



- [Solutions](#)
- [Products](#)
- [Industries](#)
- [Customers](#)
- [Partners](#)
- [Support](#)
- [Company](#)
- [Contact Us](#)



**[Solutions](#)**

**[Security & Log Management](#)**

**[Compliance Auditing](#)**

- [PCI DSS](#)
- [HIPAA](#)
- [Sarbanes-Oxley](#)
- [NISPOM](#)
- [FISMA](#)
- [DCID](#)
- [NERC](#)**
- [ISO 27002](#)

**[IT Operations & Risk Management](#)**

**[Business Data Intelligence](#)**

Federal Energy Regulatory Commission (FERC)/North American Electric Reliability Corporation (NERC) compliance is a requirement for all bulk power electricity providers in North America. NERC is a self-regulatory body charged with ensuring industry compliance with Critical Infrastructure Protection (CIP) standards that require organizations that deliver bulk electricity to the North American electrical grid to identify and protect critical cyber assets. FERC oversees the power industry, but gives NERC the responsibility for maintaining and complying with CIP.

Organizations affected by FERC/NERC must define methods, processes, and procedures for securing those systems determined to be critical cyber assets, as well as the non-critical cyber assets within the electronic security perimeter. "Cyber assets" are loosely defined as all "programmable electronic devices and communication networks including hardware, software, and data."

- Compliance with FERC/NERC requires:
  - Create and maintain a cyber security policy
  - Maintain documentation of the security perimeter, all interconnected cyber assets, and all electronic access points
  - Identify and implement electronic access controls for access to critical cyber assets within the electronic security perimeter, maintain documentation of the electronic access controls, and update that documentation at least annually
  - Continuously monitor electronic access to critical cyber assets
  - Protect information associated with critical cyber assets, plus policies and practices used to keep them secure
  - Establish system management policies and procedures for configuring and securing critical cyber assets
  - Define and document electronic incident response actions, including roles and responsibilities assigned by individual or job function.

SenSage solutions for security and compliance enable organizations affected by FERC/NERC compliance to continuously monitor access to cyber assets protect information and audit for asset configuration changes.

**Resources**

**Gartner**

[Gartner 2009 SIEM Magic Quadrant](#)

**Brochures**

[NERC](#)

**» Contact Us**