

# **SERC Compliance Monitoring and Enforcement Program**

## **Implementation Procedure 3.3 Spot Checking**



## SERC CMEP Implementation Procedure 3.3: Spot Checking

---

### Revision History

Revision	Date	Originator	Comments
0	June 1, 2007	B. Goss	Document Origination.
1	April 14, 2009	B. Goss	Added Cross Reference Table. Reorganized Procedure Steps into three separate sections and updated text throughout to better describe processes.

### Cross Reference Table

The procedures listed in the table below refer to this procedure, Compliance Implementation Procedure 3.3: Spot Checking. As revisions are made to Procedure 3.3, the Originator should review the procedures listed to determine if corresponding changes to these procedures are warranted.

Procedure Number	Procedure Title
5.0	Consolidated Compliance Enforcement Tracking
3.1	Compliance Audits

### Responsible SERC Group(s)

SERC Compliance Director  
SERC Manager of Compliance Audits

### Review and Re-Approval Requirements

This document will be reviewed every two years or as appropriate for possible revision. The existing or revised document will be re-approved by the SERC Board Compliance Committee, distributed to all SERC members by the Director of Compliance, and posted on the SERC website for Registered Entity and SERC Member reference.

## Table of Contents

1.0	Purpose .....	4
2.0	Responsibilities .....	4
3.0	References .....	4
4.0	Procedure Steps .....	4
4.1	Procedure Steps for a Non-CIP Standard Spot Check .....	5
4.2	Procedure Steps for a CIP Standard Spot Check (conducted as part of a Compliance Audit) .....	7
4.3	Procedure Steps for a CIP Standard Spot Check ( <b>NOT</b> conducted as a part of a scheduled Compliance Audit) .....	7

### 1.0 Purpose

The SERC Compliance organization may direct initiation of Spot Checking at any time to verify or confirm Self-Certifications, Self Reporting, and Periodic Data Submittals. Spot Checking may also be random or may be initiated in response to events, as described in the Reliability Standards, or by operating problems, or system events. This procedure augments Section 3.3 of the SERC Compliance Monitoring and Enforcement Program (CMEP).

### 2.0 Responsibilities

The Manager of Compliance Audits (MCA) identifies candidates for Spot-Checks based on audit results, input from compliance staff, in response to events or operating problems, or as directed by the Compliance Director (CD). Additionally, specific Reliability Standards/requirements may be identified in the NERC CMEP Annual Implementation Plan as subject to Spot Checks during the current monitoring period.

### 3.0 References

SERC CMEP Implementation Manual Section 3.3  
NERC CMEP Annual Implementation Plan  
NERC Rules of Procedure Section 1501

### 4.0 Procedure Steps

The procedure steps are divided into three categories:

- (1) Non-CIP Standard Spot Checks
- (2) CIP Standard Spot Check – conducted as part of a Compliance Audit
- (3) CIP Standard Spot Check – not conducted as part of a Compliance Audit

CIP is the acronym for Critical Infrastructure Protection. Per the NERC Rules of Procedure (ROP) Section 1501, Critical infrastructure is defined as existing or proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters.

Spot Checks are performed on Critical infrastructure (“CIP Standard Spot Check”) and Non-Critical infrastructure (“Non-CIP Standard Spot Check”). However, Spot Checks are handled differently depending on whether the systems/assets are classified as CIP or not. The primary differences include evidence handling, and whether or not the Spot Check is performed on site. CIP Standard Spot Checks are performed on-site, and most Non-CIP Standard Spot Checks are performed off-site.

Procedure steps for CIP Standard Spot Checks that are part of a Compliance Audit closely mirror those in Procedure 3.1 Compliance Audits. Therefore, the steps are not

## SERC CMEP Implementation Procedure 3.3: Spot Checking

---

repeated in this procedure. Readers should refer to Procedure 3.1 for the preparation milestones and timelines (ex: “T-90, T+14,” etc...), Report Processing, Audit (Spot Check) Conduct, and Post-Exit Actions.

Procedure steps for CIP Standard Spot Checks that are **NOT** part of a Compliance Audit are described in detail in this procedure. The timelines are different from those when the Spot Check is part of an audit and therefore Procedure 3.1 is not applicable.

### 4.1 Procedure Steps for a Non-CIP Standard Spot Check

- The Manager of Compliance Audits (MCA) defines a preliminary Spot Check scope including:
  - SERC staff responsible as the Single Point of Contact (SPOC)
  - Registered Entity(s) involved
  - Reason for the Spot Check
  - Topics and/or applicable Reliability Standards
  - Desired completion schedule
- The CD authorizes the Spot Check.
- The SPOC is notified by the MCA as to the Registered Entity (“Entity”) to be Spot Checked, the scope of the Spot Check, and the desired completion schedule. The SPOC will prepare and send the MCA blank Questionnaire/Reliability Standard Audit Worksheets (Q/Rs) for the Standards identified.
- The MCA notifies the involved Entity(s) of the intent to perform a Spot Check and the reason for the Spot Check via a Spot Check Notification Letter. The Spot Check Notification Letter identifies documentation and evidence requirements along with their required submittal date and method. (See also NERC CMEP Attachment 1: Process for Non-Submittal of Requested Data.) The notice will provide for at least 30 days to submit requested information. In cases where an advance notice period specified in the involved Reliability Standard is greater than 30 days, then the notice shall not be less than required in the Reliability Standard.

Note: SERC recognizes that there may be times when a Registered Entity has a legitimate business need to propose an alternate completion schedule. For any reasonable request, as determined by SERC, SERC and the Registered Entity will work together to find mutually agreeable dates within the required monitoring period.

- The Registered Entity provides requested documentation, evidence and Q/Rs (with the Supporting Material/Documentation section completed) to the SPOC in the specified format by the requested date.

## SERC CMEP Implementation Procedure 3.3: Spot Checking

---

- The SPOC reviews information cited in the Q/Rs to determine the level of compliance with the Reliability Standards and may request additional data and/or information as needed to ensure an accurate determination of compliance.
- The SPOC notifies the MCA if requested data is not received in the format or by the due date requested.
- In the event the Entity does not submit the requested data in the form and by the date requested, the MCA reviews the circumstances and reasonableness of the request and contacts the Registered Entity to resolve.
- If the Registered Entity fails to submit the information to SERC's satisfaction and in a timely manner following SERC's inquiry, the MCA will notify the CD and initiation of the escalation process for non-submittal of requested data, per NERC CMEP Attachment 1: "Process for Non-Submittal of Requested Data," will begin.
- The Registered Entity's documentation, evidence and Q/Rs with documents are reviewed by the SPOC, and other SERC staff as needed, and a preliminary assessment of compliance to the applicable Standard(s) is determined by a process identical to the one used in a Compliance Audit (SERC CMEP 3.1).
- The SPOC documents the assessment of the Registered Entity for compliance with the applicable Reliability Standards by completing appropriate portion(s) of applicable Q/Rs.
- The SPOC completes a formal Spot Check assessment using the current report template.
- The SPOC forwards the completed Q/Rs to the MCA along with the findings of compliance.
- The MCA reviews, or assigns other compliance staff to review, the findings submitted by the SPOC.
- If the Spot Check does not identify any possible violations, the SPOC drafts a Spot Check Report and Transmittal Letter containing the findings and forwards to the MCA for approval and distribution to the Registered Entity indicating the results of the Spot Check and that no further action will be taken.
- If the Spot Check determines the presence of a possible violation, the SPOC drafts a Spot Check Report and Transmittal Letter containing the findings and

## SERC CMEP Implementation Procedure 3.3: Spot Checking

---

forwards to the MCA for approval and distribution to the Registered Entity indicating the results of the Spot Check and that further action is warranted.

- The SPOC ensures that all relevant information is forwarded to the on-duty Screener for entry into the Compliance Tracking Database and the process enters Step 2 of the CMEP Process (in accordance with Implementation Procedure 5.0, Consolidated Compliance Enforcement Tracking), a Staff Review of the Alleged violation to determine additional action under the CMEP.
- A final copy of the Spot Check Report and Transmittal Letter is converted to PDF format and retained, in both WORD and PDF format, by SERC for the specified data retention period in accordance with the NERC ROP Section 1500 and SERC Implementation Procedure 9.0, Data Management and Confidentiality.
- The MCA approves the Spot Check Report and Transmittal Letter
- The Executive Assistant for Audit Program (EA) transmits the Spot Check Report and Transmittal Letter to the Registered Entity. If no violations are found, this process normally completes within ninety (90) days of SERC's receipt of data.

### 4.2 Procedure Steps for a CIP Standard Spot Check (conducted as part of a Compliance Audit)

As noted in Section 4.0, the procedure steps for a CIP Standard Spot Check that is conducted as part of a Compliance Audit mirror those found in Procedure 3.1, Compliance Audits, and therefore are not repeated here in their entirety. The reader should refer to Procedure 3.1 for milestones and timelines. General steps include:

- The MCA ensures appropriate audit scope based on the functions performed by the Registered Entity.
- The MCA ensures preparation and notification steps required to support the on-site audit/Spot Check are completed.
- The MCA approves Non-Public Audit Reports and CIP Standard Spot Check Reports prior to distribution.

### 4.3 Procedure Steps for a CIP Standard Spot Check (***NOT*** conducted as a part of a scheduled Compliance Audit)

#### CIP Spot Check Planning / Scheduling

- The MCA develops an annual CIP Standard Spot Check plan that defines the specific registered Entities subject to a stand-alone CIP Standard Spot Check.

## SERC CMEP Implementation Procedure 3.3: Spot Checking

---

- The MCA coordinates CIP Standard Spot Checks of Entities that are registered in multiple Regions with the appropriate regions to determine if the CIP Standard Spot Check could or should be combined into a single, multi-region CIP Standard Spot Check of the Entity.
  - If it is determined that more than one Regional Entity will participate in a combined CIP Standard Spot Check, a single Region will be designated to coordinate and conduct the CIP Standard Spot Check.
- The MCA ensures appropriate CIP Standard Spot Check scope based on the functions performed by the Registered Entity.
  - All applicable standards that have been monitored during the current and preceding three years are subject to CIP Standard Spot Check.
- The MCA ensures preparation and notification steps required to support the on-site CIP Standard Spot Check are completed. The target preparation and notification milestones for each scheduled CIP Standard Spot Check are shown below where **T-30** is the start of the on-site CIP Standard Spot Check process.

### **T-30 Days (1 month) - MCA**

- Create appropriate folders in CIP Standard Spot Check Committee on the portal
- Send to Entity:
  - CIP Standard Spot Check Detail Letter
  - Standards/requirements in scope
  - CIP Standard Spot Check Team Members
  - Data retention requirements
  - CIP Standard Spot Check Team Bios
  - CIP Standard Spot Check Team Non-Disclosure Verification
  - Documentation and Evidence Requirements
  - Questionnaire (Q/Rs)

### **Registered Entity:**

- The Registered Entity will:
    - Provide answers and any requested data.
    - Review the audit team members for objections.
- The Registered Entity response to SERC is due within 15 days.
- Post a copy of all above documents to CIP Standard Spot Check Committee
  - Save copy of email to appropriate CIP Standard Spot Check folder on the S drive

### **T-30 Days (1 month) – Audit Team Leader (ATL)**

- Finalize expected CIP Standard Spot Check duration and on-site schedule
- Provide CIP Standard Spot Check Team with Logistics and hotel information

## **SERC CMEP Implementation Procedure 3.3: Spot Checking**

---

- Provide just-in-time audit training materials to CIP Standard Spot Check team
  - ATL will send email to assign Just-In-Time auditor training (PPT) to all industry subject matter experts, non-compliance auditor staff and, at ATL discretion, SERC auditors
- Upload just-in-time auditor training PPT to CIP Standard Spot Check Committee on ftp site
- Conduct pre-CIP Standard Spot Check teleconference or web cast with CIP Standard Spot Check team
  - Answer any Just-In-Time auditor training questions
- Conduct pre-CIP Standard Spot Check teleconference or web cast with Entity

### **T-30 Days (1 month) -ATL and CIP Standard Spot Check Team**

- Determine team focus during CIP Standard Spot Check
- Review Entity compliance history, SERC Self-Certifications, Letters of Certification, Reporting Forms for applicable Standards
- Review Entity Self-Report and mitigation status and expand CIP Standard Spot Check Scope if applicable

### **T-14 Days (2 weeks) - ATL**

- Verify that Entity has been notified of any changes to CIP Standard Spot Check Team composition
  - Provide Non-Disclosure Agreement Signature Verification, if applicable
- Contact Enforcement to update review of compliance history, self-certifications, self-reporting, open and/or recently closed mitigation plans
- Assign auditor to draft CIP Standard Spot Check Report
- Address any Entity or CIP Standard Spot Check Team concerns

### **T-7 Days (1 week) – ATL**

- ATL requests MCA lock-down CIP Standard Spot Check Committee (remove all Registered Entity personnel)

## **T-0 On-Site CIP Standard Spot Check**

### **T+24 Hours**

- ATL completes Screener Worksheet, for any possible violations found during CIP Spot Check, and forwards to on-duty Screener
- Scribe reviews and corrects Q/Rs for accuracy, spelling and grammar and posts Completed Q/Rs to Standard Spot Check Committee, and notifies ATL of posting
- ATL copies Completed Q/Rs to a secure flash drive and delivers to MCA for secure storage
- ATL requests MCA restore appropriate Entity personnel to Standard Spot Check Committee

### **T+7 Days**

## SERC CMEP Implementation Procedure 3.3: Spot Checking

---

- Assigned auditor completes Draft Non-Public CIP Standard Spot Check Report (report is created on scribe's secure flash drive), then
  - Saves report to committee site
  - Notifies CIP Standard Spot Check Team and ATL that report is ready for review and comment, and copies MCA on notification.
  - All CIP Standard Spot Check reports shall include "Non-Public" as a part of the CIP Standard Spot Check report file name
  - ATL will denote date received in Audit Report Progress Database

### **T+14 Days**

- The ATL incorporates CIP Standard Spot Check Team comments into the Draft Non-Public Standard Spot Check Report, saves report to CIP Standard Spot Check Committee, notifies the EA that the report is ready for editing and copies MCA of the notification
  - ATL will denote date forwarded in Audit Report Progress Database.

### **T+19 Days**

- The EA completes review and editing of Draft Non-Public CIP Standard Spot Check Report, uploads report to Standard Spot Check committee, and notifies the ATL the report is ready for review
- EA records date report forwarded to ATL in Audit Report Progress Database

### **T+21 Days**

- ATL corrects the Non-Public CIP Standard Spot Check Report, as necessary
- ATL saves report to Standard Spot Check Committee
- ATL deletes all previous copies of report from committee
- ATL notifies EA that Draft Non-Public CIP Standard Spot Check Report for Entity Comment is ready to be copied to secure CIP Standard Spot Check Report flash drive
- ATL notifies the Entity the report is posted on the committee site for comment, and copies MCA of the notification

### **Registered Entity**

- The Registered Entity will review the Draft Non-Public Standard Spot Check Report and provide comments within 14 days.
  - ATL records date of posting in Audit Report Progress Database
- ATL notifies the designated Single Point of Contact (SPOC) that Q/Rs are available, if possible violations were determined during CIP Standard Spot Check

### **T+35 Days - ATL**

- ATL reviews and incorporates Entity comments into the Draft Non-Public CIP Standard Spot Check Report as appropriate and saves report to committee
  - ATL denotes date received in Audit Report Progress Database

## SERC CMEP Implementation Procedure 3.3: Spot Checking

---

- ATL notifies the EA that the Non-Public CIP Standard Spot Check Report is ready for editing, to save a copy of report with Entity comments to the CIP Standard Spot Check Report secure flash drive, and copies MCA on the notification
  - ATL will denote date forwarded in Audit Report Progress Database
- If the CIP Standard Spot Check indentified possible violation, the ATL notifies the assigned SPOC of the Draft CIP Standard Spot Check Report available on the committee site, and requests the MCA add the SPOC to the committee
- EA completes review and editing of Non-Public CIP Standard Spot Check Report, notifies the ATL, and copies MCA of the notification
- ATL reviews and corrects Draft Non-Public Standard CIP Spot Check Report, as necessary, posts report on CIP Standard Spot Check Committee, and notifies EA that report is ready for copying to secure CIP Standard Spot Check Report flash drive
- ATL notifies the MCA the report is ready for approval
  - ATL will denote date forwarded in CIP Standard Spot Check Report Progress Database

### **T+42 Days – MCA**

- MCA reviews and approves the Draft Non-Public CIP Standard Spot Check Report as the final Non-Public CIP Standard Spot Check Report
  - MCA denotes date approved in Audit Report Progress Database
- EA converts Draft Non-Public CIP Standard Spot Check Report to PDF format, prepares and converts Transmittal letter, signed by MCA, to PDF Format, and posts documents to committee
- EA saves copies of Final Non-Public CIP Standard Spot Check Report and Transmittal Letter, in both WORD and PDF format, to secure CIP Standard Spot Check Report flash drive

### **T+56 Days**

- The EA will notify the Spot Checked Entity that a copy of the Final Non-Public CIP Standard Spot Check Report and Transmittal Letter are available on the committee site for comment
  - The EA will record the date Entity was notified to in the Tracking Database.
- The Entity will have 10 days to download the Non-Public CIP Standard Spot Check Report and Transmittal Letter.

### **T+66 Days**

- ATL ensures that copies of all documents in CIP Standard Spot Check Committee folder are in appropriate CIP Standard Spot Check folder on S drive
  - This includes verification that the following CIP Standard Spot Check Reports are stored on the CIP Standard Spot Check Report secure flash drive:
    - Draft Non-Public CIP Standard Spot Check with Entity Comments
    - Draft Non-Public CIP Standard Spot Check for MCA Approval

## SERC CMEP Implementation Procedure 3.3: Spot Checking

---

- Final Non-Public CIP Standard Spot Check Report and Transmittal Letter
- ATL removes all documents from CIP Standard Spot Check Committee folder
- ATL notifies MCA that all documents have been removed from CIP Standard Spot Check Committee folder
- ATL notifies MCA that CIP Standard Spot Check Committee is ready to be deleted from portal