Standard CIP-007-1

-- Cyber Security --
System Security
Disclaimer

This NPCC TFIST workshop provides a forum for the presentation and discussion of member experience in the implementation of compliance programs for the NERC CIP Cyber Security Standards. Materials presented or discussed are the presenters’ own interpretation and recommendations and do not necessarily represent those of their organizations or NPCC.
CIP-007 Purpose

Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s).

***Note: Requirements apply to ALL Cyber Assets within the ESP(s).***
Summary of Requirements

R1 - Test Procedures
R2 – Ports and Services
R3 – Security Patch Management
R4 – Malicious Software Prevention
R5 – Account Management
R6 – Security Status Monitoring
R7 – Disposal or redeployment
R8 – Cyber Vulnerability Assessment
R9 – Documentation Review and Maintenance
Standard Requirements

- **R1 – Test Procedures** — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
Requirement R1 – Test Procedures

- Establish a test environment and testing procedures.
  - Minimize effects on production system and operation
  - Environment reflects the production environment
  - How each major component is to be tested
  - How test results are documented
  - Integrate into change management procedures
    - Reference to CIP-003 R6

May 15, 2008
Standard Requirements

- R2 – Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
Requirement R2 – Ports and Services

- Port discovery
  - Off-line or on-line?

- Enable only ports and services required for operation
  - How do we know?

- Technically infeasible to disable unused ports
  - Compensating measure: Perimeter firewall?

May 15, 2008
Standard Requirements

- R3 – Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
Requirement R3 – Security Patch Management

- Leverage the existing IT processes
  - Security vulnerability and patch monitoring
    - Use your vendors
    - Consider adding in new contracts
  - Patch evaluation process – within 30 days
  - Document implementation or why applicable patches are not installed
    - Compensating measures: e.g. block vulnerable services at ingress points to the ESP (firewall?), automatic with a deny by default posture?

May 15, 2008
R4 – Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
Requirement R4 – Malicious Software Prevention

- Beware: countermeasures can be deadly...
- Platform Issues
  - Windows
    - How often do you update? (They can be daily)
    - How do you test?
    - Automatic? (NO...)
  - *NIXes
    - Is there such a thing as a *NIX virus?
    - Trojans, root kits more common
    - File integrity tools: practical? Safe?
- Proprietary Platforms: technical feasibility
- Mitigations: Perimeter based defenses

May 15, 2008
R5 – Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
Requirement R5 – Account Management

- Not all systems have individual accounts
- Not all that do have role based authorization
- Required approval process
- Logging by account: keep for 90 days
- Annual review of access privileges
- Remove/disable/rename administrative, maintenance/service accounts
- Document and track shared/generic accounts
  - Eliminate or minimize
  - Have a process for personnel transfer or termination
- Password requirements are basic
  - But not always technically feasible...

May 15, 2008
R6 – Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
Requirement R6 – Security Status Monitoring

- Not all systems have security logging (or even any logging)
  - How large are they: practical considerations
  - Must keep for 90 days
- How do you implement alerting?
  - Log consolidation
    - Proprietary formats?
  - Rule based alerting – automated log review?
  - Use a commercial product
- Security events related to incidents
  - Ensure you include in incident handling procedures
  - Keep for 3 years

May 15, 2008
R7 – Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
Requirement R7 – Disposal or Redeployment

- **Disposal**
  - When equipment is salvaged
  - No data sanitization standard cited
  - Software wiping, non-destructive: 3-7 passes
  - Degaussing, destructive
    - Environmental considerations

- **Redeployment**
  - Data sanitization procedures, even between ESPs
  - Software wipe only option
  - Do not try manage internal or external non-destructive sanitization

- **Maintain Records!!!**
R8 – Cyber Vulnerability Assessment
— The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually.
Requirement R8 – Cyber Vulnerability Assessment

- Use tools and scripts if you can – use non-disruptive (passive) options
- Test on test/training systems first!!!
- Proceed cautiously!!!
  - Consider passive options on critical live systems
- Document the assessment process
- Document review of results
- Document mitigation plan and execution

May 15, 2008
R9 – Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.
Requirement R9 – Documentation Review and Maintenance

- The usual stuff
  - Annual review of all documents
  - Changes to be documented within 90 days
    - Integrate in your change management procedures

May 15, 2008