

## SECUREWORKS ALIGNMENT WITH NERC CIP REQUIREMENTS

The North American Electric Reliability Corporation (NERC) is a nonprofit corporation designed to "ensure that the bulk electric system in North America is reliable, adequate and secure." All bulk power system owners and operators are required to register with NERC through the appropriate regional entity, and users must comply with approved NERC reliability standards, including the Cyber Security Standards CIP-002 through CIP-009, effective June 1, 2006.

SecureWorks has extensive experience partnering with utility providers and we can help you improve your security and compliance posture while reducing costs. As described below, many of our Managed Security Services and Professional Services align directly with the NERC CIP Standards, allowing you to easily meet and exceed the requirements they set forth.

NERC Category	Standard #	Requirement	Professional Services	Managed Security Services
Auditing and Risk Assessment of Critical Assets	CIP-002	All network assets must be audited to identify Critical Cyber Assets. An Electronic Security Perimeter should be erected around these critical assets to provide protection. A risk-based assessment methodology should be utilized with annual reviews.	> Security Assessment > CIP Gap Analysis	> Managed Firewall > Managed NIPS/NIDS
IT Policy Creation and Control	CIP-003	Policies with adherence monitoring and change control must be documented and in place.	> Security Assessment > CIP Gap Analysis	> Security Monitoring > Security Information Management
Change Control Management	CIP-003	Change Control policies and processes must be documented and adhered to.		
Critical Cyber Security Controls	CIP-003	Definitions and documentation on access control levels for critical assets such as Internet facing systems and critical backend solutions. Solutions should be in place to mitigate risks.	> Security Assessment > CIP Gap Analysis	> Managed Firewall > Managed NIPS/NIDS > Security Monitoring > Security Information Management
Security Awareness	CIP-004	Employees should be trained on policies, access controls and general awareness issues around Social Engineering.	> Security Assessment > CIP Gap Analysis	
Employee Background Checks	CIP-004	Background checks should be performed on all users with access to computer assets.		
Electronic Security Protection	CIP-005	An Electronic Security Perimeter should be established that provides the following: <ul style="list-style-type: none"> <li>• Disable Ports and Services that are not required</li> <li>• Monitor and Log Access 24x7x365</li> <li>• Perform Annual Vulnerability Assessments (at a minimum)</li> <li>• Documentation of Network Changes</li> </ul>	> Security Assessment > CIP Gap Analysis	> Managed Firewall > Managed NIPS/NIDS > Security Monitoring > Security Information Management > Vulnerability Scanning
Physical Security Program	CIP-006	Physical Security controls should be documented and implemented that provide perimeter monitoring and logging along with robust access controls. All cyber assets used for Physical Security are considered Critical and should be treated as such.  Critical assets require perimeter protection, auditing, and monitoring. (CIP-002 & CIP-003)	> Security Assessment > CIP Gap Analysis	> Managed Firewall > Managed NIPS/NIDS > Security Monitoring > Security Information Management > Vulnerability Scanning
Systems Security Management	CIP-007	All methods, processes and procedures for securing Critical Assets and all technology solutions should be well-defined and include automated controls. System and network events should be monitored automatically with alerts sent to key personnel.  An annual vulnerability assessment should be performed.	> Security Assessment > CIP Gap Analysis	> Managed Firewall > Managed NIPS/NIDS > Security Monitoring > Security Information Management > Vulnerability Scanning
Incident Response and Reporting	CIP-008	All cyber security incidents should be addressed by an internal computer incident response team (CIRT) and reported to the ES ISAC.	> Security Assessment > CIP Gap Analysis	> Managed Firewall > Managed NIPS/NIDS > Vulnerability Scanning
Disaster Recovery	CIP-009	A disaster recovery plan should be created and tested with annual drills.	> Security Assessment > CIP Gap Analysis	