# CHANGE CONTROL & CONFIGURATION MANAGEMENT PROCESS

| | | |
|---|---|---|
| Category: | Critical Infrastructure Protection | |
| Type: | Cyber Security | |
| Document: | CIP-055 | |
| Owner: | Mike Pokas, Director, Information Technology Services | |
| Eff. Date/Rev. | 05/25/2011 | 004 |
| Approval: | Denis DesRosiers, Vice President IT & CIO | |

***** References to ITC are references to ITC Holdings Corp. together with all of its subsidiaries, unless otherwise noted.

## 1. INTRODUCTION

1.1. This process replaces CIP-055 Revision 003, dated 06/30/2010 and titled "Change Control & Configuration Management Process".

1.2. This document serves to satisfy the procedure requirements set forth in the following standards and will be reviewed annually as indicated by the associated Attachment 99 as described in GAP-001 Standard for Developing and Revising O&M Procedures:

1.2.1. NERC Cyber Security Standard CIP-003 Requirement 6

1.2.2. NERC Cyber Security Standard CIP-005 Requirement 5

1.2.3. NERC Cyber Security Standard CIP-007 Requirement 3

1.3. The purpose of this document is to record the ITC change and configuration management process employed for adding, modifying, or removing Critical Cyber Asset hardware, firmware or software within the Electronic Security Perimeter (ESP).

## 2. SCOPE AND RESPONSIBILITY

2.1. This process applies to all ITC employees, contractors, consultants, temporary employees and interns that will be collectively referred to herein as ITC resources.

2.2. This process applies to all cyber assets residing within any ITC Electronic Security Perimeter (ESP).

2.3. The characterization of configuration management varies for each area TMS, Field, Integrated Security Solution, and Physical Security Solutions and is the province of that area's Subject Matter Experts.

2.4. Change Controllers are responsible for approval and signoff of all change requests, change planning documents, impact and risk assessments, back out plans and test results.

2.4.1. A Change Controller can designate to a Subject Matter Expert (SME) roles and responsibilities for suitable management of change requests.

## 3. REFERENCES

3.1. NERC Cyber Security Standard CIP-003 Security Management Controls

3.2. NERC Cyber Security Standard CIP-005 Electronic Security Perimeter(s)

3.3. NERC Cyber Security Standard CIP-007 Systems Security Management

3.4. CIP-047 Security Control Testing Process

3.5. CIP-019 Access Controller and Change Controller Lists

3.6. NVA Report (Open Ports and Services)

3.7. TMS-002 Change Control and Configuration Management

3.8. TMS-003 Ports and Services

3.9. CIP-090 SCADA Critical Cyber Asset Document Management

3.10. CIP-091 SCADA Critical Cyber Asset Device Management

3.11. CIP-077 CIP Integrated Security Solution

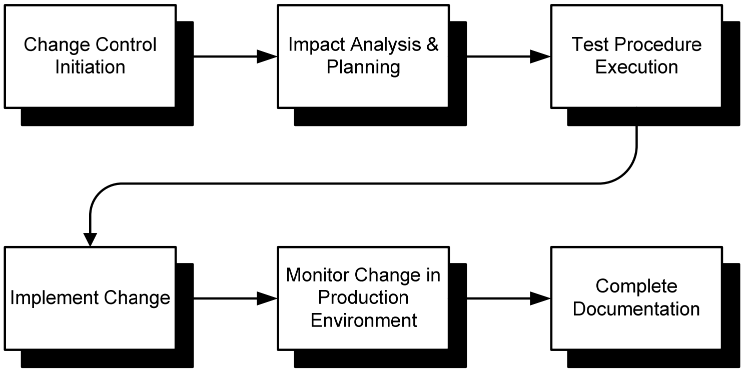
3.12. GAP-001 Standards for Developing Revising O&M Procedures

## 4. PRECAUTIONS

4.1. N/A

## 5. PROCEDURE

### 5.1. Process Flow


Change Control Initiation
Impact Analysis & Planning
Test Procedure Execution
Implement Change
Monitor Change in Production Environment
Complete Documentation

### 5.2. Change Control Initiation

5.2.1. When there is a need for adding, modifying, replacing, patching or removing Critical Cyber Asset hardware, firmware or software, the change control and configuration management process outlined in this procedure shall be initiated.

5.2.1.1. That initiation begins on request with an entry or record created in a change management tracking system by a representative of the ITC group requesting the change or on their behalf by the group responsible for the assets that will be affected.

5.2.1.2. The change management tracking system shall have restricted access to protect the integrity of its content and shall be controlled by an approved set of administrators.

5.2.1.3. The change requestor is responsible for documenting and presenting changes to the appropriate Change Controller including the nature of the change and an explanation of the change.

5.2.1.3.1. At the discretion and advice of the Change Controller, the change requestor may work with a SME to complete the elements of the Impact Analysis and planning in section 5.3 prior to the formal initiation of the change control process and to include the impact analysis assessment performed by the SME with the change request.

5.2.1.4. The list of authorized Change Controllers for each respective group is identified in the Change Controller List.

5.2.1.5. For each incoming change request the appropriate Change Controller or delegate will:

5.2.1.5.1. Review the incoming request for validity and potential impact.

5.2.1.5.2. Reject unsubstantiated, incomplete or incorrect change requests; or, where the impact assessment has been performed, changes where the impact is unacceptable or unsubstantiated.

5.2.1.6. Once the requested change is deemed valid, the Change Controller will assign it to a system Subject Matter Expert (SME) who will facilitate the impact analysis and planning for the change. This is recorded in the Change Management Tracking System.

## 5.3. Impact Analysis & Planning

5.3.1. The assigned SME shall, with consideration of the respective areas configuration management, perform and document an impact analysis that includes, as applicable:

5.3.1.1. Determination of components impacted by the change.

5.3.1.2. The ITC user group impacted by the pending change.

5.3.1.3. Identification of the resource responsible for implementing the change.

5.3.1.4. The SME shall perform an assessment of the impact analysis and submit the results to the Change Controller via the Tracking Management System for approval.

5.3.2. The Change Controller or delegate evaluates the impact assessment to determine if the change request can move forward.

5.3.2.1. If the impact of a change is deemed to be unacceptable or unsubstantiated the change request is cancelled, rejected or closed and the appropriate change requestor is notified.

5.3.2.1.1. The change requestor may be an integrated system or supporting staff.

5.3.2.2. The approval or cancellation shall be recorded in the change management tracking system.

5.3.3. Once the impact assessment has been reviewed and approved the responsible Change Controller or delegate notifies the SME that the change request can move forward.

5.3.3.1. SME develops a rollback plan for use in the event that the change needs to be backed out of the production environment.

5.3.3.2. The Change Controller delegate can move forward the request for test execution. The same is pre-authorized and recorded in the change management tracking system.

5.4. **Test Procedure Execution**

5.4.1. All testing should be performed in a testing environment where technically feasible.

5.4.2. The Change Controller or delegate assigns a Subject Matter Expert (SME) to plan and facilitate testing.

5.4.3. The SME makes a determination whether or not application testing is required for an approved change based on the nature and complexity of the change.

5.4.4. The SME determines the security control testing requirements based on CIP-047 Security Control Testing Process guidelines and system requirements.

5.4.5. The SME plans the appropriate application and security control test plans, manages the testing and performs an assessment of the results, makes recommendations, documents and submits them to the Change Controller or delegate.

5.4.6. The Change Controller or delegate reviews the test assessment and recommendations:

5.4.6.1. If the test results for a given change are not satisfactory they are rejected by the Change Controller and returned to the assigned SME for investigation, correction and/or retesting.

5.4.6.2. Satisfactory test results are approved by the Change Controller or delegate who will then assign the change to a SME to implement.

## 5.5. Implement Change

5.5.1. The SME shall plan and manage the implementation of the change in the production environment or its replica, in consideration of the impact analysis and planning previously done and in coordination with all impacted user groups.

5.5.2. The SME is responsible for documenting the implementation of the change.

## 5.6. Monitor Change in Production Environment

5.6.1. Following implementation, the SME shall observe the systems affected by the change for an appropriate time period before the change is declared successful.

5.6.1.1. The appropriate time period in which to monitor a change is determined by the assigned SME.

5.6.2. If the introduction of a change within the production environment produces results unacceptable to the users of the system, the change will be backed out.

5.6.2.1. The back out of the change will be executed in accordance with the procedures developed during the planning phase by the SME.

5.6.2.2. The back out process can be initiated by either the Change Controller, or their delegate.

## 5.7. Complete Documentation

5.7.1. Following a successful change implementation the SME shall ensure that changes are documented in the change record.

5.7.2. The Change controller will sanction the change request and will record the same in the Change Management Tracking System.

5.7.3. The Change Controller will notify the CIP Compliance Manager to determine if changes to CIP documentation are required.

### 5.8. Verification

5.8.1. The CIP Compliance Analyst will monitor for adherence to this policy.

### 5.9. Emergency Change Requests

5.9.1. In the case of an emergency change request the Change Controller or delegate will determine whether the request is warranted.

5.9.1.1. If warranted the change will be implemented.

5.9.1.2. The change management process documented above will be executed post implementation. Including:

5.9.1.2.1. Entries in the Change Management Tracking system

5.9.1.2.2. Completion of documentation and configuration management adjustments

5.9.1.3. The Change Controller will perform a post change audit to ensure that the emergency change does not affect other changes that may be in process.

## 6. ATTACHMENTS

6.1. CIP-055-Att99 Annual Review Internal-Attachment 99

## 7. MISCELLANEOUS

7.1. N/A

## 8. APPROVALS

Owner: <Signature on file> Date: 05/24/2011

Approver: <Signature on file> Date: 05/24/2011

## 9. REVISION HISTORY

| Effective Date | Revision Number | Individual Making Edits | Reason / Comments |
|---|---|---|---|
| 02/27/08 | 000 | M. Pokas | Initial version created to satisfy NERC standard CIP-003 Requirement 6 and NERC standard CIP-007 Requirement 2. |
| 04/29/09 | 001 | L. Trammer | Added Sect. 2.1.<br>Updated Sect 5.2.1 and 5.2.1.1.<br>Added Sect 5.4.1.<br>Added Sect. 5.7.3.<br>Changed “SSE” to “CIP”. |
| 03/31/10 | 002 | A. Stefan | Section 1: Added Section 1.4 and subsections 1.4.1, 1.4.2, and 1.4.3.<br>Section 3: Added Sections 3.10, 3.11, and 3.12 referencing NERC standard.<br>Section 5: To include “disabled” to Section 5.4.6.2.<br>Section 6: Added Section 6.1 referencing Att99. |

| Effective Date | Revision Number | Individual Making Edits | Reason / Comments |
|---|---|---|---|
| 06/30/2010 | 003 | T. Gruber/<br>P. Melendez | Section 1 – Added word "firmware" to 1.2 and added words "and its sub-requirements" to section 1.3.<br>Section 2 - rearranged in ascending hierarchy and added paragraph characterizing configuration management. Addition of section 2.4.1 for clarity regarding Change Controller to SME designation<br>Section 3- Removed generic Field device configuration management reference with appropriate procedures CIP-090, CIP-091 and CIP-092. Replaced NERC CIP standard requirements reference with the standard name.<br>5.2 - Reworded the 1st paragraph and moved consideration of configuration management from change controller in latter part to SME in the next section<br>5.2.1.3 – added subsection describing option for analysis to proceed formal request.<br>5.2.1.5.2, 5.2.1.6 – adjustments related to option for analysis proceeding request<br>5.3 – risk replaced with impact assessment. Added 5.3.2.1.1 to describe change request as integrated system or staff. (i.e. Asset Sentry) and section 5.3.3.2 to make pre-authorized role delegation of steps an option. Added- "or delegate" when appropriate.<br>5.4 – assignment of test resource moved up in sequence, associated most tasks to SME instead of change controller. Removed 5.4.6.2 sections on ports and services covered in CIP-047. Compressed satisfactory result actions<br>5.5 – rewrote and condensed<br>5.7 – replaced change controller with SME and removed compliance analyst sections. Section 5.7.2 was added to close out the process with Change Controller approval of the change request.<br>5.9 – compressed. |

| Effective Date | Revision Number | Individual Making Edits | Reason / Comments |
|---|---|---|---|
| 5/25/11 | 004 | C. Lewis | E. Howell and S. Stout removed as approvers.<br>Changed Mike Pokas title in header<br>Section 1.2 – Added GAP-001.<br>Removed CIP-092 from references<br>Section 3 - Added GAP-001.<br>Section 5.7.1. - Changed From ” Following a successful change implementation the SME shall ensure that documentation and configuration management adjustments have been completed appropriately.  To “ Following a successful change implementation the SME shall ensure that changes are documented in the change record.<br>Changes are documented in the change management system. |