CIP-003-9 · ATTACHMENT 1, SECTION 6

CIP SENTRY

Section 6 readiness checklist

Vendor electronic remote access at assets containing low impact BES Cyber Systems. Enforceable since April 1, 2026.

DOES SECTION 6 APPLY TO YOU?

Yes, if any asset containing low impact BES Cyber Systems **allows vendor electronic remote access** that you permit under Section 3.1. Your low impact cyber security plan then needs a process with **at least one method each to determine, disable and detect** that access. You don't need a list of low impact BES Cyber Systems, but you do need to know where vendor access exists.

START WITH SCOPE

- [ ] For each low impact asset (or group of like assets), note **whether vendors have remote access and by what path:** VPN, remote desktop, vendor portal or remote-control tool, cellular modem.
- [ ] Confirm each path is one you permit under **Section 3.1** (only necessary inbound and outbound access).
- [ ] Name **who owns the process** at each site.

SECTION 6.1
Determine

Can you show when a vendor has remote access, and that you know it's in use?

- [ ] The plan names your **method(s) for determining** vendor electronic remote access.
- [ ] One method chosen for each access path.
- [ ] A dated record you could show an auditor today.

NERC'S EVIDENCE EXAMPLES

Steps to preauthorize access; alerts on vendor log-on; session monitoring or recording; time-of-need session initiation; security information management alerts; system logs.

SECTION 6.2
Disable

Can you cut vendor access quickly, and does everyone know who can?

- [ ] The plan names your **method(s) for disabling** vendor electronic remote access.
- [ ] Who can disable it at each site, **including after hours.**
- [ ] Good practice: try it once and keep the record.

NERC'S EVIDENCE EXAMPLES

Disabling vendor accounts; disabling ports, services or permissions on the firewall, VPN, remote desktop or remote-control tools; disabling the protocols the access uses; removing physical connectivity; written steps listing the methods.

SECTION 6.3
Detect

What would catch known or suspected malicious traffic on vendor sessions, both ways?

- [ ] The plan names your **method(s) for detecting** known or suspected inbound and outbound malicious communications.
- [ ] Who reviews the alerts or logs, and how often. Write it down, then follow it.

NERC'S EVIDENCE EXAMPLES

Anti-malware; intrusion detection or prevention (IDS/IPS); automated or manual log reviews; alerting.

BEFORE YOUR NEXT AUDIT

- [ ] Your low impact cyber security policy covers vendor electronic remote access security controls (**R1.2.6**) and has CIP Senior Manager approval from the last 15 calendar months.
- [ ] Evidence is **dated and filed by section** (6.1, 6.2, 6.3) for each asset or group of assets.
- [ ] The documented low impact cyber security plan (**R2**) has language for 6.1, 6.2 and 6.3.
- [ ] When a vendor access path is added or removed, **the plan and the evidence are updated.**

CIP Sentry keeps the low impact plan, Section 6 evidence and review dates in one place, on your own server.

cipsentry.com · (888) 678-1898

Based on NERC Reliability Standard CIP-003-9: Requirement R1.2.6, Requirement R2, Attachment 1 Section 6 and Attachment 2 (examples of evidence). A planning aid, not legal advice; your Regional Entity's audit approach governs. CIP Sentry is independent software, not affiliated with or endorsed by NERC, FERC or any Regional Entity.