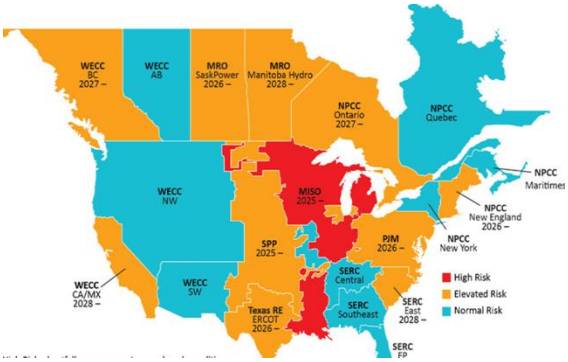
CASE STUDY 490

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

"MITIGATE CYBER-SECURITY BREACHES AND SUPPLY CHAIN RISKS BY IMPLEMENTING PROVENANCE BEST PRACTICES"



ABOUT THE CLIENT	
Industry	**Energy**
Revenue	**$100 million**
Employees	**200**
Location	**Atlanta, Georgia, U.S**
BSI Service or Solution	**Risk Management**

Key Challenges

- Hardware and software components with unverified provenance posed risks of counterfeiting.
- Lack of chain-of-custody documentation made it difficult to track changes or identify malicious actors.
- Risks from insiders, nation-states, and cybercriminals exploiting gaps in procurement and maintenance processes.
- Existing standards required stronger implementation guidance to address threats.

Why Boston Strategies was Selected

- Proven track record in developing provenance frameworks aligned with NIST, ISO, and FERC guidelines.
- Deep understanding of CIP-013 and NERC compliance requirements.
- Ability to integrate physical and logical controls into a unified strategy.
- Experience working with utilities, vendors, and federal agencies to standardize best practices.

Project Scope

- Drafting guidelines for provenance management across planning, development, installation, maintenance, and disposal.
- Establishing contract language to mandate SBOMs, multi-factor authentication, and patch verification.
- Implementing controls like denied-party screening, secure development environments, and trusted communication paths.
- Creating resources for NERC members to operationalize the framework.

Project Approach

- Mapped provenance risks across the BPS lifecycle (Table 1.1 from NERC guidelines).
- Adapted NIST IR 7622, ISO 20243, and CIP-013 recommendations into actionable steps.
- Tested controls with utilities and vendors, focusing on high-risk areas (e.g., patch management).
- Expanded the framework to all NERC regions, supported by training and metrics for continuous improvement.

Operational Benefits Realized

- Achieved 100% SBOM adoption among critical vendors, improving traceability.
- Denied-party screening prevented contracts with 15+ high-risk entities.
- Cryptographic patch verification eliminated malware incidents from updates.

Financial Benefits Realized

- Reduced incidents of counterfeit components, saving an estimated $2M+ in potential breach remediation.
- Streamlined adherence to CIP-013, avoiding penalties and audit findings.