Securing Your Critical Infrastructure

NERC CIP Cyber Vulnerability Assessment

- GATHER NERC CIP PROGRAM DOCUMENTATION
  Gather all documented data concerning the Access Points, Cyber Assets, Critical Cyber Assets, including ports/services, acocunts, community strings, and diagrams.
- ASSESS THE CURRENT NERC CIP ENVIRONMENT
  Gather all current configuration data concerning the Access Points, Cyber Assets, Critical Cyber Assets, including ports/services, acocunts, community strings, and diagrams.
- COMPARE THE DOCUMENTED ENVIRONMENT TO THE CURRENT ENVIROMENT
  Compare the documented and current environments and determine any gaps.
- DOCUMENT FINDINGS & PROVIDE ACTION PLAN
  Document results of the Cyber Vulnerability Assesmsent and provide a document/spreadsheet with the identified issues as the initial action plan.

relay SECURITY GROUP

Service Offering

Details

Relay Security Group (Relay) is owned and operated by information security professionals that previously led Symantec Corporation's Power and Energy Consulting practice. With over twenty years of cumulative IT security experience, Relay has worked in a wide range of markets. In addition to a strong general understanding of IT security, Relay consultants have over ten years of penetration testing and vulnerability assessment experience, as well as nine years of experience performing evaluations of utilities' corporate and SCADA environments and in conducting NERC CIP Gap analyses.

Relay's NERC CIP Cyber Vulnerability Assessment services are based on a proven methodology that focuses on understanding a client's unique environment and assessing the procedural and technical areas of the standard to meet the Cyber Vulnerability Assessment requirements outlined for NERC CIP-005 R4, CIP-007 R8, CIP-005 R1.5, CIP-006 R2.2. The following table details tasks that may be conducted to review the Electronic Security Perimeter (ESP) and to review the Cyber Assets and Critical Cyber Assets within the ESP as well as the electronic and physical security access control and monitoring solutions:

Task	Requirement
Conduct analysis of all data and create a report that includes the vulnerability assessment methodology, as well as findings, recommendations, and an action plan to address identified issues.	R4.1 & R8.1 A document identifying the vulnerability assessment process. R4.5 & R8.4 Documentation of the results of the assessment, the action plan(s) to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan(s).
Gather ports and service, as well as account information for each access point. If necessary, conduct additional manual (review configuration file) or automated tests to verify the configuration of default accounts, passwords, and SNMP community strings. Then compare the results to the existing documentation.	R4.2 A review to verify that only ports and services required for operations at these access points are enabled. R4.4 A review of controls for default accounts, passwords, and network management community strings.
Review existing documentation, to include diagrams and configuration files for the network devices that make up the ESP and interview staff to gain clearer picture of the environment. Conduct a site walk through and wireless site survey to verify the ESP and PSP boundary. If necessary, conduct a review of dial-up configuration files to ensure they are meeting authentication requirements. If required, conduct a war-dialing effort.	R4.3 The discovery of all access points to the ESP.
Gather port and service, as well as account information from each Cyber Asset and Critical Cyber Asset within the ESP. If necessary conduct additional manual/automated tests to verify the configuration of ports/services and default accounts and passwords. Then compare the results to the existing documentation.	R8.2 A review to verify that only ports and services required for operations of the Cyber Assets within the Electronic Security Perimeter are enabled. R8.3 A review of controls for default accounts

Note: Where appropriate, these same processes would be used to review the CIP-005 R1.5 and CIP 6 R2.2 identified solutions.

3750 Brodie Way Dublin California 94568 ☎ 800.613.0431 ✉ sales@relaysecurity.com WWW.RELAYSECURITY.COM