Scope

- Compliance Assessment Summary
  - Introspection & Analysis

- Program-In Review
  - Maturity Model review
  - Control Design review
  - Process Components of an effective Program

- Version Impact - Perspective
CIP007 R3 Assessment-Summary

- Assessment of available security patches not completed within 30 days.
- Third-party security patches not assessed for applicability.
- Security patches not assessed for all in-scope Cyber Assets.
- Documentation of security patch assessment not retained.
- Security patch not installed and no compensating measures documented and/or implemented.
CIP007 R3 Assessment - Summary

Source of Discovery

- 50% of CIP007 R3 are self reported

Annual Trend

- 2010: 4 Possible violation
- 2011: 6 Possible violation
- 2012: 6 Possible violation

Limited TFE
Patch Management Program

Assessment

Maturity Model - Classification & Review
- Level 1 - Initial
- Level 2 - Repeatable
- Level 3 - Defined
- Level 4 - Managed
- Level 5 - Optimizing

CCA Risk Profile - Determinants
- Purpose of asset role
- Hosted applications & Selection of infrastructure
- Hardening process
Control Requirement-CIP007 R3

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement 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).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
Patch Management Program

Control Design Criteria - Document and Implement

- **Tracking**
  - Develop inventory to be tracked
  - Tracking - What, How, When & Why
  - Identify source, release date, evaluation date, testing date, install date and mitigation date.

- **Evaluation of applicability - Document assessment of applicability within 30 days.**
  - What and how of evaluation
  - Against tracked vulnerabilities/risk profile criteria
  - Impact on current hardening profile
Patch Management Program

Control Design Criteria - Document and Implement

- Test - Document testing in support of cyber security controls(s)
  - Identify security controls impacted
  - Develop test plans to test security controls
  - Retention of testing records

- Install - If patch is assessed as applicable and you are not able to install or have not installed then implement and document mitigation controls.
Perspective- Version Impact

- Version 4- No Impact to Security Patch management.
- Version 5:
  - Tracking shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches [R3]
  - At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified [3.1]
  - Creation of a new or update of an existing mitigation plan- Plan to address mitigation and time to implement. Version recognizes the inherent risk of patching posed on the integrity and availability of the system(s) [3.2]
  - Plan must be implemented within the timeframe specified in the plan, or in a revised plan as approved by the CIP Senior Manager or delegate [R3.2]
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).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.
Malicious Software Prevention

Strategies & Trend

- **Signature based**
  - Known threats
  - Fast efficient
  - Ineffective to zero-day
  - Targeted malware

- **Non-Signature based**
  - I don’t know who you are but I know your behavior
  - Slow & Expensive- Work offline to identify
  - Effective for zero-day
  - False positives
Malicious Software Prevention

**Sandboxing**
- Suspect file is evaluated in virtual safe environment
- Not extrapolating pattern, only reviewing behavior.
- It is not real time - file is sent to AMA for analysis
- Ineffective as primary - delayed execution

**Challenges**
- Traditional signature based is extremely useful but limited to known signatures and behavior.
- Behavior analysis in tandem with signature based is still ineffective.
- Isolation is not bullet proof
- Advanced malware - Sandbox by itself is not effective
- IPS - By itself is not effective
Malicious Software Prevention

Options - Layered approach

- More specific and defined approaching data
  - Signature based
  - Reputation approach
  - Anomaly detection
  - Offline tools-

- Higher inspection capacity of the appliance the greater the effectiveness of successive tool.
  - Effectiveness vs Efficiency
  - Firewall - Restricted permit and encrypted file review
  - IPS instead of IDS - encrypted file review & traffic over run

- Real time
  - Signature based
  - File reputation
  - File anomaly

- Advanced malware appliance - 2% impact
  - with the exception of encrypted file
CIP007 R4-Assessment Summary

- Anti-virus management console not monitored by staff for virus alerts.
- Anti-virus signature files not tested before update applied.
- Anti-virus/anti-malware not implemented and no TFE requested.
- Anti-virus software installed but found not operational on Cyber Asset.
CIP007 R4-Assessment Summary

Source of Discovery
• 64% of CIP007 R3 are self reported

Annual Trend
• 2010: 3 Possible violation
• 2011: 4 Possible violation
• 2012: 4 Possible violation

TFE: 63 TFE asserted
Malicious Software Prevention

Control Design Review - Document and Implement

- Use of Anti-Virus & other malicious tool evaluation
  - Evaluate the device risk profile
  - Review your toolset option of a single or multiple tools to protect the devices

- Detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware
  - Review your toolset option.
Malicious Software Prevention

Control Design Criteria - Document and Implement

- Document and Apply compensating measures
  - Assess traffic and communication path
  - Review conflict with IPS and Firewall rules
  - Network based appliance on switches
  - Assert TFE

- Document & Implement – Process for updating signature files
  - Process to include testing & installation
  - Review of signature update
**Perspective - Version Impact**

- **Version 4 - No Impact to Malicious Software Prevention Requirement.**

- **Version 5:**
  - transitions to from R4 to R3
  - Holistic less prescriptive- competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.
  - The use of, “Deploy method(s) to deter, detect, **or** prevent malicious code” is less prescriptive but does put the burden on the method to deter, detect or prevent.
Compliance & Beyond

Good vulnerability prevention program include:

- Develop relationship with vendors & subscribe to vendor updates, blogs and admin groups.
- Governance structure - Change Control Board & Change control program adoption
- Define and implement patch cycle
- Documentation to support - Track, Assess, Test, Schedule, Implement and Mitigate
- Configuration management plan
- Assess impact on related CIP & 693
Compliance & Beyond

- Backup & Recovery
- Incident Response Plan
- Disaster Recovery Plan
- Periodically assess the effectiveness of hardening criteria.
- Effective use of tool set.

- Monitor vulnerabilities
  - US CERT quarterly report of known vulnerability
  - NIST National Vulnerability Database
  - Other vendor based sites
Reference Materials

“A Strategic Approach to Protecting SCADA and Process Control Systems,” IBM Global Services


