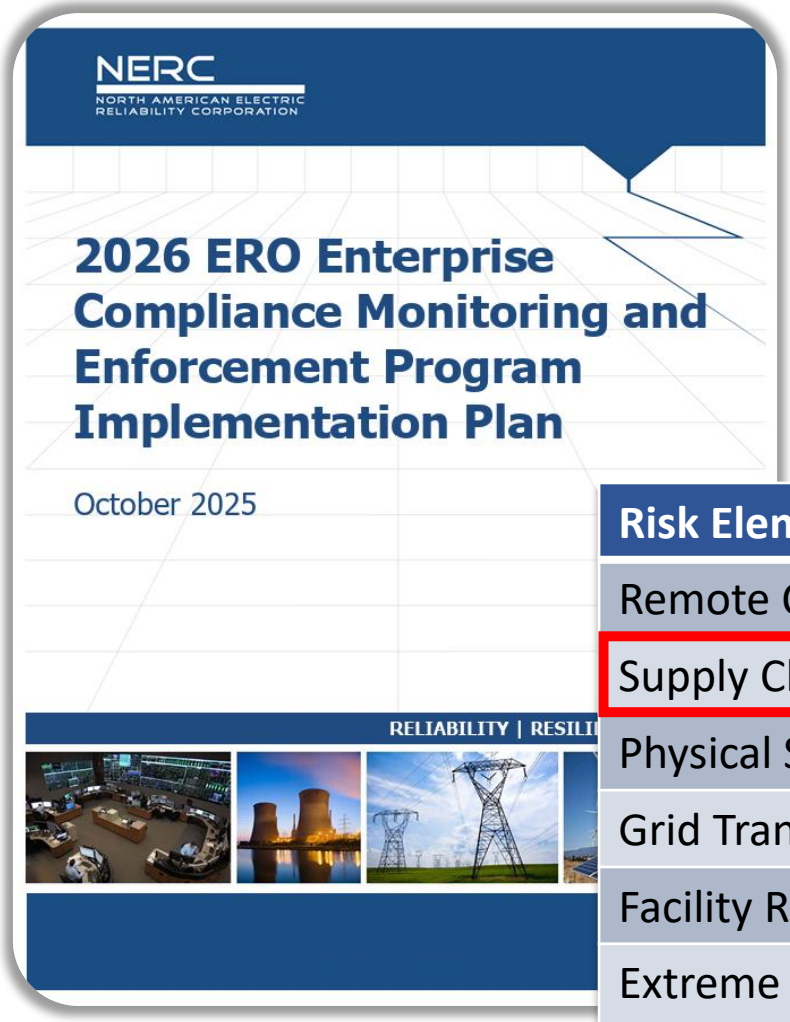
TEXAS RE

CIP-007-6 R2
Security Patch Management

Kerrick Rosemond, Jr.
CIP Cyber & Physical Security Analyst

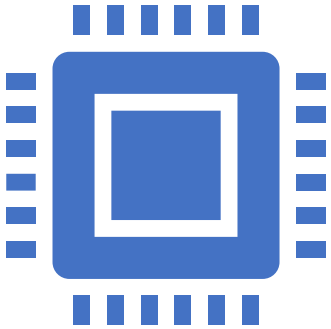
February 6, 2026

Risk Focus & CMEP IP Risk Factors



Risk Elements
Remote Connectivity
Supply Chain
Physical Security
Grid Transformation
Facility Ratings
Extreme Weather Response

CIP-007-6 Table R2 – Security Patch Management



2.1 A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.

Considerations

- Does your process language include detailed instructions?
- How is compliance documentation stored?
- Does your process include controls to track applicable Cyber Assets?

Best Practices and Internal Controls

- Framework for patch management process
- Regularly reviewing and updating documentation
- Management tools
- List of monitored sources

CIP-007-6 Table R2 – Security Patch Management

2.2 At least once every 35 calendar days, evaluate security patches for applicability that have been released **since the last evaluation** from the source or sources identified in Part 2.1.

Considerations

- Release notes
- Controls in place for requirement deadlines
- Methods to verify the evaluation completion date

Best Practice and Internal Controls

- Reminders & alerts
- Peer reviews
- Tools that logs evaluation dates automatically

CIP-007-6 Table R2 – Security Patch Management

2.3 For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:

Apply the applicable patches

Create a dated mitigation plan

Revise an existing mitigation plan

Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.

Considerations

- How do you verify the installation date of patches?
- Are there controls in place to verify the patch was installed?
- Does your mitigation plan address the vulnerabilities?
- How does this apply to other standards?

Best Practices and Internal Controls

- Real-time updates and change management system
- Peer reviews

CIP-007-6 Table R2 – Security Patch Management

2.4 For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP senior manager or delegate.

Considerations

- How are mitigation plan deadlines tracked?
- How is implementation evidence of mitigation plans stored?

Best Practices and Internal Controls

- Tools to visualize timelines and progress
- Secure platform for documents related to mitigation plans
- Workflow that requires CIP senior manager or delegate approval with time constraints

TEXAS RE
Ensuring electric reliability for Texans