WHITE PAPER · CRITICAL INFRASTRUCTURE

Reliability Is Not Resilience

How ALIGN Applies NERC CIP Standards for Electric Utilities and Critical Infrastructure Operators

AUTHOR
Paul Corgel

PUBLISHED
June 2026

READ TIME
9 min

SECTORS
Electric Utilities · Critical Infrastructure · Energy Sector

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are the mandatory regulatory framework for cybersecurity and operational resilience of the Bulk Electric System (BES). Enforced by NERC, regional entities, and FERC, the CIP standards establish minimum requirements for asset identification, access control, personnel security, physical protection, incident response, and recovery planning across utilities that operate or depend on the interconnected grid.

For NERC auditors, CIP compliance is the standard. For the utility, CIP compliance is not the same thing as operational resilience.

The CIP standards were designed to establish mandatory minimums for cybersecurity and physical security of the Bulk Electric System, not to produce operational resilience programs that hold when a black-sky event, physical attack, or sophisticated cyber intrusion tests multiple standards simultaneously. Utilities focused only on CIP compliance often end up with programs that do not connect to each other.

ALIGN applies NERC CIP compliance into integrated operational resilience. Each CIP standard maps to an ALIGN phase, but ALIGN goes further, connecting CIP requirements to the government emergency management network, building cross-functional decision architecture, and validating plans through scenario-based exercises that reflect the complexity of a real grid disruption event.

NERC CIP: What the Standards Require

The NERC CIP standards most relevant to operational resilience and continuity planning are:

- CIP-002 — BES Cyber System Categorization: risk-based categorization into High, Medium, and Low impact levels, which determines the scope of applicable security controls
- CIP-008 — Incident Reporting and Response Planning: cybersecurity incident response plan requirements including identification, categorization, notification to E-ISAC, CISA, and NERC, and response procedures
- CIP-009 — Recovery Plans for BES Cyber Systems: recovery plan requirements for High and Medium impact BES Cyber Systems, including backup and restore procedures and recovery plan testing

- CIP-013 — Supply Chain Risk Management: vendor risk management requirements for hardware, software, and services for BES Cyber Systems
- CIP-014 — Physical Security: physical security assessments for Transmission Stations, Substations, and Primary Control Centers, including risk assessment, corrective action planning, and third-party verification of both the risk assessment and the physical security plan

What these standards do not define is how CIP-compliant programs connect to government emergency management, how incident response integrates with utility emergency operations, or how recovery plans are validated against the realistic complexity of a grid disruption and restoration event.

The ALIGN – NERC CIP Crosswalk

ALIGN PHASE	NERC CIP STANDARD	ALIGNMENT DESCRIPTION
A — Assess Diagnose	CIP-002: BES Cyber System Categorization; CIP-014: Physical Security Threat Assessment	BES asset categorization and physical security assessment ground the ALIGN Assess phase in CIP-002 and CIP-014 requirements, while decision architecture analysis identifies how operational decisions, escalation pathways, and cross-functional coordination actually function during a BES disruption event.
L — Link Coordinate	CIP-008: E-ISAC / CISA / NERC Incident Notification; CIP-013: Supply Chain Vendor Coordination; ESCC / E-ISAC Integration	Mapping incident notification pathways, supply chain coordination, and government emergency management integration applies CIP-008's regulatory notification requirements as functional operational systems, connecting the utility's planning to E-ISAC, CISA, DOE, and state emergency management frameworks.

ALIGN PHASE	NERC CIP STANDARD	ALIGNMENT DESCRIPTION
I — Integrate Build	CIP-008: Incident Response Plans; CIP-009: Recovery Plans for BES Cyber Systems; CIP-014: Physical Security Corrective Action	Operational integration of incident response and recovery plans across BES Cyber Systems, physical security, and utility emergency operations fulfills CIP-008 and CIP-009 plan requirements with operational precision, ensuring recovery plans reflect realistic grid restoration sequencing assumptions.
G — Generate Stress Test	CIP-008: Incident Response Plan Testing; CIP-009: Recovery Plan Testing; NERC GridEx; High-Consequence Event Scenarios	Scenario-based exercises using realistic grid disruption, restoration sequencing, and simultaneous cyber-physical attack scenarios apply CIP-008 and CIP-009 testing requirements with HSEEP-informed, maturity-scored discipline, incorporating GridEx scenarios and government restoration prioritization assumptions.
N — Normalize Sustain	CIP-009: Annual Recovery Plan Review; CIP-010: Configuration Change Management;	CIP compliance monitoring integration, maturity benchmarking, and continuous improvement cadence sustains CIP-008, CIP-

ALIGN PHASE	NERC CIP STANDARD	ALIGNMENT DESCRIPTION
	NERC Compliance Monitoring	009, and CIP-014 program currency across NERC audit cycles while building the cross-functional resilience discipline that compliance monitoring alone does not require.

Where ALIGN Goes Further: Five Critical Infrastructure Differentiators

1. Cross-Functional Operational Decision Architecture

NERC CIP standards address cybersecurity and physical security compliance programs, which often operate in organizational silos from utility emergency operations, customer service, and corporate communications. ALIGN maps the decision architecture across all domains, identifying where coordination will break during a simultaneous cyber-physical incident.

2. IT/OT Convergence in Continuity Planning

Electric utilities operate at the convergence of Information Technology (IT) and Operational Technology (OT) systems. ALIGN's Integrate phase builds recovery plans that function across both domains, connecting BES Cyber System recovery procedures to operational continuity programs for generation dispatch, transmission operations, and distribution restoration.

3. Government Emergency Management Integration

Grid restoration following a major disruption is not a utility-only operation. Federal and state emergency management agencies, DOE, CISA, and the Electricity Subsector Coordinating Council (ESCC) all have roles in prioritizing restoration. ALIGN's Link and Generate Stress phases explicitly incorporate these frameworks.

4. High-Consequence Event Scenario Design

ALIGN's Generate Stress phase designs exercises that reflect the complexity of high-consequence events: simultaneous cyber intrusion and physical attack, extended grid restoration following a natural disaster, and nation-state-level threat scenarios that activate E-ISAC and DOE emergency coordination.

5. Supply Chain and Third-Party Resilience Integration

ALIGN extends CIP-013 into operational continuity planning, mapping how vendor failures, delayed hardware supply chains, and third-party OT service disruptions cascade into operational continuity risk, and building response procedures for supply chain disruption scenarios.

Conclusion

NERC CIP compliance is mandatory for bulk electric system operators and a legitimate starting point for utility cybersecurity and physical security programs. For utilities operating in an environment where threats are sophisticated, infrastructure is interconnected, and grid restoration is a multi-stakeholder operation, compliance is the floor of what resilience requires, not its ceiling.

ALIGN builds the program structure above that floor: connecting CIP programs to government emergency management, integrating IT and OT continuity planning, and validating programs through exercises that reflect the real complexity of a high-consequence grid disruption event. Reliability is the standard CIP defines. Resilience is the capability ALIGN builds.

Sentinel Resilience Partners provides emergency management and resilience consulting for electric utilities and critical infrastructure operators including NERC CIP compliance support, AWIA risk assessment support, black-sky event planning, and HSEEP-aligned exercise programs. ALIGN engagements are structured at four tiers: Audit, Build, Validate, and Sustain.

Paul Corgel

CEO & Principal Consultant, Sentinel Resilience Partners. Project lead on CPG 101 Version 3.0, *Planning Considerations: Putting People First*, and *Private-Public Partnerships Guidance and Tools*. Two decades of national preparedness programs and disaster response operations at FEMA.