

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

Vulnerability Assessment Requirements

1. **Introduction.** Vulnerability assessment testing is required for all access points into an electronic security perimeter (ESP), all cyber assets within the ESP, and all cyber assets that authorize and/or log access to the Physical Security Perimeter(s) (PSPs), exclusive of hardware at the Physical Perimeter access point such as electronic lock control mechanisms and badge readers.
2. **Requirements.** The following table lists the minimum requirements defined in CIP-005, R4 and CIP-007,. Reclamation requirements for conducting the vulnerability assessments are outlined thereafter.

ESP Access Point Vulnerability Testing Requirements (CIP-005)	Cyber Assets within the ESP Vulnerability Testing Requirements (CIP-007)
R4.1: Vulnerability assessment process documented.	R8.1: Vulnerability assessment process documented.
R4.2: Verify the minimal ports and services for each Access Point into the ESP	R8.2: Verify the minimal ports and services for each cyber asset within the ESP.
R4.3: Discovery of all access points into the ESP	N/A
R4.4: Review of controls for default accounts, passwords, and network management community strings.	R8.3: Review of controls for default accounts.
R4.5: Assessment results documented, remediation or mitigation plans developed, tracking and execution of the mitigation or remediation plans.	R8.4: Assessment results documented, remediation or mitigation plans developed, tracking and execution of the mitigation or remediation plans.

A. **Vulnerability Assessment Process.** The assessment process must be documented and identified as a NERC CIP-005, Electronic Security Perimeter or a CIP-007, Systems Security Management Vulnerability Assessment Plan. The minimum required documentation includes:

- (1) dates of the assessment;
- (2) named individual or individuals conducting the assessment;
- (3) scope of the assessments (supported by “current” network diagrams, ESP, Critical Cyber Assets (CCA), and Critical Asset (CA) Inventories)
- (4) description of the testing environment (test system, sub-system, or operational system); and

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- (5) assessment or test procedures for each requirement (see the appropriate paragraphs below).

B. Verification of Ports and Services. The vulnerability assessment will verify that a process to identify the minimal ports and services associated with all CCAs, CAs, and ESP access points has been conducted and documented. The verification will include a review of the process or testing conducted to identify the minimal ports and services, as well as, a review and analysis of any compensating measures applied to mitigate risk exposure, where technical limitations did not permit certain ports or services to be disabled. Technical feasibility exceptions (TFE's) for devices that do not permit disabling of unused ports and service must be reviewed.

- (1) In addition to the review and analysis above, the vulnerability assessment for ports and services must include:
- (a) Automated port scans (using Nmap, Nessus, or equivalent tools) of each cyber asset identified as in scope. Note: Automated scans of ESP access point devices must be conducted against internal and external (i.e., protected and unprotected) interfaces. While various operating systems include domain, workgroup, and system tools that can be used to validate and report on enabled services and ports, these tools are internal to the systems and cannot be used to validate system configuration. These tools are good for configuration management, change control, and they do provide a capability of monitoring unauthorized configuration changes. For the purposes of testing enabled ports and services, tools that are independent of the system internals and present an external view must be used to validate system configuration changes.
 - (b) Where automated scans are not possible, manual reviews of running services must include observations of cyber assets where ports and services are identified.
 - (c) A comparison and analysis of the automated port scan or manual review results with the desired configuration settings of each included cyber asset.
- (2) All efforts shall be afforded to conduct the assessment, including port scans, to minimize any potential negative impact on operational systems. The testing of operational systems must be conducted when the CCAs, CAs, and ESP access point devices are NOT in control of an operational CA (i.e., during a scheduled

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

outage, etc.) to avoid system failures. Such testing must be documented in the vulnerability assessment plan and coordinated with the CA plant or facility manager.

- (3) When utilizing NMAP, Nessus, or equivalent tools, procedures shall be established to ensure that only non-intrusive port scans are conducted. The procedure must include an observation by the local system administrator or information system security officer (ISSO) to ensure that the tool settings are enabled to execute port verification testing only. The vulnerability testing must not be executed without a complete and thorough review of all testing conducted as part of the configuration baseline determinations. System administrators and/or ISSO must review proposed assessment procedures prior to any scanning activities to identify any known, documented, or potential negative impacts or disruptive events that have resulted from prior scanning activities.

C. Discovery of Access Points into the ESP. Verification of all entry points into an ESP is a process that must be verified through a number of various activities such as: port scanning, observation of configuration settings, physical port reviews on network devices (i.e., tracing cables on switches, etc.), hardware and network inventories, and network traffic analysis. Each of these activities must be used to identify known or unknown access points.

- (1) The following list, while not complete, provides a recommended starting point in developing a plan for access point discovery. There are two phases embedded within this list: validation of existing access points and discovery of unknown access points.
 - (a) Verify network diagrams, ESP inventories, flow control documentation, or other relevant documents to identify all previously identified access points.
 - (b) Review configuration setting for all cyber assets within the ESP to ensure that unnecessary ports or services are disabled for external access.
 - (c) Network discovery tools must be used to validate known and unknown devices that exist within an ESP boundary (examples include NMAP for IP networks and SNMP discovery tools such as Solar Winds).
 - (d) Passive vulnerability and network analysis tools such as Wireshark and CACE Pilot (developed by CACE Technologies) may be used to identify unknown broadcasts and transmission control protocol or user datagram protocol traffic originating from unknown hosts.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

- (e) Conduct hardware inspections of all ESP network layer devices and all cyber assets within the ESP to identify all connected ports (e.g., serial, Ethernet, or wireless). These inspections will identify unknown communication channels.
 - (f) 802.11 Wireless Local Area Network or WiFi scanning with spectrum analysis will be utilized to identify unknown wireless communication channels within an ESP.
- (2) After a review of the existing access points, inventories, and configuration settings identified in the steps above, formal access point verification and discovery test plan must be documented, together with the obtained approvals for testing.

D. Review of Default Accounts. NERC CIP-003, R6, Configuration Management and CIP-007, R5, Account Management, if implemented properly, must inventory all application, system, and accounts, including any generic or default accounts. However, a requirement for review of default accounts extends beyond those known and documented. Reviewing accounts as part of a vulnerability assessment also includes the discovery of any “unknown” application, system, or user accounts as well. A review of default accounts also includes the verification that all “default” account names and passwords have been changed, and that procedures (as controls) for implementing, maintaining, and deleting accounts are consistent with CIP-007, R5.2 (R5.2.1 – R5.2.3). The following table summarizes the minimal activities associated with reviewing default accounts:

Requirements	Activities
Controls for all generic or default accounts are documented and implemented accordingly.	<ul style="list-style-type: none"> • Identify documented procedures and review for consistency with the requirements in CIP-007, R5.2.
Generic and default accounts included within Configuration Management and Chance Control processes (see CIP-003, R6).	<ul style="list-style-type: none"> • Review all documented accounts (originally generic or default). • Conduct a discovery activity of all default accounts within hardware, software, and firmware. (Review hardware and application manuals or system documentation, and observe the actual account as it exists within the hardware, software, or firmware.)
Default accounts names and passwords have been changed according to the CIP-007, R3 (where technically feasible).	<ul style="list-style-type: none"> • Develop a list of all default accounts, including the name and password, compare the default account names with those actually implemented.

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

Requirements	Activities
	<ul style="list-style-type: none"> • Test by observed log-on attempts using the default account names and passwords for each hardware device, application software, operating system (embedded or installed), and any firmware access. • For the ESP access point devices, default account testing also includes community string account names. For PLCs, default account includes those accessed for configuration purposes typically associated with a direct serial interface and those accessible by other protocols (telnet, http, or snmp).
Document testing activities and results.	<ul style="list-style-type: none"> • Document the type of test (observation, review, test) and results (compliant or non-compliant), and identify any non-compliance justification pursuant to a TFE or supported by a Mitigation Plan.

3. Glossary of Terms:

- A. **Access Controls.** Technical, operational, or management security controls, put in place at access points to reduce the risk that unauthorized access (either logical or physical) can be gained to cyber assets protected by the access controls.
- B. **Access Point.** A communications mechanism (port or communication line), exposed at the boundary of an ESP that provides logical access to cyber assets within the ESP.
- C. **CA.** Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BES. Specific Reclamation assets have been identified as critical based on the criteria and procedures established by Reclamation Manual, IRM TRMR-10-1, Appendix A, *Critical Asset Identification Methodology: Pursuant to NERC Critical Infrastructure Protection (CIP) Standards*.
- D. **CCA.** Cyber assets, including programmable electronic devices, communication networks, hardware, software, and data that are essential to the reliable operation of CAs.
- E. **ESP.** An ESP is the logical border surrounding a network to which CCAs are connected and for which access is controlled. All cyber assets and components internal

Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2013)

to the ESP boundary, as well as, all cyber assets and components which reside on the ESP boundary are subject to the security requirements of this D&S, its companion D&S, and overarching policy.

- F. **Ports and Services.** The set of enabled ports and service used to transfer data based on a particular digital communications protocol (for example TCP/IP).
- G. **Security Vulnerability Assessment.** A systematic approach to identifying weaknesses in the logical protections that have been put in place.
- H. **Reliability Standards.** Any number of NERC or Western Electricity Coordinating Council Standards, the specific requirements of which are applicable to Reclamation, and which defines tasks, procedures or conditions for maintaining the reliability of the BES. For purposes of this D&S, the specific Reliability Standards of concern include Standards CIP-002 through CIP-009, inclusive. Although CIP-001 is identifiable as a CIP Reliability Standard, it does not specifically address the security of CCAs and is identified as outside the scope of this D&S. As used throughout this D&S, Standards CIP-002 through CIP-009 will be referred to collectively as the NERC CIP Reliability Standards.
- I. **TFE.** An exception from strict compliance with the terms of an applicable NERC CIP requirement on the grounds of technical feasibility or technical limitation. For more information see *NERC Compliance Process Bulletin #2009-007*.