

# CASE STUDY



## Strengthening Cybersecurity for a Regional Telecom's FCC Compliance

To meet requirements for the BEAD program, which funds broadband expansion in rural and underserved high-cost areas, the client partnered with AIS Network for a two-phase cybersecurity initiative. Aligned with NIST 800-53, and FCC standards, AISN delivered tailored security policies, vulnerability scanning and remediation, penetration testing, incident response planning, and a sustainable compliance roadmap to ensure regulatory adherence and protect critical infrastructure.

## Client

A rural telephone cooperative operating in the Appalachian region and providing state-of-the-art voice and data services in a global environment. As a participant in the Broadband Equity, Access, and Deployment (BEAD) program, the client must meet stringent cybersecurity and compliance requirements to secure federal funding for broadband expansion.

## Challenge

The client had submitted a Cybersecurity Risk Management Plan to meet Federal Communications Commission funding criteria but lacked the technical and organizational controls for full compliance. Under FCC pressure to demonstrate immediate due diligence and address vulnerabilities, the organization needed a sustainable, NIST-based security program. With limited internal resources and a small IT team, they sought a managed security services partner for expert guidance, technical implementation, and cost-effective support.

## Solution

AISN launched a focused initiative to meet urgent regulatory goals, starting with scans of internal, external, and subscriber networks, system hardening, and establishment of monthly scans and biannual penetration tests. AISN also crafted a NIST 800-53-aligned security policy suite and an incident response plan, validated through a tabletop simulation to refine decision-making and test escalation protocols. Further, AISN streamlined governance, appointed an internal Information Security Officer, and provided threat intelligence feeds, endpoint protection, and staff awareness training.

## Results

AISN remediated the identified vulnerabilities, enabling the client to maintain a robust cybersecurity posture with hardened systems, tested incident response procedures, and a comprehensive policy suite aligned with BEAD program requirements. AISN's vulnerability scanning and penetration testing strengthened proactive risk management across internal and subscriber-facing systems. The client has implemented routine scanning and ongoing security operations and is well-positioned to secure and retain BEAD funding, expand broadband access safely, and serve as a model for rural telecom providers.

