GLOBAL DIGITAL FORENSICS

Power OT NERC CIP Scoping Pack

NERC CIP versions, New York and New Jersey utility rules and the evidence to gather before a power OT assessment

Edition 2026-11-03 | November 3, 2026

For security, engineering and compliance teams preparing OT assessment work at generation, transmission and distribution facilities. Use it to confirm the operating boundary, the CIP versions in force and the evidence that already exists before choosing a technical scope.

Fill in the worksheets by hand or copy them into your own records.

Questions about this document: call (800) 868-8189 or write to info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Contents

1. Confirm Entity and System Applicability
2. CIP Versions in Force and Coming
3. Where an Assessment Supports CIP Evidence
4. New York and New Jersey Utility Rules
5. Evidence Checklist
6. Illustrative Finding
7. Assessment Scope Worksheet
8. Corrective Action Worksheet
9. Sources

© 2026 Global Digital Forensics, Inc. All rights reserved.

Confirm Entity and System Applicability

NERC CIP obligations follow the registered entity's functions and the categorization of its BES Cyber Systems under CIP-002, so start with the compliance owner's current categorization. High and medium impact systems carry the full set of applicable requirements; low impact assets fall under CIP-003. Distribution, gas and other energy facilities outside the Bulk Electric System are governed by state rules and contracts instead.

CIP Versions in Force and Coming

Virtualization revisions, FERC Order No. 919

Order No. 919, published March 24, 2026 and effective May 26, 2026, approved CIP-002-7, CIP-003-10, CIP-004-8, CIP-005-8, CIP-006-7.1, CIP-007-7.1, CIP-008-7.1, CIP-009-7.1, CIP-010-5, CIP-011-4.1 and CIP-013-3. Under the NERC implementation plan they become effective on the later of April 1, 2026 or the first day of the first calendar quarter 24 months after the effective date of the order, with optional early adoption. CIP-002-8 and CIP-003-11 were approved in separate concurrent orders. Until the new versions take effect, the currently enforceable versions apply, so record both the version in force on the assessment date and the version the entity is preparing for.

Internal network security monitoring, CIP-015-1

FERC approved CIP-015-1 in Order No. 907, effective September 2, 2025. The standard becomes effective on the first day of the first calendar quarter 36 months after that date, October 1, 2028, for systems at Control Centers and backup Control Centers identified under CIP-002 Requirement R1.1 and R1.2, high and medium impact alike. Medium impact BES Cyber Systems with External Routable Connectivity outside Control Centers follow 24 months later, under the NERC implementation plan. Order No. 907 also directed NERC to extend monitoring to electronic access control and monitoring systems and physical access control systems outside the electronic security perimeter.

Where an Assessment Supports CIP Evidence

An OT assessment produces evidence that maps to specific requirements once applicability is settled: electronic access points and remote access under CIP-005, ports, services and security event monitoring under CIP-007, recovery plans under CIP-009, and configuration baselines and vulnerability assessments under CIP-010. Record each mapping against the requirement and version it supports.

Preserve operating authority

Engineering and operations approve active targets, methods, operating windows, stop conditions and recovery support. Use a laboratory or representative system where production work is unsuitable. Passive collection needs an approved design too, because installing a tap or a mirror port is a change to the network.

© 2026 Global Digital Forensics, Inc. All rights reserved.

New York and New Jersey Utility Rules

New York Public Service Commission

Electric utilities with 50,000 or more service lines fall under the Commission’s utility cybersecurity rules, Part 1200, effective June 1, 2026. Those rules cover information technology rather than OT, require notice of a qualifying incident within 72 hours and call for a first certification by June 30, 2027.

New Jersey Board of Public Utilities

Each public utility reports to the Board within six hours of becoming aware of a cyber attack resulting in outages or service issues, a confirmed breach or intrusion, or an attempted intrusion that slows or disrupts service, under N.J.A.C. 14:3-6.7(a)6 and 7. Keep these state obligations and any contract duties in their own rows beside the NERC evidence.

Evidence Checklist

For each item, name the owner, the record that exists today, its date and what is still missing.

Item	What to gather
Applicability record	The registered functions, BES Cyber System categorization, applicable requirements, the version in force and the compliance owner.
Electronic access	Remote access paths, intermediate systems, electronic access points and dated configuration evidence for the systems in scope.
Account authorization	Vendor approvals, responsible parties, authentication, access limits and revocation evidence.
Monitoring evidence	Session records, access events, time synchronization, retention and the person who reviews and preserves them.
Configuration and vulnerability evidence	Baselines, change records, the assessment method the requirement calls for, and open findings.
Recovery readiness	Configurations, restoration procedures, licensing, spares, vendor dependencies and dated recovery tests, with untested assumptions marked.
Validation authorization	Targets, excluded commands, traffic limits, maintenance windows, stop authority, communications and recovery support.
State reporting	The PSC or BPU reporting contacts and clocks that apply, recorded apart from the NERC evidence.

Illustrative Finding

A fictional example showing how a well documented finding is written.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Observed condition

A vendor support account belongs to an access group whose recorded policy reaches more control zone destinations than the documented support task needs.

Source evidence

Dated access approval, identity group membership, jump host policy and firewall configuration, each tied to the system owner and the date it was reviewed.

Operating consequence

If the account were compromised, an attacker could reach additional assets that support the process. Confirming that path needs an approved reachability check and the engineers' view of the operating dependencies.

Basis of the finding

The finding rests on dated configuration records; an approved reachability check confirms it in the live environment.

Corrective work

The operator assigns an owner to narrow the access to the support task, review revocation and session records, and agree the change with the equipment vendor and engineering team.

Verification

Agree the method, targets, maintenance dependency, stop authority and evidence needed to verify the corrected boundary, and track recommended, implemented and verified states separately.

Assessment Scope Worksheet

Use broad descriptions here and keep sensitive system details in your controlled records.

Operating process and boundary
Operations, engineering and security owners
Applicable program, requirement and evidence owner
Available records, their dates and gaps
Approved passive methods and proposed active validation

© 2026 Global Digital Forensics, Inc. All rights reserved.

Excluded systems, commands and actions

Operating window, stop authority and communications

Recovery arrangements and open dependencies

Corrective Action Worksheet

Record one action per copy, and keep implementation and verification evidence separate.

Finding, evidence reference and operating consequence

Corrective owner, dependency and target date

Status: recommended, implemented or verified, with supporting evidence

Verification method, result and date

Sources

Sources checked November 3, 2026.

Federal Register FERC Order No. 919, Virtualization Reliability Standards, 91 FR (March 24, 2026): https://www.govinfo.gov/content/pkg/FR-2026-03-24/html/2026-05716.htm

Federal Register FERC Order No. 907, CIP-015-1 Internal Network Security Monitoring (July 2, 2025): https://www.govinfo.gov/content/pkg/FR-2025-07-02/html/2025-12309.htm

© 2026 Global Digital Forensics, Inc. All rights reserved.

NERC Project 2023-03 implementation plan for CIP-015-1: https://www.nerc.com/pa/Stand/Project_202303_INSM_DL/2023%2003%20Implementation%20Plan%20clean_Feb2024.pdf

NERC CIP standards: https://www.nerc.com/standards/reliability-standards/cip

New York Public Service Commission Case 25-M-0302, order adopting 16 NYCRR Part 1200 (April 16, 2026), and the announcement: https://dps.ny.gov/node/29056

New Jersey Register 54 N.J.R. 1612 (August 15, 2022), adopted amendments to N.J.A.C. 14:3-6.7, published by the Office of Administrative Law

NIST SP 800-82 Revision 3, Guide to Operational Technology Security: https://csrc.nist.gov/pubs/sp/800/82/r3/final

© 2026 Global Digital Forensics, Inc. All rights reserved.

Talk to a Senior OT Assessor

Global Digital Forensics plans power OT assessments with the operations and engineering owners around physical safety and the real architecture, and maps the findings to the CIP requirements and versions the compliance lead must answer. On the first call we review this checklist with your engineers and agree what can be examined safely.

Get a free consultation. The initial consultation is free, and requests are handled in confidence.

Call (800) 868-8189 at any hour, or write to info@evestigate.com.

Request a consultation online at evestigate.com/contact.

© 2026 Global Digital Forensics, Inc. All rights reserved.