TRANS Standard Programs and Processes	**Security Patch Management for Control Centers and Telecom Assets**	**TRANS-SPP-12.006** **Rev. 0000** **Page 1 of 9**
		Validation Date XX-XX- Review Frequency 2 years Validated By John D. Tracy
		Effective Date 04-01-2016

Responsible Executive Organization: Transmission & Power Supply

Approved by: _____ _____

Jacinda B. Woodward, Senior Vice President, Transmission & Power Supply

Date

Revision Log

Revision or Change Number	Effective Date	Affected Page Numbers	Description of Revision/Change
0000	04/01/2016	All	Initial issue.

Table of Contents

1.0 PURPOSE

This document establishes the Transmission & Power Supply (TPS) Security Patch Management Program which includes the process for tracking, evaluating, and installing cyber security patches. This program is aligned with TVA-SPP-12.004 TVA *Cyber Security Patch and Vulnerability Management Program*, and the North American Electric Reliability Corporation (NERC) Cyber Security Standard CIP-007-5 Systems Security Management R2 *Security Patch Management* [C1].

2.0 SCOPE

This document is applicable to cyber assets that are managed, maintained, and supported by Transmission Operations & Power Supply (TOPS) and Telecom & Control Systems (TCS). This includes cyber assets that are subject to TVA's Federal Information System Management Act (FISMA) Program and NERC Critical Infrastructure Protection (CIP) Cyber Security Standards.

Review Cadence: This document will be reviewed every two years.

3.0 PROCESS

3.1 Roles and Responsibilities

3.1.1 Senior Vice President of Transmission and Power Supply (TPS)

The SVP TPS is the owner of this SPP and responsible for oversight of patch management activities of assets owned and/or managed by TPS Strategic Business Units (SBUs). The TPS Senior Vice President is responsible for the governance and oversight for this procedure.

3.1.2 Telecommunications Control Systems (TCS)

TCS is responsible for assets that are under their management and support; including providing patch source information for security patches, assessment of patches for applicability based on TVA's specific configuration, and security implications; administering security patches and authoring mitigation plans, and providing artifacts of remediation or mitigation for medium impact BES Cyber Systems. TCS is responsible for the execution and support functions for this procedure.

3.1.3 TOPS Central Operations & Infrastructure

TOPS CO&I is responsible for assets that are under their management and support; including providing patch source information for security patches, assessment of patches for applicability based on TVA's specific configuration, and security implications; administering security patches and authoring mitigation plans, and providing artifacts of remediation or mitigation for high impact BES Cyber Systems.

TOPS CO&I is responsible for maintaining the patch management process, maintaining a patch information database, discovering patches, communicating patch availability to relevant Subject Matter Experts (SME), and providing reporting of program performance. TOPS CO&I is responsible for the oversight, execution, and support for this procedure.

3.1.4 Patch Intake Coordinator (PIC)

The PIC maintains the list of sources tracked for cyber security patches [C1] and checks those sources for new security patches at least once every 35 days [C2]. Upon the receipt of patch availability, the PIC validates whether the patch has security implications, and where applicable creates Patch Availability Notices (PAN) in Security Patch Manager (SPM), and tracks evaluation by appropriate technical SME. The PIC is responsible for the execution and support functions for this procedure.

3.1.5 Subject Matter Expert (SME)

The SME is a relevant technical resource (i.e. desktop, server, TCS Engineering Specialist, or network admin) who provides evaluation as to the applicability of a given patch to the environment or specific system configuration. For applicable patches the SME provides the decision whether to remediate the vulnerability or initiate mitigation activities [C3].

The SME is responsible for initiating relevant change management activities for remediation activities and has the execution and support functions for this procedure.

3.1.6 SME Supervisor

The SME's immediate supervisor is the delegated approver of mitigation plans and must receive and sign-off on all mitigation decisions, and is the designated owner of any mitigation plan. [C4].

The SME Supervisor has execution and support functions for this procedure.

3.2 Program Elements

3.2.1 Patch Management Process

The patch management process is the system of record for intake, evaluation, and disposition of remediation and/or mitigation activities for vendor provided security patches. A visual representation of the process is provided in Appendix A: Patch Management Process Overview".

A. Patch Discovery & Intake

At least once every 35 days, the PIC will check the documented patch sources for newly available security patches [C1]. Upon discovery of a new patch, the PIC creates a Patch Availability Notification (PAN) containing the following information:

- Vendor (patch source)
- Date patch released
- Date of patch discovery
- Target Platform(s) to which the patch applies (eg Windows Server 2012, Red Hat Enterprise Linux 6, etc)
- Vendor Patch ID (eg MS16-001, RHSA-2016:0001, etc)

3.2.1 Patch Management Process (continued)

- Technical details provided by patch source
- Due date for evaluation completion (calculated as "Date patch released" plus 35 calendar days) [C2]

B. Patch Evaluation for Applicability

The PAN is then submitted to SBU specific SME(s) via an e-mail notification. Within the threshold specified by the "Due date for evaluation completion," the SME will provide a technical analysis of the PAN to determine if the patch is applicable to the environment and the specific system configurations in use [C2]. The date of evaluation will be recorded.

C. Remediation or Mitigation

Within 35 calendar days of the evaluation completion, Remediation actions will be complete, or a Mitigation plan will be created/revised [C3]. The SME will document whether the patch is to be addressed via Remediation or Mitigation.

If Remediation is utilized to address a PAN, specific configuration management & change control activities will be documented in the SBU's Change Management processes. Change Management ticket(s) will be recorded within the PAN to document completion of remediation actions.

If Mitigation is utilized to address a PAN, the SME will author a Mitigation Plan which will include planned actions to mitigate the vulnerability with specific timeframes [C3]. All mitigation plans require approval by the SME Supervisor. Approval will be documented within the Patch Management process [C4].

3.2.2 Patch Database Information

The SPM shall record the following patch information and key process decision times and outcomes including:

- Patch discovery by Patch Intake Coordinators along with its unique identity, description, release date and applicable system versions as reported by the patch source
- Determination of patch qualification as a security relevant patch that matches systems in use by TPS SBUs
- SME notification of patch availability
- SME evaluation of a patch’s applicability including disposition for Remediation or Mitigation
- Completion of remediation activities, or
- Mitigation Plans and their approval including status of Mitigation Plan actions

4.0 RECORDS

4.1 QA Records

None

4.2 Non-QA Records

None

5.0 DEFINITIONS

Change Management - SBU specific process(es) which govern modifications to cyber systems

Mitigation - actions taken to minimize risk without complete elimination of a specific vulnerability (e.g. implementing additional process checks, adding access control mechanisms, authoring Intrusion Detection System rules to detect anomalous activities)

Remediation - a security-related set of actions that results in a change to a system's state and may consist of changes motivated by the need to enforce organizational security policies, address discovered vulnerabilities, or correct misconfigurations. Remediation can include changes to operating system and application software configuration settings, the installation of patches, and the installation or removal of applications, software components or libraries (based on NIST Interim Report 7670 DRAFT Feb 2011)

Security Patch Manager (SPM) - Security Patch Manager is the application that houses artifacts documenting patch intake, evaluation decisions and dates, and mitigation plans

Patch Availability Notice (PAN) - Patch Availability Notice is the vehicle for tracking a vendor's patch notification through the patch management process

6.0 REFERENCES

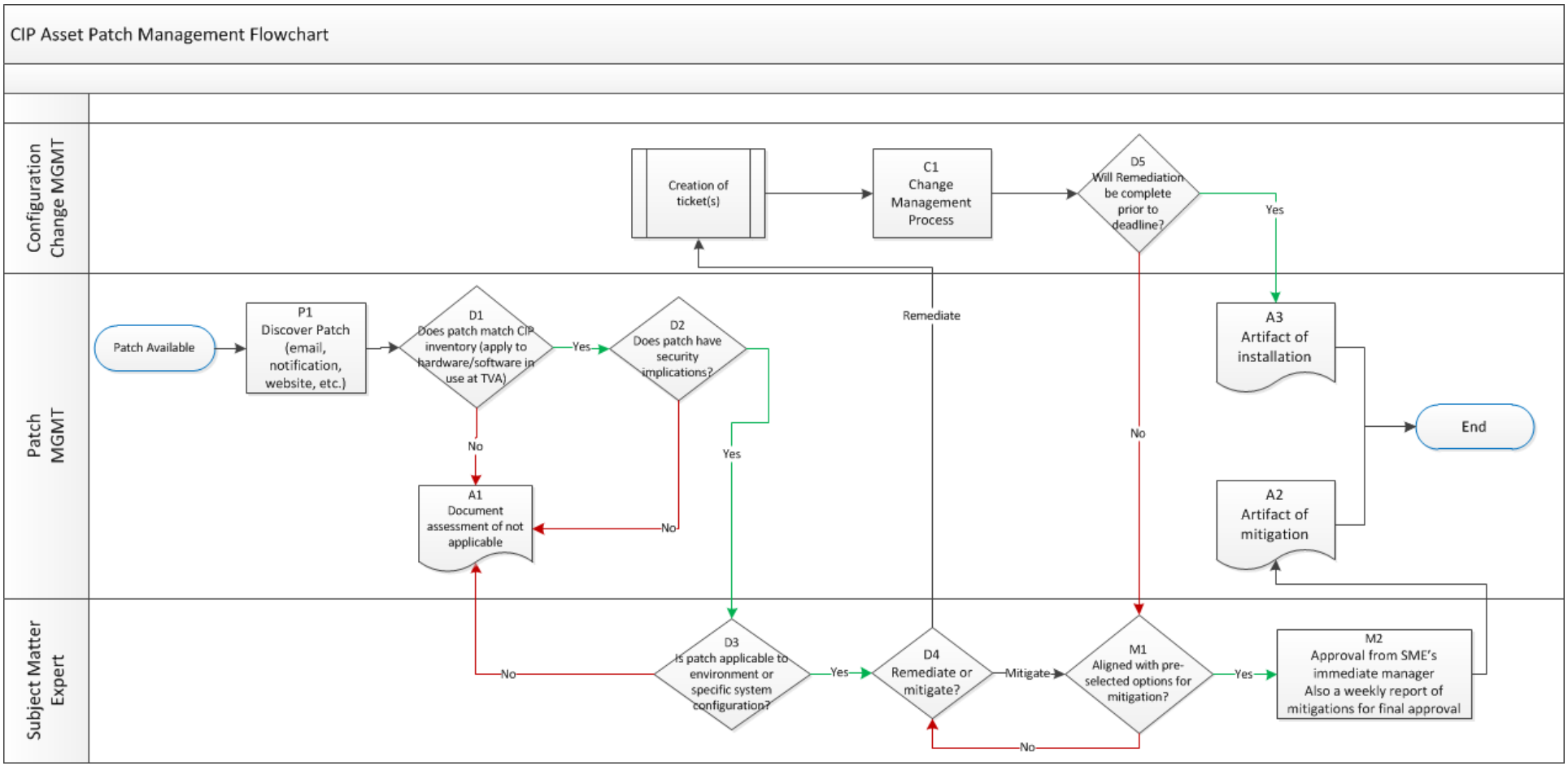
NERC CIP-007-5 Security Patch Management

TVA-SPP-12.004 TVA Cyber Security Patch and Vulnerability Management Program

NIST Interim Report (NISTIR) 7670 Proposed Open Specifications for Enterprise Information Security Remediation (DRAFT)

Appendix A
(Page 1 of 1)

Patch Management Process Overview



Source Notes
(Page 1 of 1)

Requirements Statement	Source Document	Implementing Statement
• Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.	NERC CIP 007-5	[C1]
• **2.1** A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.		
• **2.2** 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 in Part 2.1.	NERC CIP 007-5	[C2]
• **2.3** For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: Apply the applicable patches; or - Create a dated mitigation plan; or - Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	NERC CIP 007-5	[C3]
• 2.4 For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate	NERC CIP 007-5	[C4]