Testimony of Robert Mayer
Senior Vice President, Cybersecurity and Innovation
USTelecom – The Broadband Association

Before the Senate Committee on Commerce, Science, and Transportation's Subcommittee on Telecommunications and Media

Signal Under Siege: Defending America's Communications Networks

December 2, 2025

The Threat Landscape

Chair Fischer, Ranking Member Luján, and Members of the Subcommittee:

Thank you for the opportunity to testify. I am Robert Mayer, Senior Vice President of Cybersecurity and Innovation at USTelecom – The Broadband Association whose members include the full scope of our nation's communications providers – including national, regional and local companies and cooperatives. I also serve as Chair of the Communications Sector Coordinating Council which represents broadcast, cable, satellite wireless, and wireline industries. The mission of said council is to ensure that communications networks and systems are secure, resilient, and rapidly restored after a natural or man-made disaster.

Cybersecurity has become one of the most persistent and complex national security challenges our country faces. That challenge spans the nation's entire critical infrastructure landscape. Energy systems, financial networks, transportation systems, cloud environments, public sector networks, and communications providers all contend with sophisticated, state-backed and state-funded adversaries - such as China, Russia, and Iran. These actors have positioned themselves to conduct long-running campaigns designed not just to disrupt, but to stealthily infiltrate multiple sectors of U.S. infrastructure.

These threats are not hypothetical. In recent years, state-sponsored actors have attempted to infiltrate or actually infiltrated: US energy grids, water utilities, ports, and telecommunications infrastructure. Not only are these attacks more overt, more sustained, and more aggressive than we have seen before, but the attack surface has also gotten a lot broader. Instead of just denying service to a single website or releasing ransomware at a single location, these actors are looking to preposition deep into network infrastructure, and they are looking at the entire ecosystem of cybersecurity, sometimes using third-party vendors and other more distant access points to get at critical infrastructure.

Beyond incidents visible to the public lies the quiet, steady probing by these state-sponsored adversaries who use automation, machine learning, and tailored tradecraft to identify and exploit vulnerabilities, test defensive reactions, and constantly adapt their tactics, techniques and procedures. They do this across critical infrastructure as a whole.

In a landscape like this, cybersecurity cannot be treated as a static checklist or a one-time investment. It has to be a continuous mission: understanding how adversaries are changing, how technologies are evolving, and where the most serious risks are emerging. It requires close and continuous coordination between those who operate critical systems and those in government who see the broader pattern of foreign activity. Private industry is a critical stakeholder in this environment, but we cannot do it alone.

Our national response must remain anchored in a clear understanding of responsibility: the culpability for these attacks lies with the nation-states that conduct them, not the industries and organizations that are aggressively working to defend against them. Importantly, under the leadership of National Cyber Director Sean Cairncross, we expect the updated US National Cybersecurity Strategy will underscore this point—emphasizing a more proactive, consequence-based approach tied to real-world threats. As an industry, we stand ready to work closely with the White House and Congress, aligning our capabilities with the strategy's expected call for strengthened public-private partnerships and shared defense efforts.

What We Are Doing

Over the past two decades, the communications sector and the federal government have built a partnership model that has grown more mature and more operational over time. In our sector, that collaboration is organized through the Communications Sector Coordinating Council (CSCC), which includes 57 companies of different sizes, technologies, and regional footprints. The CSCC works closely with the Government Coordinating Council, which brings together DHS, CISA, the FCC, DOJ, the Department of War, NSA, and other agencies. Together, these bodies provide the basic architecture for joint planning, risk assessment, and information sharing. Providers participate in regular operational briefings, including classified briefings on a biweekly cadence, with CISA, law enforcement, as well as military and intelligence agencies. In these settings, industry and government experts discuss constantly evolving threats and mitigation strategies.

In addition to these recurring engagements, communications providers participate in a broader ecosystem of public-private collaboration. That includes the Joint Cyber Defense Collaborative, which brings industry and government together on joint planning and response; the Communications Information Sharing and Analysis Center, which supports operational information sharing among providers; the Network Security Information Exchange and the National Security Telecommunications Advisory Committee, which provides technical and strategic perspectives; and the Enduring Security Framework led by NSA and CISA, which focuses on the intersection of national security and commercial technology. Each of these forums plays a different role, but together they create a fabric of collaboration that has proven its value repeatedly.

Cybersecurity programs are continuously evolving. Our members meet—and very often exceed—cybersecurity requirements as conditions for authorization to provide services, bid on government contracts, and participate in government programs, as well as to ensure customer trust in the competitive global marketplace.

Not every network is the same. A large nationwide carrier, a regional operator, and a local rural provider have unique network architectures. But across the sector, you see the same themes: more rigorous identity and access management; stronger protections around administrative interfaces; increased segmentation of networks so that an issue in one area does not automatically spread to others; more systematic logging and analysis of activity; implementation of zero trust architecture; and a steady push to close known vulnerabilities faster.

Recent campaigns attributed to sophisticated state-sponsored actors have pushed these efforts further. Providers have shortened patching timelines, reexamined remote-access configurations, expanded threat-hunting programs that look for subtle indicators of compromise, tightened vendor-security requirements, and invested in new analytic capabilities that help distinguish normal from abnormal behavior in large volumes of data. Many are also planning ahead for future classes of risk, including the eventual need for quantum-resistant cryptography to protect the most sensitive communications.

Industry collaboration has deepened as well. Providers, through CISO-level coordination among major North American carriers**,** are standing up the Communications Cybersecurity Information Sharing and Analysis Center (C2 ISAC), a next-generation platform for real-time threat sharing and joint analysis. At USTelecom, we also have created various coordinating and information-sharing platforms such as the International Communications CISO Council (ICCC), and the Council to Secure the Digital Economy (CSDE), bringing together high-level U.S. and international executives to foster sharing best practices, information, and insights. These initiatives reflect a simple reality: no single company sees everything, and timely peer-to-peer sharing of high-quality information makes every participant more resilient.

All of this work takes place while communications providers continue to deliver reliable service at national scale, all while expanding both the infrastructure that will enable AI to promote American economic competitiveness, scientific and engineering discovery, and cyber defenses themselves, as well as the broadband access that brings education, healthcare, and economic opportunity to more Americans.

Call to Action

Congress can help advance our sector's mission. The goal should be to reinforce what is working in our national cybersecurity posture and to avoid unintentionally weakening it.

Foremost, our existing **public–private partnership model should be preserved and strengthened**. The existing ecosystem—Sector Coordinating Councils, Government Coordinating Councils, information-sharing organizations, and joint planning bodies—gives us a way to bring together operational experience and national-level intelligence. It has the flexibility to evolve as threats evolve. It encourages frank discussion and early reporting. Those are not easy things to recreate once lost.

From the perspective of communications providers, several additional principles stand out. First, Congress can make a tangible difference by **strengthening information-sharing authorities**. The CISA 2015 framework establishes clear guidance and protections that enable

companies to report threats quickly and safely. The current short-term extension is helpful, but Congress must pass a long-term reauthorization to maintain trust, improve early voluntary reporting, and better align industry capabilities with federal intelligence and response efforts. Restoring those authorities would reinforce trust and encourage the early voluntary reporting that is so important to effective defense.

As part of this information sharing, **interagency collaboration needs to be enhanced**. We continue to see challenges in collaboration between Federal agencies, which at times has placed the industry in the position of helping coordinate between multiple agencies. Congress can play an important role in driving more effective and sustained interagency collaboration.

Any, **cybersecurity frameworks need to be flexible and adaptive.** While there may be a natural impulse to impose a detailed cybersecurity checklist, when requirements are fixed in place they create two primary problems; they lag behind adversaries who change their techniques faster than any rule can be written, and they shift attention from managing real risk to managing paperwork, which means a provider can be fully compliant yet still exposed. Cybersecurity regulations end up hardwiring yesterday's best practices into law while the adversary moves on.

In a sector as diverse as communications, technical prescriptions are especially problematic for regional and smaller carriers that differ widely in resources, size, topology, and technology. Forcing all of them into a single mold will redirect limited resources away from high value security investments.

Most importantly, overly prescriptive mandates can have a chilling effect on the very collaboration that has proven essential. When every deviation from a mandated standard carries potential regulatory consequences, organizations become more cautious about what they share and who they share it with. Early and validated reporting of threats is what allows a pattern to be recognized and properly addressed. We should be encouraging companies to share information quickly and avoid liabilities that make them hesitant to do so.

Second, we must **future-proof our nation's cybersecurity investments** by ensuring American leadership in AI, quantum, and other emerging technologies. The boundaries between cybersecurity and AI innovation are becoming increasingly indistinguishable as AI becomes both a critical tool for defending networks and a powerful capability in the hands of adversaries. Strengthening our position in AI is therefore inseparable from strengthening our cyber posture, which makes it all the more essential to accelerate the infrastructure that AI depends on.

In parallel with these efforts, Congress can help providers deploy more modern and secure networks by retiring outdated copper infrastructure regulation and streamlining AI infrastructure and broadband permitting processes. Our members stand ready to deploy modern networks, but permitting obstacles at the federal, state, and local level result in costly delays. Congress should speed up National Environmental Policy Act (NEPA) and National Historic Preservation Act (NHPA) approvals for AI infrastructure and broadband permits.

Third, policy should ensure that **local and regional providers are not left behind**. While large carriers may have extensive internal cybersecurity resources dedicated to engagement with

federal partners, smaller providers do not always have that opportunity. Existing funding mechanisms—such as BEAD non-deployment funds and related federal or state initiatives—should therefore be strategically leveraged to strengthen local and regional providers' capabilities, including the retirement of vulnerable end-of-life equipment. These programs can also play a critical role in supporting cyber workforce development, ensuring that smaller providers have sustained access to trained personnel who can effectively manage evolving threats.

Communications providers are committed to doing their part. We are investing significantly in our own defenses, engaging actively in public–private partnerships, and recognizing that the threat environment is only growing more complex. Cybersecurity is a shared responsibility, and the most effective path forward is one that combines operational expertise, national-level intelligence, and policy frameworks that support collaboration rather than rigidity.