FRAMEWORK MAPPING

NERC CIP (Critical Infrastructure Protection)

Publisher. NERC

Control mappings. 22 controls

Statement date. 2026-08-03

Critical Infrastructure Protection standards for Bulk Electric System operators. Etch addresses CIP-007 systems security management and CIP-011 information protection through signed evidence trails and BYOK HSM attestation.

Control mapping

Every row names a specific control from the framework and describes how Etch addresses it. The response prose commits to what Etch signs on the chain, not to runtime enforcement. Etch is an evidence layer.

Control ref	Control name	How Etch addresses it
`CIP-002-5.1a R1`	BES Cyber System identification	Each project on Etch is a distinct BES Cyber System scope. Cross project federation is possible but not required.
`CIP-003-8 R1`	Security management controls	Bounded authority receipt records policy assignments. Signed dissent captures second line of defense disagreement.
`CIP-004-6 R2`	Cyber security training	Training completion signed via authority receipt with identity, scope, and expiration binds the training record to the specific individual and time window.
`CIP-004-6 R4`	Access management program	Token scopes segregate mcp:read, mcp:write, admin:project. Token issuance and revocation are chain signed via the admin API.

Control ref	Control name	How Etch addresses it
`CIP-005-6 R1`	Electronic security perimeter	Internal service traffic on 127.0.0.1 loopback only. All external traffic terminates at TLS 1.2 or higher.
`CIP-006-6 R1`	Physical security plan	Physical security posture depends on the hosting provider or BYOK HSM. HSM attestation endpoint accepts tpm2, yubikey, aws-nitro, gcp-shielded, azure-attestation, sev-snp, intel-tdx.
`CIP-007-6 R1`	Ports and services	Public port surface documented and minimized. Internal service traffic on 127.0.0.1 only.
`CIP-007-6 R2`	Security patch management	Every code release is Sigstore attested through PyPI Trusted Publishing. pip audit runs on every CI build. SBOM available under NDA.
`CIP-007-6 R3`	Malicious code prevention	No binary uploads accepted. No customer code executed. Chain append is a pure data path validated by Pydantic.
`CIP-007-6 R4`	Security event monitoring	Every event chain signed. Ingest adapter accepts OTel GenAI, LangSmith, CloudTrail, Vercel AI, and custom formats. Retention is hot cold split.
`CIP-007-6 R5`	System access control	Token scopes segregate access. HSM attestation lets the operator bring its own hardware anchor for signing keys.
`CIP-008-6 R1`	Cyber security incident response plan	Signed postmortem event records incident retrospective with signer identity, corrective action, and optional retroactive confidence downgrade.
`CIP-008-6 R2`	Incident response plan implementation	Explicit stop condition endpoint records incident response halts. The verifier flags post halt writes.
`CIP-009-6 R1`	Recovery plans	Chain data replicates to a hot standby in a second AZ. Recovery point objective under 15 minutes.

Control ref	Control name	How Etch addresses it
`CIP-009-6 R2`	Recovery plan testing	The adversarial benchmark repository tests tamper detection continuously. Recovery integrity verifiable against pinned public keys.
`CIP-010-3 R1`	Configuration change management	Every deploy snapshots each customer chain byte identical before and asserts unchanged after. Change management guarantee has held across every deploy of the current build.
`CIP-010-3 R2`	Configuration monitoring	The offline verifier walks chain state and reports on 11 check categories. Configuration drift is detectable.
`CIP-011-2 R1`	Information protection	Chain payload commits hashes not raw content. KMS encrypted signing keys. HSM attested BYOK deployments for BES relevant workloads.
`CIP-011-2 R2`	BES Cyber System Information reuse	SQL layer append only triggers prevent silent reuse or overwrite. Any UPDATE or DELETE attempt raises the trigger.
`CIP-013-2 R1`	Supply chain risk management	Sigstore attested releases. Cross chain federation records upstream and downstream third party chain references. Supply chain evidence is walkable across boundaries.
`CIP-013-2 R2`	Supply chain risk management plan implementation	Signed release attestation via PyPI Trusted Publishing. pip audit on every CI build.
`CIP-014-2 R1`	Physical security of transmission stations	Physical layer depends on the hosting provider or BYOK HSM. HSM attestation binds signing to hardware.