chief of the Enforcement Bureau.

Slide 23: Monetary Overview

Peter Hyun, Acting Chief, Enforcement Bureau

Good morning, Chairwoman Rosenworcel, Commissioners, and thank you to Deb Jordan for the introduction.

I am privileged to serve as the Acting Chief of the FCC's Enforcement Bureau, alongside its talented professionals. Before I begin, I want to note that the highlights that will follow represent a small snapshot of the Enforcement Bureau's efforts over the past four years. I am limited by time and the topic of this panel, but it is important to say that I am extremely grateful and proud of all of the hard work undertaken by the dedicated public servants that make up the Bureau, as well as all of those here at the Commission.

In the past year alone, we have issued enforcement monetary actions amounting to over 340 million dollars. That's over 80 enforcement items released against entities and individuals who have violated our rules and, in turn, placed at risk not only the consumers who rely on our communications networks, but our nation's security as well. While monetary fines deter future bad acts, we have also sought to ensure that regulated entities implement measurable changes in practices and policies to comply with the law and the Commission's rules. As you will hear, through our Consent Decrees, the Enforcement Bureau required necessary improvements in how regulatees protect customer data, fix network vulnerabilities, and timely report incidents to the Commission. These terms will protect American consumers while simultaneously hardening our nation's networks from attacks from foreign adversaries.

Slide 24: Data Protection

After its creation in 2023, the Enforcement Bureau led the Commission's first Privacy and Data Protection Task Force. I want to thank all of the bureaus and offices for their continued efforts to coordinate across the Commission on a wide range of enforcement, rulemaking, and public awareness needs related to privacy and data protection. Through this Task Force, we undertook a number of substantial enforcement actions to protect consumers:

- We completed and resolved data breach investigations with all three major wireless carriers amounting to more than 50 million dollars in civil penalties and ordered significant changes to company cybersecurity and data protection practices.

- We issued over 200 million dollars in fines related to the major carriers' failure to protect consumer location data.
- In a case that was the first of its kind, the Bureau settled an investigation involving a carrier that violated not only the Commission's data breach notification rules, but also the carrier's obligations under a national security agreement with agencies from the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector's (commonly known as Team Telecom) where compliance with that agreement was a condition of the company's FCC license.
- We obtained a resolution in an investigation into a leading provider of captioning services for hearing and speech impaired individuals, for that company's illegal retention of call content.
    - That settlement amounted to 34 million dollars, an amount allocated to recovering taxpayer dollars for the U.S. Treasury, reimbursing FCC programs, and investments into required data protection improvements by the company across its suite of services.

Slide 25: Robocalls

Moving on to robocalls and robotexts. Through the Robocall Response Team, we have strengthened the Robocall Mitigation Database and our STIR/SHAKEN rules to reduce the number of scams that reach consumers.

- We have also mandated technology to stop illegal call spoofing, thereby empowering consumers to decide which calls they would like to receive.
- The Bureau supported the Commission's efforts to advance rules that enable the Commission to red flag phone numbers and require carriers to block texts from flagged numbers.
- In a case that was the first of its kind involving generative AI and audio deepfakes, the Commission adopted a 6 million dollar Forfeiture Order against an individual -- Steve Kramer -- for perpetrating an illegal spoofing campaign carrying an audio deepfake purporting to be President Joe Biden in an attempt to interfere with the New Hampshire presidential primary election. And we entered into a settlement with Lingo Telecom for its role in carrying this traffic without properly adhering to "Know Your Customer" obligations.
- We issued our first ever Consumer Communications Information Services Threat or C-CIST designation against Royal Tiger, a classification name given to a group of individuals and entities operating in India, the UK, the UAE, and the US, who persistently facilitated illegal robocalls aimed at defrauding and harming consumers. The classification was sent to state and federal and international partners and helps ensure that Royal Tiger traffic is no longer carried on the U.S. network.
    - And we have already followed up with C-CIST2, Green Mirage. Green Mirage is a network of threat actors that impersonate mortgage institutions to take advantage of vulnerable homeowners experiencing financial hardship. Green Mirage has spoofed the phone numbers of over 400 lenders and defrauded victims of hundreds of thousands of dollars. Our designation exposes Green Mirage's tactics, educates consumers, and strengthens industry and law enforcement's ability to detect these bad actors.

- Through EB's Spring Cleaning Initiative, we have sent Cease and Desist letters to a series of voice providers for facilitating illegal robocall campaigns on their networks that ranged from fake student loan scam calls to fraudulent debt consolidations efforts.

Slide 26: Securing Our Networks

The Bureau's national security-related efforts involved in some of the most important and impactful results. With close collaboration with our sister Bureaus and Offices, EB supported the Commission's shared goal to promote the reliability and security of our nation's networks:

- After a cyberattack caused a major 911 network outage, we resolved an investigation with Charter for 15 million dollars. Importantly, the settlement included first of its kind cybersecurity compliance terms, such as network segmentation and vulnerability mitigation management.
- In cases that highlights the Commission's important role regulating submarine cable landing licenses, the Bureau resolved two investigations for 1 million dollars each into the América Móvil Submarine Cable System, which connected the United States to two additional cable landing stations located in Colombia and Costa Rica, respectively, without FCC approval. Critically, the entities circumvented Team Telecom's important national security and law enforcement risk reviews – which is an essential part of the Commission's decision as to whether an authorization is in the public interest.
    - These settlements were groundbreaking. While they involved avoiding national security and law enforcement risk reviews for submarine cable licenses, they also demonstrated that avoiding Team Telecom reviews for foreign investment in communications infrastructure will similarly not be tolerated.
- And last year, the Commission enforced rules to hold accountable foreign manufacturers of FCC-authorized equipment, including consumer wireless devices. We will continue to act to protect the integrity of the Commission's equipment authorization program.

Lastly, I'll close by highlighting the important relationships we've established with our local, state, and international partners to protect consumers and protect those who seek to compromise our communications networks.

- The Bureau now has partnerships with 49 states, DC, and Guam on robocall enforcement matters.
- We now have information sharing agreements several international partners, including Ofcom and the Information Commissioner's Office in the United Kingdom, as well as the Privacy Commissioner of Canada.
- And, for the first time in the Bureau's history, the Enforcement Bureau convened regulatory partners from Australia, Canada, New Zealand, and the United Kingdom to discuss enforcement tools to address new and emerging threats to cybersecurity, data privacy, and national security. We hope to continue holding this event in the years ahead.

With that, I would like to reiterate my thanks to Chairwoman Rosenworcel, the Commissioners, the Bureaus and Offices, and, in particular, all of the Enforcement Bureau staff for all their work. Now, let me turn it over to Rosemary Harold, Acting Chief of the Media Bureau.

Slide 27: Key Highlights – Consumer Protections in Media

Rosemary Harold, Acting Chief, Media Bureau

Good morning, Chairwoman and Commissioners. In media services, an active consumer protection agenda included eliminating hidden billing fees and requiring "all-in" pricing disclosure by cable operators and satellite TV providers. Access to clear and accurate pricing helps consumers make informed choices. Also, we are requiring that cable and satellite TV operators provide public notifications when blackouts of a broadcast TV station occur due to a retransmission consent impasse lasting over 24 hours. This action allows consumers access to prompt and accurate information about service disruptions.

We took actions to make video programming more accessible to persons with disabilities. We adopted a plan to gradually expand audio description requirements to all television markets. In addition, we updated closed captioning display settings standards by requiring that such standards are readily accessible to individuals who are deaf and hard of hearing. These enhancements to accessibility will enable persons with disabilities to be better connected and informed by television programming.

To enable all consumers to be better informed, we adopted rules requiring for broadcast radio and television stations to identify and disclose purchases of airtime sponsored by foreign governments. This action upholds a long-standing tenet of broadcasting that the public has a right to know the identity of those who use the public airwaves. Also to support transparency, we initiated a proceeding regarding the use of Artificial Intelligence in political advertising.

And speaking of future technologies, we accepted the National Association of Broadcasters' invitation to participate in a public-private Future of TV initiative. This initiative worked to identify a roadmap, new ideas, and solutions to orderly transition ATSC 1.0 to ATSC 3.0-based services as smoothly as possible, and at the lowest possible cost, for consumers.

Thank you for the opportunity to highlight these important efforts. I'd like to now turn the mic over to our next presenter, Alejandro Roark of the Consumer and Government Affairs Bureau.

Slide 28: Protecting Consumers

Alejandro Roark, Chief, Consumer and Governmental Affairs Bureau

Protecting consumers is a core mission of the FCC. This is a responsibility we have taken seriously in the past four years by pursuing an aggressive consumer protection agenda.

Unwanted and illegal calls and texts have been a particular focus. These continue to plague consumers, and complaints about robocalls and robotexts perennially top the Commission's list of consumer complaints. We, therefore, worked over the past four years to further protect consumers from these unwanted and annoying communications.

First, the Commission bolstered its existing rules on robocall blocking and robocall mitigation, requiring providers to block illegal and unwanted calls before they reach consumers. Our new rules help stop scam calls coming from abroad, close loopholes in existing rules, and strengthen consumers' ability to stop unwanted and illegal calls.

The Commission also adopted its first-ever rules requiring the blocking of illegal robotexts. Unfortunately, illegal texts are becoming a common occurrence, and they present many of the same problems as illegal calls – an annoyance at best and a vehicle for fraud at worst. Thus, our rules now require that text messaging service providers block certain types of texts that are highly likely to be illegal.

Second, the Commission moved quickly to ensure that consumers are protected from harmful AI-generated robocalls and robotexts. The Commission proposed its first-ever rules to require that callers and texters inform consumers if such calls and texts are AI-generated. In doing so, the Commission proposed certain protections to ensure that positive uses of AI that may help people with disabilities can thrive. Taken together, these proposals represent a first step in addressing emerging technologies' impact on consumers.

On top of blocking and our focus on AI, the Commission made clear that when consumers change their mind after consenting to wanted robocalls and robotexts, they should be able to quickly and easily revoke that consent. And just last week the Commission adopted new rules to further tighten filing requirements for the Robocall Mitigation Database to better ensure widespread compliance and heightened awareness of provider responsibilities to protect consumers.

In addition to its work on robocalls and robotexts, the Commission took further efforts to enhance our consumer transparency initiatives and to ensure that consumers receive quality customer service from their providers.

For example, the Commission adopted rules requiring broadband providers to display, at the point-of-sale, labels that provide clear, easy-to-understand, and accurate information about the cost and performance of high-speed Internet services. The labels are modeled after the FDA nutrition labels and will help consumers comparison shop for the broadband plan that best meets their needs and budget.

More recently, the Commission launched a formal proceeding to review the quality of customer service that cable, broadband, satellite television, and voice service providers give their customers. This proceeding can help pave the way for future actions to ensure that customers are treated fairly and receive the best possible customer support from their providers.

In closing, I would like to thank the staff of the Consumer and Governmental Affairs Bureau for their hard work and diligence in developing policies that protect consumers. Without their dedication, none of these important policy achievements could have been accomplished.

Slide 29: National Security & International Affairs

Tom Sullivan, Deputy Chief, Office of International Affairs

Good morning, Chairwoman and Commissioners. The Office of International Affairs is proud to describe the efforts we have undertaken to help promote national security interests. In addition to concluding the Commission's revocation proceedings against four Chinese state-owned network operators, OIA has also undertaken three significant initiatives in recent times to help strengthen national security. First, we helped launch a rulemaking that explores regular review of international Section 214 authorizations to account for evolving security risks.

Stemming from this effort, a second achievement was completing the first-ever comprehensive collection of information from existing international section 214 holders regarding their foreign ownership. This information will help inform the Commission's next steps in the process.

The third significant action is a comprehensive review of the Commission's submarine cable policies. This is the first such effort in over 20 years and seeks to improve and streamline the rules to encourage deployment of these facilities while supporting the security, resilience, and protection of this infrastructure in a modern way. The item also proposes to keep foreign companies that have been denied or had its section 214 authorization revoked under the Communications Act on national security grounds

from obtaining submarine cable landing licenses. At the same time, it proposes to bar the use of equipment or services that are on the FCC Covered List from these licensed facilities.

Thank you, Chairwoman Rosenworcel and Commissioners.