

# VULNERABILITY AND POLICY MANAGEMENT FOR NERC COMPLIANCE

## **NERC Defined**

NERC Standards are a U.S. regulation managing the Critical Cyber Assets of Bulk Electric Systems. CIP-002 through CIP-009 provides a cyber security framework for the identification and protection of these assets, and supports reliable operation of the Bulk Electric System. In other words, vulnerabilities of these assets can be reduced. Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets, supporting critical reliability functions and processes, to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets. These Critical Assets are to be identified through the application of a risk-based assessment.

## **Asset and Vulnerability Identification are part of the NERC Process**

Asset identification and vulnerability assessment are critical parts of the NERC regulations. Upon creation of the cyber security framework, it becomes crucial to then identify all assets that manage Bulk Electric Systems and to support reliable operations that would warrant vulnerability identification and remediation. CIP-002 through CIP-009 communicates the guiding principles for secure technology choices – principles that are provided by Qualys' on-demand risk and vulnerability management service, QualysGuard.

## **QualysGuard Meets Key NERC Compliance Rules**

The QualysGuard vulnerability management and policy compliance solution meets key security technology auditing requirements detailed in the North American Electric Reliability Council charter, adopted June 1st, 2006 (see back page for details). QualysGuard fulfills key Administrative Safeguards for asset identification, evaluation, security management, security incident procedures, training, and security assurance requirements of NERC.

## **Automation Makes Compliance Easier and Cost Effective**

As an on demand web service, QualysGuard enables immediate compliance with NERC Critical Cyber Asset identification regulations by allowing subscribers to automatically discover and manage all devices and applications on the network, identify and remediate network security vulnerabilities, measure and manage overall security exposure and risk, and ensure compliance with internal and external policies for NERC.

QualysGuard’s capabilities directly address many key Administrative Safeguards. The following matrix quotes NERC Critical Cyber Identification standards and implementation specifications of CIP-002 through CIP-009, and associates each with QualysGuard capabilities.

NERC Requirements	QualysGuard Capabilities
<p><b>CIP- 002 Critical Cyber Asset Identification</b> – Identify and document a risk-based assessment method that will be used to identify critical assets. R2 requires an identifiable list and annual asset list review to update all critical cyber assets. Management will approve the list of critical cyber assets. A third-party, without vested interest, shall monitor the compliance to CIP – 002 outcome of NERC.</p>	<p>On demand risk assessment with QualysGuard’s Vulnerability Manager automatically fulfill the Cyber Asset Identification requirement of NERC by discovering all assets on the critical network and documenting security vulnerabilities for remediation (R2 and R3). Management is given the opportunity to review and approve the assets and assessments with either the vulnerability or policy compliance modules (R4). Qualys becomes the third party with no vested interest.</p>
<p><b>CIP- 003 Cyber Security Management Controls</b> – “The responsible entity shall document and implement cyber security policy that represents management’s commitment and ability to secure critical assets. Exceptions to cyber security policy must include an explanation and approval.</p>	<p>QualysGuard’s Policy Compliance has the technical controls for the cyber assets, along with the datapoints or policies for those technical assets, and management’s ability to add their own company or technical policies. Additionally, the exceptions, approvals and denials are documented by QualysGuard (R3).</p>
<p><b>CIP- 005 Cyber Electronic Security Perimeter(s)</b> – Requires the identification and protection of the Electronic Security Perimeter(s) and Access Points where Cyber Assets reside (R1 and R4).</p>	<p>QualysGuard automatically fulfills the requirement to identify by discovery and protect by means of Vulnerability Manager, the Cyber Assets and Electronic Security devices, including Access Points. QualysGuard uses the largest database of vulnerability tests and intelligent scanning technology to ensure comprehensiveness and accuracy.</p>
<p><b>CIP- 007 Cyber Systems Security Management</b> – Define methods, processes and procedures for securing those systems determined to be Critical Cyber Assets (R1 and R3)”. “Document technical and procedural controls to enforce authentication, accountability and user activity (R5)”. Finally, a third party annual review is required of the perimeter (R8).</p>	<p>Automated, comprehensive reports from QualysGuard provide instant assessment of risks, priorities and tips for vulnerability remediation. Policy Compliance includes the guidelines provided by vendors and best practice or adopted frameworks. Additionally security patch management information is passed on to the user/assessor. Policy Compliance also includes controls for authentication and account management. Qualys becomes the third party annual reviewer.</p>
<p><b>CIP- 008 Cyber Security Incident Reporting and Response Planning</b> – “...ensure the identification, classification, response and reporting of Cyber Incidents”.</p>	<p>QualysGuard automatically documents all security incidents and subsequent effects of vulnerability remediation. Security audit assessments provided by QualysGuard provide hard data for conceiving, implementing and managing security incidents.</p>
<p><b>CIP- 009 Cyber Security Recovery Plans for Critical Cyber Assets</b> – Compliance monitoring must in affect as well as data retention, of auditability of records for three years.</p>	<p>QualysGuard Policy Compliance provides the customization for adding multiple compliance’ for monitoring and retention is managed by business owner.</p>



**USA – Qualys, Inc.**  
 1600 Bridge Parkway  
 Redwood Shores  
 CA 94065  
 T: 1 (650) 801 6100  
 sales@qualys.com

**UK – Qualys, Ltd.**  
 224 Berwick Avenue  
 Slough, Berkshire  
 SL1 4QT  
 T: +44 (0) 1753 872101

**Germany – Qualys GmbH**  
 München Airport  
 Terminalstrasse Mitte 18  
 85356 München  
 T: +49 (0) 89 97007 146

**France – Qualys Technologies**  
 Maison de la Défense  
 7 Place de la Défense  
 92400 Courbevoie  
 T: +33 (0) 1 41 97 35 70

