OneLayer & NERC CIP Compliance

Extending Internal Network Security Monitoring (CIP-015) Across PLTE and Public Cellular Networks

Executive Summary

As utilities evolve toward digital, distributed, and connected infrastructures, both Private LTE (PLTE) and Public Cellular APNs play a central role in critical operations. These cellular networks now form part of the Electronic Security Perimeter (ESP) around Bulk Electric System (BES) assets, bringing new visibility and compliance challenges under the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards.

OneLayer bridges the gap between traditional OT network security and cellular connectivity, offering continuous monitoring, device-level visibility, and policy enforcement that align directly with the most recent NERC CIP mandates—including the new CIP-015 Internal Network Security Monitoring (INSM) requirement.

The Evolving NERC CIP Context

NERC CIP defines the cybersecurity standards that protect the reliability of North America's Bulk Electric System. These standards mandate the identification, protection, monitoring, and control of all systems impacting BES operations, with fines of up to $1M per day for non-compliance.

Recent revisions to NERC CIP introduce stronger requirements for Internal Network Security Monitoring (CIP-015)—demanding that utilities detect and respond to anomalous activity within the ESP, not just at its boundary. This shift recognizes that cyber threats often originate inside the network—whether through compromised endpoints, rogue devices, or misconfigured assets.

Defining the ESP in Cellular Environments

The concept of an Electronic Security Perimeter changes when extended into cellular domains.

Private LTE (PLTE)

ESP Consideration

The PLTE core (EPC/5GC) resides inside the ESP. The ESP may extend to include the radio segments carrying BES traffic.

CPE / SIM Role

The CPE and SIM serve as authenticated gateways—forming micro-perimeters within the ESP.

Public Cellular (APN)

ESP Consideration

The APN and its secure tunnel (VPN, MPLS, or SD-WAN backhaul) extend the ESP into the public carrier domain.

CPE / SIM Role

The CPE/SIM identity represents the logical boundary for visibility, policy, and anomaly detection.

How OneLayer Enables CIP-015 Compliance

Internal Network Visibility

Monitors **control, management, and user planes** across PLTE and APN traffic.

Detects unauthorized activity such as rogue or misconfigured device connections, lateral movement, or abnormal data patterns.

Provides visibility even within carrier-managed APN infrastructures. This includes the ability to centralize device visibility across multiple carrier portals.

Maintains a real-time, accurate device inventory, including the identification and monitoring of non-cellular devices connected downstream of cellular routers and adapters.

Defined Electronic Security Boundaries

Maps device identities (IMEI, IMSI, SIM) to BES assets and operational zones.

Establishes micro-perimeters per device or SIM, aligned with ESP segmentation principles.

Integrates with carrier and enterprise policy frameworks for unified security posture.

Anomaly Detection and Response

Correlates events with SIEM/SOC tools to detect anomalies early.

Flags deviations from expected behavior (e.g., geography, communication peers, DNS domains).

Enables automated containment and adaptive response based on risk scoring.

Re-identifies and takes necessary action on devices returning from failover/roaming to public carrier networks

Compliance-Ready Monitoring and Reporting

Generates logs aligned with CIP-008 (Incident Response), CIP-010 (Change Management), and CIP-015 (INSM) requirements.

Delivers audit-ready reports and dashboards that simplify regulatory validation.

Reduces audit effort through continuous compliance evidence.

OneLayer's Broader NERC CIP Alignment

NERC CIP Standard	Description	OneLayer Contribution
CIP-002	BES Cyber System Categorization	Device fingerprinting and dynamic inventory across PLTE and APN-connected assets
CIP-005	Electronic Security Perimeter	Defines and enforces access control across private and carrier networks
CIP-006	Physical Security	Detects unauthorized LTE device associations
CIP-007	System Security Management	Monitors compliance with baselines and patch status for cellular assets
CIP-008	Incident Response	Triggers incident workflows for cellular-based anomalies
CIP-010	Configuration Change Management	Detects firmware or configuration deviations on cellular endpoints
CIP-011	Information Protection	Enforces encryption, secure SIM provisioning, and data protection policies
CIP-013	Supply Chain Risk Management	Validates SIM and device integrity throughout vendor lifecycle
CIP-015	Internal Network Security Monitoring (INSM)	Enables continuous, behavior-based monitoring inside PLTE and public APN environments; including public/private hybrid network setups

Business Impact for Utilities

Without OneLayer:

Cellular traffic remains opaque to traditional IT/OT monitoring tools, creating compliance blind spots within the ESP.

With OneLayer:

Cellular domains become visible, traceable, and secure—helping utilities:

- Maintain full visibility into BES-connected devices, regardless of network type.
- Detect and contain cyber anomalies before they impact critical operations.
- Demonstrate CIP-015 readiness through actionable telemetry and audit evidence.
- Maintain compliance across public, private, and hybrid scenarios as your network strategy evolves

CIP-015 requires utilities to detect threats inside their ESPs. OneLayer extends that visibility into every cellular domain—Private LTE and Public APN alike.

By unifying visibility across all cellular connections, OneLayer ensures utilities can protect their expanding digital perimeter and stay fully aligned with evolving NERC CIP standards.

Let’s Secure Your PLTE Network — Together

Contact our team to schedule a demo today!

Email: info@onelayer.com
Website: www.onelayer.com

ONELAYER

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION