REDSEAL

NORTH AMERICAN ELECTRICAL UTILITIES

NERC CIP VERSION 5 COMPLIANCE BEGINS WITH REDSEAL

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

BACKGROUND

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards define a comprehensive set of requirements that are the basis for maintaining the reliability of the North American Bulk Electric System (BES) and protecting it from cyber-attacks. However, NERC Registered Entities struggle to define security best practices and controls that will easily meet the standards. The entities are finding different ways to balance compliance risks with operational or security risk.

NERC Sanction Guidelines include penalties of up to $1 million per day per violation - which is the highest financial penalty of any regulatory framework in North America. Also, the NERC CIP Standards continue to evolve, as do the interpretations as to what constitutes acceptable control activities under the standard. Deploying the correct controls and tools are the keys to sustaining NERC compliance beyond just the current interpretation of the standard and into the future as the regulatory model for electric utilities continues to mature.

While all requirements within the NERC CIP Framework cannot be addressed by any single vendor, RedSeal provides strong support in the areas of network architecture, testing, device inventory, and simulation. RedSeal's strengths map directly to NERC-specific controls as well as controls associated with other security frameworks such as NIST 800-53.

REDSEAL AND FEDERAL GOVERNMENT CYBERSECURITY

RedSeal has a history of support for federal government cybersecurity initiatives. The company's innovative software solution is installed in numerous Department of Defense, intelligence, and civilian organizations for the purpose of continuous monitoring. At the highest level, RedSeal delivers three core security controls:

HIGHLIGHTS

- NERC CIP Version 5 introduces new requirements for Electronic Security Perimeters (ESP), malicious code mitigation, and more
- Penalties for non-compliance range up to $1M per day
- RedSeal delivers simplified compliance with key CIP Version 5 controls:
    - Continuous validation of the ESP for mixed vendor environments
    - Malicious code mitigation via least privilege network access
    - Vulnerability remediation prioritization based on actual risk
    - Change simulation
- RedSeal's proven scalability supports the largest networks with low staff overhead

- Visibility: Automated network mapping and situational awareness
- Verification: Continuous comparison of network security architecture against desired posture
- Prioritization: Analysis of vulnerability scan data and network architecture to identify the highest risk vulnerabilities that must be remediated immediately

These controls have now been largely incorporated into the NERC CIP framework.

These controls apply to both existing deployments and new architectures. In existing deployments, RedSeal allows you to understand your existing environment and quickly identify security control gaps. In new architectures, RedSeal validates that the network is built and operated as designed. And in all situations, RedSeal vastly increases the value of scanning and penetration testing by prioritizing those vulnerabilities that are the most dangerous cybersecurity threats.

REDSEAL SUPPORT FOR NERC CIP CONTROLS

RedSeal's cybersecurity capabilities closely align with many of the controls in NERC CIP. RedSeal supports a total of 17 controls within four of the individual NERC CIP Version 5 Standards. RedSeal provides strongest support for CIP-005-5, which requires BES Cyber Systems to be protected within a defined Electronic Security Perimeter (ESP). RedSeal supports ESP and intermediate system architecture design and validation, all components of CIP-005-5.

Details of RedSeal's NERC CIP Version 5 support can be found in the appendix to this document. At a high level, RedSeal supports NERC CIP control areas as follows:

NERC CIP CONTROL AREA	REDSEAL
Electronic Security Perimeter and intermediate system validation	✓
Device inventory and network map	✓
Least privilege network access validation for malicious code mitigation	✓
Vulnerability remediation prioritization	✓
Change simulation	✓
Configuration baseline and hardening	✓

With RedSeal, NERC Registered Entities can significantly reduce the cost associated with enforcing compliance with NERC CIP by automating assessment of many of the NERC CIP controls. Certain controls have traditionally been very difficult to automate, and therefore resource intensive to maintain and audit. However, RedSeal's unique technology can automate and prioritize these troublesome controls, greatly decreasing resource requirements while actually improving the quality of the control. For example:

- Electronic Security Perimeter: Internal and external network isolation based on router ACLs and firewall rules is a fundamental control in NERC CIP and in many other compliance regimens. But testing the control at scale is a massive task, especially in multi-vendor environments. Many thousands of rules on hundreds of devices may be deployed to create just one isolated domain, and analyzing these against a security policy is a huge effort with lots of potential for error. RedSeal not only automates this analysis in preparation for an audit; it also continuously monitors the control and provides daily reporting on control integrity. This significantly improves threat defense posture while not requiring additional personnel or technical resources.

- Configuration Management/Vulnerability Assessments: Comprehensive vulnerability and penetration testing involves a combination of automated and manual procedures. A typical pen testing control activity calls for re-testing when there is any change to the controls being tested (e.g. perimeter defenses). When this scales to a large environment where a large number of changes are taking place, blanket manual processes are no longer realistic. RedSeal lets you focus the pen testing on the boundaries most likely to be affected by a change and with the highest risk potential.

  With respect to Configuration Management, RedSeal automatically analyzes devices for compliance with baseline configurations. The system includes over 100 out-of-the-box configuration checks for firewalls, routers, load balancers, and wireless controllers. Examples of configuration checks include password policies, services enabled, logical port configuration, and networking parameters. Custom checks are also easily defined. In addition to enforcing baseline configurations, the solution makes it easy to detect deviations from baseline that may be acceptable, but require authorization. It can also identify access (firewall and ACL) configuration changes that could impact the Electronic Security Perimeter.

- Vulnerability Scanning: All vulnerability scanning control activities are implemented for the purpose of identifying and remediating vulnerabilities; identifying the vulnerabilities is just the start of the process. But like pen testing, vulnerability scanning doesn't scale easily and can get expensive quickly. You need to

determine where to launch scans and toward which targets. And when you find vulnerabilities by the hundreds, you need to determine which ones to resolve first. RedSeal rationalizes vulnerability scanning by combining scan results with its analysis of exploitation potential. This has two benefits: the most dangerous vulnerabilities are identified and can be corrected first, and the scanning effort can be tailored to focus in the areas where risk is highest.

SUMMARY

As NERC CIP Version 5 compliance becomes mandatory, utilities need to invest in systems that allow them to meet the standard with the lowest operational overhead. RedSeal's unique ability to analyze large scale, multi-vendor networks and evaluate them against a target security architecture makes reaching that goal much easier. By replacing labor intensive manual analysis with automation, organizations can become CIP Version 5 compliant on a continuous basis, simultaneously improving security and lowering costs.

REDSEAL

REDSEAL SUPPORT FOR NERC CIP VERSION 5 CONTROLS

PART	REQUIREMENTS	REDSEAL SUPPORT
CIP-002-5.1: BES Cyber System Categorization		
1.1 & 1.2	Identify each of the high and medium impact BES Cyber Systems according to Attachment 1, Section 1.	RedSeal creates and maintains an inventory of EACMS in-scope devices. Also provides inventory of in-scope subnets, which informs potential scope of devices.
2.1	Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1.	Continuous inventory of EACMS in-scope devices and ESP subnets to facilitate review
CIP-005-5: Electronic Security Perimeter		
1.1	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	Automated creation and maintenance of network map, which documents architecture of electronic security perimeter and interior topology and subnets. RedSeal evaluation and continuous monitoring of access paths validates routable paths into and within the ESP
1.2	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	RedSeal continuously calculates all access paths between the ESP and any external device. Any path that does not pass through an EAP is immediately identified.
1.3	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	RedSeal performs regular comparisons of actual access permissions with CIP ESP access control requirements. Any policy violation or unapproved additional access is immediately identified.
2.1	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Comparison of actual network architecture with CIP ESP access control requirements. Validation of intermediate system requirement for remote access: ensure that remote access connections only terminate on Intermediate Systems. Immediate identification of policy violation if direct remote access is permitted to any system within the ESP.
2.2	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	Network access path policy validation at the logical port level to ensure that only encrypted ports are accessible on the intermediate system.

CIP-007-5: Systems Security Management		
1.1	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Continuous evaluation of actual EACMS system configurations versus policy to ensure only authorized logical port services are enabled. Validation of EACMS ACL and firewall rules to ensure that only authorized logical ports are accessible.
1.2	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	Continuous evaluation of actual EACMS system configurations versus policy to ensure only authorized physical ports are enabled.
3.1	Deploy method(s) to deter, detect, or prevent malicious code.	Support for development and implementation of least privilege network access to minimize ability of malicious code to deploy and propagate. Crucially, this control can be deployed within the ESP, to degrade the ability of malware to spread within the environment.
CIP-010-1: Configuration Change Management and Vulnerability Assessments		
1.1	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Creation of baseline configuration policy for multi-vendor network environment, in particular EACMS systems. Continuous evaluation of actual EACMS system configurations versus policy to ensure only authorized services and ports are enabled.
1.2	Authorize and document changes that deviate from the existing baseline configuration.	Continuous reporting and documentation of any deviation from approved baseline configuration policy.
1.4	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	Verification of CIP-005 controls: Following any change from the baseline configuration policy, the solution validates that CIP-005 controls for ESP and ESP access have not been adversely affected.

5	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	What-if analysis of proposed configuration effects on cyber controls: Proposed changes to access policy (FW/ACL/load balancing configurations) are evaluated in a test RedSeal environment to ensure that CIP-005 and CIP-007 controls are not adversely affected, and if so exactly what the degradation is.
2.1	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	Continuous reporting and documentation of any deviation from approved baseline configuration.
3.4	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Prioritization of remediation based on actual threat level created by vulnerabilities. This prioritization drives the creation of the action plan to both simplify that creation and to maximize its effectiveness.