July 30, 2025

The Honorable Kristi Noem
Secretary
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Avenue SE
Washington, D.C. 20528

The Honorable Kash Patel
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue NW
Washington, D.C. 20535

RE: Critical Infrastructure Attacks Posing a Serious Threat to Public Safety, Daily Life, and Economic Security

Dear Secretary Noem and Director Patel,

On behalf of the undersigned trade associations representing broadband internet service providers across America, thank you and your agencies for your steadfast commitment to safeguarding the nation's critical infrastructure. We write today to highlight a significant and rapidly growing threat demanding urgent, coordinated federal, state, and local action: widespread, organized critical infrastructure attacks targeting our nation's communications networks.

Communications Networks as Critical Infrastructure

Today, communications networks form the backbone of virtually every modern service on which we rely—from emergency response and healthcare to transportation, finance, energy, and beyond. The Department of Homeland Security designates telecommunications as one of 16 critical infrastructure sectors, and the interdependencies that exist among these sectors mean that an attack on communications inflicts cascading damage across the economy, public safety and national security. When a fiber-optic cable is cut, or communications equipment is stolen, 911 centers go offline, hospitals lose access to cloud-based patient records, financial transactions stall, air traffic control and logistics systems stumble, and first responders are cut off from their dispatch centers. In short, our networks serve as lifelines that must be defended as vigilantly as power grids, water supplies, and transportation hubs.

As documented in our 2025 report, *Protecting the Nation's Critical Communications Infrastructure from Theft & Vandalism*, there were at least 5,770 reported incidents of targeted theft and vandalism against communications infrastructure reported nationwide in the last seven

months of 2024, disrupting internet service for over 1.5 million Americans and causing millions of dollars in damages. These attacks pose an existential risk to emergency response systems, healthcare services, transportation, financial networks, and the daily operations of communities across the country.

Critical infrastructure attacks pose a significant national security threat. These attacks demonstrate increasing sophistication, coordination and intent to disrupt services with potential economic and societal consequences. For example, in multiple cases, criminals have disabled 911 call centers, interrupted first responder networks, impacted airport operations, and even severed communications links at military bases—actions that far exceed petty theft and directly jeopardize public safety.

We deeply appreciate the investigative and enforcement efforts DHS and the FBI have undertaken to date and are grateful for your participation in our recent Summits on Protecting Critical Communications Infrastructure. Your engagement with industry leaders, state officials, and law enforcement has been instrumental in developing effective public-private strategies.

We also applaud recent interagency coordination efforts and the support you have provided to state and local partners in incident response. We encourage you to (1) treat these infrastructure attacks as domestic terrorism when the facts warrant, (2) allocate additional federal investigation and enforcement resources to high-incident regions, and (3) expand intelligence-sharing initiatives across federal, state, and local entities as well as with communications providers.

Expanding Resources and Tools to Combat Willful Attacks

Equally important, we ask for your support as we urge Congress to amend Title 18, Section 1362 of the U.S. Code so that willful acts against private communications networks—not just systems controlled or operated by the government—are explicitly criminalized at the federal level. While existing statutes reach government-targeted attacks, a gap remains in protecting the vast array of privately owned but publicly essential networks. By extending Title 18's destruction-of-communications provisions to apply to private infrastructure, Congress would close this loophole, ensuring that all perpetrators face the full weight of the law.

To this end, we urge the Administration to support H.R. 2784, Stopping the Theft and Destruction of Broadband Act of 2025. This bill reaffirms federal jurisdiction and imposes penalties for destruction and theft of private communications network facilities. Administration support of such legislation would underscore the government's commitment to safeguarding the physical security of critical assets and to prosecuting those who seek to sow economic and social upheaval by attacking the networks upon which so many consumers and businesses rely.

Communications providers stand ready to partner at every level of government to protect America's essential networks. These infrastructures are far more than economic engines—they

are lifelines that connect families, sustain communities, and keep our nation safe. Together, we must treat these threats with the urgency and gravity they deserve.

Thank you for your steadfast service in defense of our nation's critical infrastructure and public safety. We look forward to deepening our partnership to secure America's communications networks.

Sincerely,

ACA CONNECTS | AMERICA'S COMMUNICATIONS ASSOCIATION

ncta THE INTERNET & TELEVISION ASSOCIATION

NTCA THE RURAL BROADBAND ASSOCIATION®

USTELECOM THE BROADBAND ASSOCIATION