Remarks of FCC Commissioner Olivia Trusty

"Securing America's Communications Infrastructure: A Strategic Agenda for U.S. Leadership"

Hudson Institute

Washington, D.C.

January 12, 2026

Good afternoon. It is a pleasure to join you at the Hudson Institute. And a special thanks to Dr. Harold Furchtgott-Roth for the invitation to speak with you today.

Hudson has been a home to some of the most serious thinking on national security and technology policy anywhere in Washington, DC. Many of the conversations that have shaped U.S. strategy in the digital age have started in rooms just like this. So it is a privilege to contribute to that dialogue today.

When Americans think about national security, they often picture warships, warfighters parachuting out of helicopters, satellites, intelligence agencies, cyber defenders, and more. Those images matter. But underneath all of those images is something more fundamental: the strength and security of the communications infrastructure that connects our country.

Our military runs on it.

Our financial markets depend on it.

Our hospitals, power grids, schools, small businesses, and emergency responders rely on it every hour of every day.

We live in a world where everything from 911 calls to the stability of the global economy flows across networks built with fiber, spectrum, satellite pathways, and increasingly, software-defined architectures.

That means the security and resilience of these networks are not niche concerns. Indeed, this is not just an "IT issue." It is a foundational national priority.

Today, I want to explore what securing America's communications infrastructure means in a more contested environment; how the threat landscape has evolved; and what steps the FCC can consider as part of a broader national effort, working collaboratively with industry, federal partners, and Congress,

A Changing and More Complex Risk Landscape

My first point is simple: the threats and risks facing our communications networks today are more numerous, more sophisticated, and more intertwined than at any point in recent history.

The United States is in a strategic competition with authoritarian governments that view communications technologies as instruments of geopolitical influence. For example, China's investments across telecommunication supply chains, undersea cables, advanced wireless systems, and satellite constellations are extensive. Beijing is seeking to shape global standards, deployment models, and, in some cases, dependencies.

Russia, although smaller economically, remains aggressive in probing communications systems through cyber operations, jamming, and electronic warfare. Events in Europe have demonstrated how quickly communications disruptions can become national, regional, or even global-level challenges.

And other nations are developing sophisticated tools to target communications pathways, whether through cyber means, radio frequency exploitation, or interference with space systems.

All of these threats and more are expertly documented in President Trump's National Security Strategy.

But, one lesson is clear: communications networks are strategic terrain. And authoritarian competitors are increasingly acting like it.

There's another category of risk, that at times, is perhaps much closer to home.

Across the country, we are seeing a steady rise in physical threats to communications infrastructure. These include everything from opportunistic copper theft, to vandalism of cell towers, to coordinated attacks on network facilities. These trends are reflected in industry data, federal reporting, and state-level law enforcement coordination.

Although the motives vary, from criminal activity, to attempts to disrupt essential services, the outcomes are remarkably similar: damaged infrastructure, costly repairs, and service outages that affect entire communities.

When a major fiber line is cut, it can disrupt 911 services, interrupt broadband access for homes and businesses, delay transportation operations, and hinder critical facilities such as hospitals and financial centers. Even short duration outages can have cascading consequences in sectors that rely on precise timing or continuous connectivity.

And the most concerning threats increasingly combine physical and digital measures.

A physical disruption could be paired with a cyber intrusion. GPS interference might be timed to obscure unauthorized access to a critical site. Routing or cloud systems could be manipulated to coincide with targeted outages. Even a supply-chain weakness can be exploited during periods of network instability.

Responding to these types of threats requires innovative thinking about how to design networks to deter or detect these types of intrusions, adapt quickly, and recover gracefully when disruptions occur.

It also requires vigilance in maintaining clear lines of responsibility, coordinated preparedness, and information sharing across the entire ecosystem.

Now, I like to think that my focus on these issues is shaped, at least in part, by some of my childhood experiences. Growing up with six siblings, I quickly learned that no lock or closed door was ever truly secure. My younger sisters had a way of finding my hidden treasures including bracelets, clothes, even secret snacks, no matter how carefully I protected them. But, what I learned then, remains true now: threats are often creative, persistent, and unexpected. You can put up safeguards, but determined actors will probe for weaknesses. That's why, when it comes to our communications networks, resilience, redundancy, and rapid response matter just as much as prevention.

My time working on the Senate Armed Services Committee was also instructive. I saw firsthand how deeply the security of our communications networks is intertwined with America's military readiness and national resilience. It became clearer to me that cyber vulnerabilities are no longer abstractions debated in classified briefings, they have real-world implications for deterrence, crisis response, and the safety of our service members deployed around the world. That experience impressed upon me that protecting communications infrastructure is not only a technical challenge; it is a national security imperative. And it is for these reasons I have made this work a priority of mine at the FCC.

The FCC's National Security Role

Now, I understand that the FCC is not the Pentagon. It is not an intelligence agency either. And it is not the federal government's incident response arm. Nor should it be. But it does play a critical national security role, and has for decades.

That role is rooted in the Commission's responsibility to promote the reliability, resilience, and continuity of the nation's communications networks. Cybersecurity, in this sense, is a shared responsibility across the government and industry. While other agencies lead on threat intelligence and incident response, the FCC's focus is on ensuring that networks are built, operated and maintained in ways that reduce risk, limit disruption, and enable rapid recovery if or when incidents occur.

In recognition of the growing importance of this mission, the FCC has established a Council on National Security to strengthen coordination across bureaus and offices and to deepen engagement with our federal partners. That structure reflects an understanding that national security considerations touch nearly every aspect of the Commission's work, from licensing and spectrum policy to infrastructure reliability and space systems, to device integrity and security addressed through the Cyber Trust Mark program and other equipment authorization processes.

One important responsibility of the Commission is to evaluate applications and determine what vendors, technologies, and operators are permitted to participate in U.S. communications networks. Through the Covered List, licensing decisions, and close coordination with the national security community, the FCC helps prevent untrusted equipment from becoming embedded in the systems that underpin our country's economic and national life. A network is only as secure as its most vulnerable component. Our licensing decisions recognize that fact.

When it comes to spectrum, it is the nation's invisible infrastructure. It supports aviation, satellite connectivity, public safety, defense, and commercial innovation. Interference can disable GPS. It can compromise precision agriculture and financial timing systems. It can disrupt emergency operations, aviation safety, and other mission and life-critical services.

As spectrum gets more crowded and more valuable, the FCC's responsibility to ensure predictability, reliability, and protection from harmful interference becomes increasingly vital.

And, there's the FCC longstanding authority over outage reporting, 911 reliability, and disaster coordination. Many of those frameworks were built for yesterday's communications systems, systems based on copper loops, circuit switching, and geographically bound networks. Today's networks are hybrid, cloud-based, software-defined, and distributed. The Commission's ongoing efforts to reexamine how outage information is collected, how disruptions are addressed, and how reliability expectations are defined in an era of constantly evolving threats can enhance public safety, network resilience, and national security.

A Framework for Modern Resilience

As part of the broader Build America agenda, the Commission's work to modernize the resilience of our communications networks, I believe, rests on the following four pillars:

Pillar 1: Modernizing Legacy Infrastructure

Legacy copper networks are increasingly vulnerable to theft, weather-driven failures, and sabotage. Fiber networks, by contrast, are far more resilient, harder to steal, easier to secure, and more reliable. Modernization is not simply a broadband goal, it is a security goal.

As states, providers, and federal programs continue investments in next-generation networks, security and resilience should be explicit- not implicit- objectives by adhering to NIST best practices and CISA guidance. Modern infrastructure is not just faster; it is structurally harder to exploit.

Any review of resiliency frameworks should consider ways to support the transition to more modern systems, while ensuring no community is left behind.

Pillar 2: Hardening Critical Nodes

America’s networks have strategic choke points: long-haul fiber junctions; submarine cable landing stations; central offices and switching centers; satellite gateways; cloud interconnection hubs; and 911 centers.

A disruption to any of these can have regional or national consequences. While industry-led initiatives are essential, federal partners, including the FCC, can help encourage stronger protections, improved situational awareness, and deeper coordination as well as threat intelligence sharing with law enforcement. These issues are best addressed through public-private partnerships and collaborative models. We should avoid prescriptive regulations, or a one-size-fits-all approach, that reduces agility and flexibility in responding to new and emerging threats and ultimately create a false sense of security.

We should also be candid that some of our most significant vulnerabilities sit at precisely these intersections, places where digital and physical systems converge. Hardening them requires joint planning, realistic exercises, and a better, shared picture of risk.

Pillar 3: Space and Satellite Security

We are entering an era where LEO constellations, satellite backhaul, and hybrid networks are integral to our national infrastructure. Space is now a viable and growing part of our critical communications ecosystem.

The FCC’s responsibilities regarding licensing, orbital safety, debris mitigation, and spectrum management, are increasingly tied to ensuring a resilient and secure space economy. Our processes should reflect that reality.

And as space systems become more central to civilian and military communications, the Commission’s work will increasingly intersect with broader national security considerations, including interference resilience, supply-chain integrity for satellite components, and coordination with our allies to preserve a stable orbital environment.

Pillar 4: Data, Analytics, and Emerging Technologies

The FCC has access to enormous amounts of data, on outages, spectrum usage, equipment, and network performance. Data-driven tools, including AI, can strengthen detection of anomalous interference, predict outage risks, identify unauthorized devices, and illuminate supply-chain vulnerabilities.

The opportunity is not simply to collect more data, but to convert the data we already have into actionable insights. Advanced analytics, using artificial intelligence and quantum computing, can help spot patterns, across geographies, technologies, or time, that might otherwise remain invisible.

Leveraging these tools can help inform decisions more quickly and more accurately.

Expanded Focus Areas for Strengthening Communications Security

As the FCC looks ahead, several additional areas warrant deeper, sustained attention.

First, the United States must place greater emphasis on protecting submarine cables, the backbone of the global internet, from sabotage, untrusted equipment, and surveillance risks. This work necessarily requires close coordination with the State Department, the intelligence community, and our allied partners, because these cables are both international assets and shared vulnerabilities.

Second, we need stronger cross-border spectrum coordination, especially in regions where foreign military activity or state-backed operations may create interference risks for U.S. aviation, GPS, satellite systems, and other critical services. These issues cannot be managed solely within our borders. They demand a strategic, international approach.

Third, the FCC can help support more robust situational awareness tools for state, local, and tribal emergency authorities. These officials increasingly depend on timely, accurate, and actionable information about network outages, and modernizing those tools would strengthen response and recovery during crises.

Fourth, the FCC, in coordination with our federal partners and the private sector, would benefit from engaging in more realistic, multi-sector resilience exercises – drills that simulate the kinds of complex emergencies our networks may face. These should test scenarios such as a coordinated physical attack on a fiber hub occurring simultaneously with a cyber intrusion on a cloud routing provider. Exercises like these help highlight seams, reveal dependencies, and strengthen preparedness long before a real crisis occurs.

Finally, international engagement remains essential. Promoting secure standards and trusted vendors in global forums ensures that vulnerabilities are not embedded in systems before they even reach U.S. shores. Early engagement in standards bodies can help shape a more secure, interoperable, and resilient global communications environment.

Characteristics of Resilient Networks

Now, stepping back for a moment: when it comes to security investments we know they are not free. But the costs of insecurity are far higher. Every year, physical attacks, cyber incidents, and network failures impose massive economic costs on businesses, consumers, and governments.

Resilient networks share common characteristics: redundancy, modern equipment, trusted vendors, backup power, clear reporting processes, and coordinated engagement with public safety

Policies that support these characteristics, through clarity, predictability, and adaptability, can strengthen the entire system.

And as discussions around the future of the Universal Service Fund continue in Congress and at the FCC, it is worth recognizing that resilient networks in rural America are as important to national security as those in major hubs.

A Shared Responsibility

Back at the Commission, where we continue to create a "Golden Age of Communications," resiliency remains a key part of this ongoing effort.

The FCC, however, cannot do this alone. In fact, no single agency can. Industry owns and operates the vast majority of America's communications infrastructure. Their expertise and visibility are indispensable. We need strong information-sharing channels, joint preparedness exercises, clear communication during emergencies, and continued leadership in developing best practices.

Likewise, interagency coordination, with NTIA, CISA, The Department of War, State Department, and others, is essential for spectrum planning, supply chain risk reviews, disaster response, and international engagement.

And, as I mentioned earlier, this work must extend beyond our borders. Allies and partners face many of the same challenges we do: untrusted vendors, growing space congestion, interference concerns, and submarine cable vulnerabilities. Through standards bodies, bilateral engagement, and multinational forums, we can promote secure, interoperable, and democratic communications systems worldwide.

Let me offer a short list of areas where I believe the FCC, working with its federal partners, industry, and Congress, could constructively focus in the years ahead: reevaluating outage reporting to reflect modern networks; strengthening transparency around supply-chain risks; supporting responsible space and satellite growth; advancing spectrum policies that incorporate security considerations; encouraging modernization of vulnerable legacy networks; integrating AI into networks and FCC decision-making; expanding coordination with law enforcement on infrastructure vandalism; and deepening collaboration with allies on international communications security.

These are all areas where thoughtful work can make our national communications ecosystem stronger and more secure.

Finally, let me close with a simple truth: the strength of America's communications infrastructure has always been a source of national power. It has supported our economy, connected our people, and provided the foundation for our leadership in the world.

But maintaining that strength requires vigilance, investment, and a recognition that every fiber link, every antenna, every satellite, and every switch is part of a larger system that underpins our national life.

Securing that system is not the job of any one agency or any one Commissioner. It is a shared responsibility, across industry, government, and international partners.

If we meet that responsibility with seriousness and unity of purpose, America will continue to lead the world in innovation, resilience, and strategic strength.

Thank you.