CIP-007 Compliance

Kevin B. Perry
Dir, Critical Infrastructure Protection
kperry@spp.org · 501.614.3251
Agenda

- CIP-007 Purpose
- CIP-007 Requirement Overview
- Past Non-Compliance
- Potential Non-Compliance Concerns
CIP-007 Purpose

- **Systems Security Management**
  - **Purpose**: Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.
CIP-007 Requirement Overview

• Systems Security Management
  – Nine 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 – Document Review and Maintenance
Past Non-Compliance

• 2009 – 2010: CIP spot checks
  – Requirement R1
    ▪ Included in 13-requirement CIP spot check
    ▪ R1: Did not test security controls
    ▪ R1.3: Did not maintain documentation of testing
    ▪ R1: Wandering laptop
  – Requirement R5
    ▪ Spot check expansion for cause
    ▪ R5.2.3: Did not secure shared user accounts when user retired, resigned, or transferred
    ▪ R5.3.3: Did not change passwords at least annually
Potential Non-Compliance Concerns

• CIP-007-3 Overall
  – Include ALL Cyber Assets in Electronic Security Perimeter
  – Include ALL physical and electronic access control and monitoring systems
  – TFE Applicability
    ▪ R2.3 (cannot disable ports and services)
    ▪ R3.2 (cannot implement security patch)
    ▪ R4 (cannot install anti-virus/anti-malware)
    ▪ R5.3; R5.3.1; R5.3.2; R5.3.3 (password management)
    ▪ R6; R6.3 (cannot log or monitor security events)
Potential Non-Compliance Concerns

- R1 – Test Procedures
  - Test:
    - Operating system patches and service packs
    - Application software changes
    - Database management system changes
    - Firmware updates
  - Test security configuration (system hardening) parameters
  - Demonstrate testing was conducted (test results)
  - New and existing Cyber Assets
Potential Non-Compliance Concerns

• R2 – Ports and Services
  – Document ports and services needed for normal and emergency operations
    ▪ Focus on well known ports and services
    ▪ Focus on “established” and “listening” ports
    ▪ Document both TCP and UDP ports
    ▪ Be able to explain what the port or service is used for
  – Disable ports and services not required
  – Request a TFE and implement compensating measures when ports/services cannot be disabled
Potential Non-Compliance Concerns

• R3 – Security Patch Management
  – Pay attention to all installed software and firmware
    ▪ Know what is running on your Cyber Assets
    ▪ Subscribe to notification services
    ▪ Subscribe to vendor support
  – Review for applicability within 30 days of availability
  – Implement or request a TFE
    ▪ Implement compensating measures until patch or update can be installed
    ▪ Request a TFE if patch cannot be installed
Potential Non-Compliance Concerns

• R4 – Malicious Software Prevention
  – More than just anti-virus
  – Not just at the perimeter
  – Black list or White list – both have advantages and disadvantages
  – Be creative – look for ways to protect your systems
  – Request a TFE and implement compensating measures if anti-malware cannot be installed
Potential Non-Compliance Concerns

- R5 – Account Management
  - Manage all of your user accounts
    - Don’t forget operating system user accounts
    - Don’t forget local user accounts in an AD environment
    - Have a defined authorization process and documentation
  - Log access
  - Change the shared user account password when user list changes
  - Enable complexity enforcement whenever possible
  - Request a TFE when you cannot enforce full CIP compliance
Potential Non-Compliance Concerns

• R6 – Security Status Monitoring
  – Use remote Syslog when possible
  – Consider implementing a Security Information and Event Management (SIEM) tool
  – Don’t forget application logs
  – Act on alerts
  – Make sure you are keeping logs for at least 90 days
  – Make sure you can capture logs for 3-year retention
  – Request a TFE if you cannot monitor or log events
Potential Non-Compliance Concerns

• R7 – Disposal or Redeployment
  – You must eradicate data before disposal
    ▪ Deleting files does not eradicate data
    ▪ What if the disk drive has failed?
    ▪ Warranty returns may be an issue
  – You must erase data before redeployment
    ▪ Once again, deleting files is not the same
  – Don’t forget non-disk media
    ▪ Physical destruction may be your only option
  – Keep records
Potential Non-Compliance Concerns

• R8 – Cyber Vulnerability Assessment
  – Must document the annual process
  – Must, at a minimum:
    ▪ Review open ports and services
    ▪ Review controls for default accounts
  – Consider a scanning tool
    ▪ Be wary of scanning a production network
  – Document the results
  – Action plan for any identified vulnerabilities
  – Execute the plan and maintain execution status
Potential Non-Compliance Concerns

• R9 – Document Review and Maintenance
  – Test procedures
  – Process to verify only required ports and services open
  – Security patch management program
  – Anti-malware tools and test/implementation procedures
  – Account management procedures and controls
  – Security event monitoring procedures
  – Disposal/redeployment procedures
  – Vulnerability assessment process
Resources

• Review the CIP Audit Evidence Request and Inventory Workbooks
  – One workbook for each standard
  – Documents the types of evidence expected to demonstrate compliance
  – Posted on the SPP RE web site: [SPP.org > Regional Entity > Compliance & Enforcement](http://SPP.org) current year Compliance folder on left

• System Configuration Benchmarks
  – Look at the [Center for Internet Security benchmarks](http://Center for Internet Security benchmarks)
CIP Compliance Team

• Kevin B. Perry
  Director, Critical Infrastructure Protection
  Kperry.re@spp.org - (501) 614-3251

• Shon Austin
  Senior Compliance Specialist – CIP
  Saustin.re@spp.org - (501) 614-3273

• Leesa Oakes
  Compliance Specialist II – CIP
  Loakes.re@spp.org - (501) 614-3274