Root Automation

112 4 H Way
Yreka, CA
96097

rroot@rootautomation.com
Ph: (530) 842-2690

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554
In the Matter of)
)
Build America: Eliminating Barriers) **WC Docket No. 25-253**
to Wireline Deployments)

REPLY COMMENT OF AN INDEPENDENT INTERNET SERVICE PROVIDER AND FORMAL NOTICE OF DATA SOVEREIGNTY AND JURISDICTIONAL LIABILITY

An independent, law-abiding facility-based Internet Service Provider (ISP) operating within the State of California respectfully submits these Reply Comments in response to initial filings concerning the Commission's proposed rules to establish expedited 120-day "shot clocks" and federal rights-of-way (ROW) permitting mandates.

These comments serve as a formal, explicit public warning to the Commission, state authorities, and competing telecommunications entities. The federal government has been, and is currently, funding infrastructure deployment via public grants to entities that willfully refuse to operate as historic, transparent, strict ISP-only common carriers. By permitting these entities to exploit federal public utility protections while operating as borderless, unregulated cloud-based Managed Service Providers (MSPs), the Commission is actively manufacturing a severe national security vulnerability and a systemic crisis of data liability.

I. The Jurisdictional and Statutory Fraud of "Commingled Services"

The initial comments filed by major telecommunications consortia seek to weaponize Section 253 of the Communications Act to strip local and municipal authorities of their historic rights-of-way governance. These large corporate entities argue that physical fiber-optic builds should enjoy expedited federal permitting shot clocks because the physical pipe *could* carry commingled telecommunications services (such as interconnected VoIP).

The Commission is fully aware that broadband internet access service is explicitly categorized as an *information service*, not a telecommunications service. A true public utility delivers a passive physical commodity to a property line and walks away. However, the corporate entities pushing for these federal mandates do not operate as passive conduits. They deploy vendor-locked hardware that actively monitors, inspects, and manages user traffic through closed-source, proprietary code.

By forcing local authorities to grant expedited rights-of-way access to networks running cloud-locked, non-auditable hardware, the FCC is enabling an illegal regulatory bait-and-switch. An entity that refuses to maintain clear local data boundaries—and instead operates an opaque management plane—forfeits any legitimate claim to public utility "common carrier" protections.

II. The Operational Collapse of CALEA and the Investigative Blind Spot

The Commission and federal law enforcement agencies are fully aware of the operational nightmare created by the death of localized hardware management. Under the Communications Assistance for Law Enforcement Act (CALEA), a facility-based broadband ISP is legally required to expeditiously isolate and deliver network metadata upon receiving a valid court order.

However, because the federal government has subsidized the deployment of hardware requiring mandatory tethers to centralized multi-state and international vendor clouds, local ISPs, no longer possess or control their own network telemetry. Customer IP assignments, locations, and internal router logs are scattered across borderless cloud data matrices.

When a law-abiding ISP obeys a court order, it can only hand over the outer packet pipe. The critical device-level metadata is buried in corporate cloud legal departments, completely paralyzing local, state, federal, and tribal law enforcement investigations. This Commission cannot, in good faith,

112 4 H Way
Yreka, CA
96097

rroot@rootautomation.com
Ph: (530) 842-2690

enforce expedited federal permitting shot clocks for hardware architectures that make statutory CALEA compliance and verifiable chains of custody mathematically impossible.

III. Formal Notice of Liability and the Multi-State Cloud Risk

Centralized corporate management clouds represent absolute single-points-of-failure for critical infrastructure. A single vulnerability or breach within a vendor's centralized "single pane of glass" web node leaves public utility networks, municipal services, tribal lands, and millions of residential routers wide open to mass exploitation by foreign adversaries.

Let this filing serve as definitive, permanent public notice: Any federal, state, or local entity that forces the expedited deployment of un-auditable, cloud-locked hardware by stripping local authorities of their rights-of-way gating powers assumes the direct legal and financial liability for the national security failures and consumer data privacy breaches that inevitably result.

IV. The Required Standard: A Return to Physical Isolation

To resolve this crisis and protect the public interest, the Commission must explicitly condition any federal shot-clock privileges or public grant eligibility on a strict **Right-to-Telemetry and Open Interface Standard.**

A true, safe public utility router must feature an unbundled, fully documented, locally controlled cryptographic API (such as standard REST or gRPC streaming) and be capable of complete configuration and operation without requiring data transit through an external vendor cloud. This hardware-isolated architecture allows a law-abiding ISP to remain a secure common carrier, empowers consumers to delegate network management to state-licensed local MSPs, and provides law enforcement with an unadulterated, instant local data trail.

Conclusion

The Commission can no longer deny the underlying financial machinery of the broken cybersecurity economy it is protecting. Centralized cloud lock-in does not protect the consumer; it protects a multi-billion dollar loop of recurring SaaS revenue, predatory software audits, and cyber-insurance cartels. The Commission must reject the self-serving mandates requested by big-tech monopolies and instead recognize that localized data sovereignty and strict out-of-band hardware management are the ultimate requirements for national cyber-resilience.

Respectfully submitted,

Dated: October 1, 2026