DELIVERABLES

EASY DYNAMICS℠

MANAGED CYBERSECURITY SERVICES FOR RURAL BROADBAND

Rural broadband service providers face unique cybersecurity and compliance challenges. Our experts are here to help.

Telecommunications service providers understand that cybersecurity is critical to their daily operations: Safeguarding data, ensuring network reliability, complying with federal mandates, and securing supply chains are all vital concerns. For broadband providers operating in rural areas, these efforts can be particularly frustrating due to limited available resources and underinvestment in security measures. **To help clear these hurdles, Easy Dynamics has developed a tailored approach to managing the rural broadband industry's unique cybersecurity and compliance challenges.**

Regulatory Background

In December 2024, national security officials reported that state-sponsored hackers had successfully infiltrated the networks of at least eight U.S. telecommunications companies. The foreign operation not only compromised sensitive systems and data, it also underscored the vulnerabilities in our critical communications infrastructure. In response, the Federal Communications Commission (FCC) **issued a Declatory Ruling and proposed new cybersecurity requirements,** both actions aimed at strengthening telecommunications network security.

The CALEA Declaratory Ruling

Prior to 2025, the FCC agreed that under section 105 of the Communications Assistance for Law Enforcement Act (CALEA), telecommunications carriers' duties were limited to avoiding the risks associated with using untrusted equipment in their networks. However, in its January 2025 Declaratory Ruling, the FCC clarified that carriers' affirmative obligations extend beyond their physical equipment to include their network management practices:

> *"...With this Declaratory Ruling, we clarify that telecommunications carriers' duties under section 105 of CALEA* ***extend not only to the equipment they choose to use in their networks, but also to how they manage their networks."***

To satisfy these requirements, telecommunications carriers are expected to implement basic security hygiene practices like minimum password strength, multifactor authentication, and role-based access controls. Carriers will need to deploy enterprise-level cybersecurity measures across their networks, including patching vulnerabilities to protect surveillance systems and other network elements against known exploits. **Without these basic measures in place, it's unlikely that carriers will meet their section 105 obligations and avoid monetary penalties.**

Newly-Proposed Requirements

The FCC has also proposed requiring telecommunications providers to create and implement cybersecurity and supply chain risk management plans. Under the new rule, providers would need to demonstrate how they protect their networks and supply chains from security threats, and submit annual certifications that their plans are in place and enforced. Aside from the Enhanced ACAM providers that this mandate already applies to, the requirements would extend to a wider range of telecommunications services, including broadband, cable, wireless, and satellite. While these newly-proposed rules are temporarily paused pending review, **it's vital that telecommunications providers prepare themselves now to comply with these potential new requirements.**

How Can Easy Dynamics Help?

Easy Dynamics offers a subscription-based suite of managed cybersecurity services specifically tailored for rural broadband providers, effectively bridging the resource gap to solve compliance challenges and address the industry's top cybersecurity priorities. With our team as your trusted partner, you'll get the technical support and expert guidance to successfully navigate complex federal requirements, maintain program funding, and deliver reliable services to your community well into the future.

✓ Critical Infrastructure Security

Assess the vulnerability of your critical infrastructure and develop strategies to resolve security gaps

✓ Data Security

Review data handling procedures to identify potential security vulnerabilities and improve cyber hygiene practices

✓ Network Reliability

Identify potential threats to your network reliability and deploy proactive mitigation strategies

✓ Enhanced ACAM Compliance

Leverage our hands-on experience navigating compliance mandates to maintain your federal program funding

✓ Supply Chain Threats & Vulnerabilities

Identify security gaps in your supply chain, develop mitigation strategies, and deploy proactive risk management policies

✓ Security Hygiene Awareness & Training

Ensure your workforce adheres to security hygiene best practices with expert-led awareness and training services

CONTACT US

Ravi Shankar
Director of Risk Management
rshankar@easydynamics.com

FEDERAL EXPERIENCE

- Department of Agriculture
- Department of Homeland Security
- Defense Information Systems Agency
- Defense Logistics Agency
- Naval Special Warfare Command
- Federal Law Enforcement Training Center
- National Institute of Standards and Technology
- Cybersecurity and Infrastructure Security Agency
- Internal Revenue Service
- General Services Administration
- Department of the Treasury
- Health & Human Services
- Social Security Administration
- Department of Education

CORE CYBERSECURITY CAPABILITIES

- ICAM
- Cloud Modernization
- Risk Management
- Automation & Resiliency

aws PARTNER Select Tier Services
Microsoft Solutions Partner
SailPoint okta
CMMI DEV/3 CMMI SVC/3