



Overview

This document provides an overview of the Critical Infrastructure Protection (CIP) portion of the North American Electric Reliability Council (NERC) Reliability Standards and clarifies Redspin's role as an objective, third-party security partner.

Background

The CIP Reliability Standards are often referred to as the NERC Cyber Security Standards. They are divided into eight specific areas (CIP-002 through CIP-009). For more information on NERC and the full set of the NERC Reliability Standards, please visit www.nerc.com.

These standards require certain users, owners, and operators of the Bulk Power System to comply with specific requirements to safeguard Critical Cyber Assets. Critical Cyber Assets are defined as programmable electronic devices and communication networks including hardware, software, and data that are essential to the reliable operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Power System.

Redspin's Role

Redspin works with our client-partners to provide a risk-based gap analysis of their compliance with the NERC Cyber Standards and also to perform the specific Cyber Vulnerability Assessments required in CIP-005 and CIP-007.

Redspin's role as a trusted security adviser is to responsibly interpret the often general

requirements, help balance remedy-mitigation-and risk tradeoffs, and focus partner resources on the most critical tasks to meet security and compliance standards. Redspin helps protect critical infrastructure by providing objective guidance and the technical expertise to enable our partners to make the most informed risk management decisions.

CIP Reliability Standards

The NERC Cyber Security Standards mirror established standards in the financial sector, healthcare sector, and the organizations encompassed by the payment card industry. As with the best industry standards, the Cyber Security Standards recognize that compliance is not an episodic or one-time event – it is an ongoing process.

There are eight specific standards that must be addressed. Each standard has multiple requirements ranging from two requirements in CIP-008 (Incident Reporting and Response Management) to nine requirements in CIP-007 (Systems Security Management).

Many requirements have sub-requirements that help clarify and specify the scope or process that is acceptable.

NERC developed an Implementation Plan which outlined a three-year phase-in for all Responsible Entities to achieve full compliance with all requirements. For the most part, all covered entities were to be compliant by 2nd Quarter 2009 and are to be *Auditably Compliant* by 2nd Quarter 2010. *Auditably Compliant* primarily refers to the state of having 12-calendar-months of auditable data and documentation.



Roadmap to Cyber Security Compliance

As proven by more mature compliance standards in other industries, establishing and following a risk management framework is the most cost-effective approach to securing Critical Cyber Assets: 1) Identifying the Risks, 2) Implementing Controls / Mitigating the Risks, and 3) Maintaining Acceptable Risk Levels Through Evaluation and Monitoring.

Cyber Security Lifecycle



Essentially, the NERC Cyber Security Standards sequentially leads each Responsible Entity through this process. A quick review of each standard reveals the careful construction of this time-tested approach:

1 Identifying the Risks
CIP-002 – Critical Cyber Asset Identification Requires a risk-based assessment methodology to be identified and documented and then employed to identify and list all Critical Assets and further identify and list the Critical Cyber Assets among these.
CIP-003 – Security Management Controls Requires the creation of a Cyber Security Policy and the identification of a single senior manager with overall responsibility and authority for leading and managing the implementation and adherence to these standards including the establishment of information protection, access control, and a change control and configuration management system.
2 Implementing Controls / Mitigating the Risks
CIP-004 – Personnel & Training Requires training and awareness of all personnel with access to Critical Cyber Assets including personnel risk assessments (identify verification and criminal check).
CIP-005 – Electronic Security Perimeters Requires the placement of every Critical Cyber Asset within a defined Electronic Security Perimeter and the identification of all access points to these assets, including monitoring and active testing of the access points.
CIP-006 – Physical Security of Critical Cyber Assets Requires the establishment and maintenance of a physical security plan including logging physical access to Critical Cyber Assets.
CIP-007 – System Security Management Requires the creation of methods, processes, and procedures which secure all Cyber Assets (critical and non-critical) within the Security Perimeter. This covers ports and services, patch management, malicious software, account management, asset disposal, event monitoring, and active testing for vulnerabilities.
3 Maintaining Acceptable Risk Levels Through Evaluation and Monitoring
CIP-008 – Incident Reporting and Response Planning Requires the identification, classification, response plan, and reporting plan of all cyber security incidents.
CIP-009 – Recovery Plans for Critical Cyber Assets Requires the establishment and testing of recovery plans for Critical Cyber Assets.

About Redspin, Inc.

Redspin delivers the highest quality information security assessments through technical expertise, business acumen and objectivity. Redspin customers include leading companies in areas such as healthcare, financial services, hotels, casinos and resorts as well as retailers and technology providers. Some of the largest communications providers and commercial banks rely upon Redspin to provide an effective technical solution tailored to their business context, allowing them to reduce risk, maintain compliance and increase the value of their business unit and IT portfolios.

WEB
WWW.REDSPIN.COM

PHONE
800-721-9177

EMAIL
INFO@REDSPIN.COM

WHEN YOU REALLY WANT TO KNOW...CALL REDSPIN.