

SERC Compliance Monitoring and Enforcement Program

Implementation Procedure 3.1 Compliance Audits



SERC CMEP Implementation Procedure 3.1: Compliance Audits

Revision History

Revision	Date	Originator	Comments
0	May 31, 2007	B. Goss	Document Origination.
1	June 28, 2007	T. Galloway	Initiator for revs to Appendix G, addition of Appendices H & I
2	March 14, 2008	B. Goss and J. Harrell	Major procedure revisions, deletion and addition of Appendices, disposition of stakeholder comments to Rev. 2 draft, and new NERC Audit Report processing requirements
3	October 2, 2008	J. Harrell	Change approval authority for Non-Public Audit Reports from CD to MCA and updated audit time-lines.
4	April 21, 2009	B. Goss	Removed appendices. Updated job and document titles. General clarifications.

Responsible SERC Group(s)

SERC Compliance Director
SERC Compliance Enforcement Manager
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 (BCC), distributed by the Compliance Director to all applicable SERC staff, and posted on the website for Registered Entity and SERC Member reference.

Cross Reference Table

The procedures listed in the table below refer to this procedure. As revisions are made to this procedure, 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 Tracking
3.3	Spot Checking

Table of Contents

1.0	Purpose	4
2.0	Responsibilities	4
3.0	References	4
4.0	Procedure Steps	5
4.1	Audit Planning / Scheduling	5
4.2	Audit Conduct	13
4.2.1.	Entrance Briefing	13
4.2.2.	Team Focus / Assignments.....	13
4.2.3.	Completion of Reliability Standard Audit Worksheets (RSAWs)(Q/Rs)	14
4.2.4.	Evidence Retention.....	14
4.2.5.	Daily Updates	14
4.2.6.	Team Interaction	15
4.2.7.	Exit Briefing.....	15
4.3	Post-Exit Actions	15
4.4	Unscheduled Audits	16

1.0 Purpose

The Compliance Enforcement Authority conducts compliance audits as required by the NERC Rules of Procedure. The purpose of this procedure is to define the steps required to plan and execute compliance audits (scheduled and unscheduled). All registered entities are subject to audit for compliance with all Reliability Standards applicable to the functions for which the Registered Entity is registered. This procedure augments Section 3.1 of the SERC Compliance Monitoring and Enforcement Program (CMEP).

2.0 Responsibilities

- The SERC Manager of Compliance Audits (MCA) Audit Team Leaders (ATL) and Audit Program Executive Assistant (EA) are responsible for meeting the requirements and implementing the applicable sections of this procedure.
- All Compliance Audit Participants*are responsible for:
 - Adhering to the the requirements set forth in this procedure
 - Adhering to the agreed upon schedules and timeframes for the turnaround of information as set forth in this procedure.
 - Maintaining audit materials as confidential.
 - Complying with the NERC Antitrust Compliance Guidelines and signing applicable confidentiality agreements.
 - Identifying any circumstances that could represent a potential conflict of interest or impede impartial treatment of the audited entity.
 - Completing and signing Conflict of Interest forms for each audited entity.
 - Adhering to the requirements of SERC Auditor Objectivity, Independence and Impairment
 - Adhering to the requirements of SERC Auditor Rules of Evidence and Professional Judgment.

*Compliance Audit Participants are defined in the SERC CMEP as, “Registered Entities scheduled to be audited and the audit team members.”

- The Compliance Director is responsible for:
 - Approval of the long-range and annual audit schedules
 - Coordinating audits in response to directives from FERC
 - Ruling on all Registered Entity objections to team composition.
 - Approval of unscheduled audits
 - Final approval of Public Audit Reports and of report transmission to NERC.

3.0 References

- NERC Auditor Guide
- NERC Pre-Audit Questionnaires and Reliability Standard Audit Worksheets

SERC CMEP Implementation Procedure 3.1: Compliance Audits

- SERC CMEP Implementation Manual Section 3.1
- NERC Rules of Procedure Section 403.11
- Government Accountability Office Government Auditing Standards
- Implementation Procedure 5.0 Consolidated Compliance Enforcement Tracking

4.0 Procedure Steps

4.1 Audit Planning / Scheduling

- The Manager of Compliance Audits (MCA) annually updates a long-range audit plan to ensure each of the registered entities is audited per the required frequency. As part of the annual audit plan development, the MCA will review any changes to Generally Accepted Government Auditing Standards (GAGAS) that have occurred for consideration in modifying the audit plan.
 - Registered entities performing Reliability Coordinator (RC), Balancing Authority (BA), or Transmission Operator (TOP) functions will be audited once every three (3) years.
 - Generator Operators (GOPs) will each be audited for compliance with TOP-003 requirements once per three (3) years. Off-site audits / spot checks can be used in lieu of an on-site audit, as appropriate, to allow for specific focus on TOP-003.
 - Registered entities that do not perform RC, BA, or TOP functions will typically be audited at least once every six (6) years.
 - Audits can involve on-site visits or off-site reviews as allowed by applicable Reliability Standards.
 - The MCA issues an annual audit plan that defines the specific registered entities subject to audit, audit type, and the candidate month. The annual audit plan is coordinated with NERC and periodic updates are provided to NERC and registered entities. The annual audit plan references the Reliability Standards in effect and selected for monitoring for the year. Prior to January 1 of the year covered by the annual audit plan, SERC will post a schedule and identify Registered Entities subject to compliance audits for the upcoming year and provide the audit schedules, methods, and data requirements for the audit.
- The MCA coordinates audits of entities that are registered in multiple Regions both with NERC and the Compliance Monitoring Processes Working Group (CMPWG) (comprised of representatives from all Regional Entities) to determine if the audit could or should be combined into a single audit of the entity.
 - If it is determined that more than one Regional Entity will participate in a combined audit, a single Region, or NERC, will be designated to coordinate all audit processes and requirements to meet the criteria of a single audit.
- The MCA ensures appropriate audit scope based on the functions performed by the Registered Entity. A Compliance Audit will include all Reliability Standards applicable to the Registered Entity and monitored in the NERC

SERC CMEP Implementation Procedure 3.1: Compliance Audits

Implementation Plans in the current and three previous years, and may include other Reliability Standards applicable to the Registered Entity. The audit period will be the lesser timeframe of the date of the Registered Entity's last audit, June 18, 2007, or date of entity registration.

- The MCA ensures preparation and notification steps as required to support the on-site audit are completed. The target preparation and notification milestones for each scheduled audit are shown below where **T-0** is the start of the on-site audit.
- The MCA approves Non-Public Audit Reports prior to distribution.

NOTE: The following preparation milestones are for SERC internal planning use and are subject to variations based on prevailing circumstances at the time of audit process implementation. They do not pertain to unscheduled audits. However, for all scheduled audits registered entities will be provided a list of audit team members at least two months in advance to allow for objections. Similarly, registered entities can also object to audit team members for unscheduled audits.

T-270 Days (9 months) - MCA

- Initial contact with entity (MCA)
 - Schedule audit week
 - SERC and the Registered Entity work together to find mutually agreeable dates within the required audit timeframe.
 - Verbal confirmation of registered functions
 - Determine Audit Contact person of Registered Entity
 - Name
 - Title
 - Phone
 - Cell
 - Email
 - Send audit week confirmation email to Registered Entity
- Save email to appropriate folder in S: drive audit folder

T-180 Days (6 months) - MCA

- Determine Audit Team Leader
- Send audited entity:
 - Introduction Letter
 - Initial Audit Notification Letter, and
 - Pre-Audit Survey
- Save documents and email to appropriate folders in S: drive audit folder

Registered Entity:

The Registered Entity is responsible for providing answers and any requested data; the Registered Entity response to SERC is due within 30 days.

SERC CMEP Implementation Procedure 3.1: Compliance Audits

T-150 Days (5 months) - MCA

- Save entity response email and attached documents to appropriate folder in S: drive audit folder
- Verify entity registered functions (response to Initial Audit Letter)
- Determine Audit Scope (standards applicable)
- Determine Audit Team members
- Determine Audit Team Member required qualifications

T-120 Days (4 months)

MCA

- Confirm each selected Audit Team Member's participation in the audit
- Prepare Non-Disclosure Agreement Verification
- Create Audit Committee on Portal
 - Create appropriate folders in Audit Committee on the portal
 - Populate Audit Committee with Audit Team Member, and specified entity contacts (verify entity personnel have appropriate access permissions)

ATL/EA

- For each Audit Team Member, verify receipt or confirmation, as applicable, of:
 - Signed Non-Disclosure Agreement
 - Signed Conflict of Interest Forms
 - Not employed by entity for 6 months (preferably 2 years)
 - Auditor and industry subject matter expert(s) Bio(s) as required
 - Completion of required NERC auditor training completed
- Assemble Non-Disclosure Agreement Verification, COI's and Bios for all team members and save to Team Credentials folder in appropriate S drive audit folder (ATL)
- Assemble Pre-Audit Questionnaire/RSAs (Q/R) and post in the Audit Committee folder(EA)
- Draft Compliance Audit Certification Letter (EA)
 - Draft "Documentation and Evidence Requirements" list
 - Determine subset of static data to be requested for pre-audit disposition of selected standards

T-90 Days (3 months) – MCA

- Send to entity
 - Audit Detail Letter
 - Standards in scope
 - Audit Team Members
 - Data retention requirements
 - Audit Team Bios
 - Audit Team Non-Disclosure Verification
 - Compliance Audit Certification Letter

SERC CMEP Implementation Procedure 3.1: Compliance Audits

- Documentation and Evidence Requirements
- Data Certification
 - Ensure Pre-Audit Questionnaire/RSAW (Q/R) are posted in Audit Committee on portal
 - Request for Static Data for early disposition of appropriate standards
- Save copy of email and individual files to appropriate audit folder in the S drive audit folder
- Save copy of email and individual files to appropriate folders in Audit Committee folder on the portal.

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 60 days.

Objections:

A Registered Entity subject to a Compliance Audit may object to any member of the audit team on grounds of a conflict of interest or the existence of other circumstances that could interfere with the team member's impartial performance of his or her duties. Such objections must be provided in writing to SERC no later than fifteen (15) days prior to the start of on-site audit work. Detailed information on Objections is provided in the SERC CMEP Section 3.1.

T-60 Days (2 months)

MCA

- Reconcile any required changes to Audit Team
 - Verify Non-Disclosure Agreements, COI's, employment history and Bios for any new team members are up to date
 - Notify entity of any changes in team composition

ATL

- Conduct pre-audit teleconference or web cast with entity
- Ensure entity notification of any Audit Team changes
- Ensure all advance documents are saved to appropriate audit committee folders on ftp site and S drive audit folder
- Finalize expected audit duration and on-site schedule
- Provide Audit Team with Logistics and hotel information
- Provide just-in-time audit training materials to audit 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 Audit Committee on ftp site

T-30 Days (1 month)

ATL

- Distribute advance information to team
- Conduct pre-audit teleconference or web cast with audit team
 - Answer any Just-In-Time auditor training questions
- Assign auditor to draft Q/Rs for any standards that can be completed prior to on-site audit
 - Completed pre-disposition Q/Rs are forwarded to the ATL for review

ATL and Audit Team

- Determine team focus during audit (See Section 4.2.2)
 - Review advance information.
 - Perform preliminary assessment of conformance with the requirements of the Reliability Standards prior to performing the audit.
 - Review entity compliance history, SERC Self-Certifications, Letters of Certification and Reporting Forms for applicable standards
 - Review entity self-report and mitigation status and expand Audit Scope if applicable

T-14 Days (2 weeks) - ATL

- Conduct Pre-Audit Compliance Program teleconference or web cast
- Verify that entity has been notified of any changes to Audit 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 Audit Report
- Ensure Registered Entity has all relevant audit materials, schedules, and agendas.
- Address any entity or Audit Team concerns
- Save entity approved pre-dispositioned Q/Rs to Completed Q/Rs folder in entity audit folder on S drive

T-0 On-Site Audit

T+24 Hours- ATL

- ATL completes Screener Worksheet, for any possible violations found during audit, and forwards to on-duty Screener. See Implementation Procedure 5.0 Consolidated Compliance Enforcement Tracking
- Audit track scribe(s) reviews and corrects Q/Rs for accuracy, spelling and grammar and forwards to ATL
 - When an audit team is divided into two or more teams (tracks), each team will have a designated scribe (audit track scribe). Each audit track scribe will

SERC CMEP Implementation Procedure 3.1: Compliance Audits

be responsible for reviewing, correcting and forwarding their respective Q/Rs to the ATL.

T+7 Days -ATL and MCA

- Assigned auditor completes Draft Non-Public Audit Report, using the current NERC Audit Report Template, and forwards to Audit Team and ATL for review and comment, and copies MCA
 - All draft audit reports shall include “Non-Public” as a part of the audit report file name
 - ATL will denote date received in Audit Report Progress Database
- Regional Self-Certification Form
 - ATL completes and forwards to MCA
 - MCA forwards to NERC Regional Primary Contact

T+14 Days - ATL

- The ATL incorporates Audit Team comments into the Draft Non-Public Audit Report, forwards report to the Executive Assistant (EA) for editing and copies MCA
 - ATL will denote date forwarded in Audit Report Progress Database.

T+19 Days - EA

- The EA completes review and editing of Draft Non-Public Audit Report and forwards to ATL for review
 - EA records date report forwarded to ATL in Audit Report Progress Database

T+21 Days - ATL

- ATL corrects the Non-Public Audit Report, as necessary, forwards to entity for comments, and copies MCA
 - Audit Reports sent to entity for comments by email should be marked Confidential, and require both Receive and Read Receipts
- ATL notifies the designated Single Point of Contact (SPOC) of Q/R posting if possible violations were determined during audit

Registered Entity

- The Registered Entity will review the Draft Non-Public Audit Report and provide comments within 14 days.

T+35 Days – ATL/EA

- ATL reviews and incorporates entity comments into the Draft Non-Public Audit Report as appropriate
 - ATL will denote date received in Audit Report Progress Database
- ATL forwards Non-Public Audit Report to EA for editing, and copies MCA
 - ATL will denote date forwarded in Audit Report Progress Database

SERC CMEP Implementation Procedure 3.1: Compliance Audits

- ATL forwards copy of Draft Audit Report, with entity comments, to designated SPOC for identified possible violation(s)

T+40 Days – ATL/EA

- EA completes review and editing of Draft Non-Public Audit Report, forwards to ATL and copies MCA
- ATL reviews and corrects Draft Non-Public Audit Report, as necessary, and forwards to MCA for approval
 - ATL will denote date forwarded in Audit Report Progress Database
- ATL saves copy of Draft Non-Public Audit Report to appropriate Audit folder on S drive

T+42 Days – MCA

- MCA reviews and approves the Draft Non-Public Audit Report as the final Non-Public Audit Report
 - MCA denotes date approved in Audit Report Progress Database

T+56 Days

- The EA will forward a copy of the final Non-Public Audit Report to the audited entity and to NERC simultaneously
 - The EA will record the date the report was forwarded to the entity and NERC in the Tracking Database and save a copy of the email on the S drive.
 - The EA will save a copies of the Final Non-Public report, in both WORD and PDF file formats, to the appropriate audit folder on the S drive
- EA ensures that copies of all documents in Audit Committee folder are in appropriate Audit folders on S drive
- EA removes all documents from Audit Committee folder
- EA notifies MCA that all documents have been removed from Audit Committee folder.
- EA notifies ATL of Non-Public Audit Report submittal to Registered Entity and NERC and requests ATL notify all Audit Team members to destroy all audit documents and electronic files from their computers
- ATL notifies Audit Team members to destroy all audit documents and electronic files related to the audit and to confirm destruction
 - Notification is made by email and requires both Receive and Read Receipts
- Audit Team members will destroy all audit related documents and files and acknowledge completion of destruction to ATL
- ATL will notify MCA of completion of document destruction

NOTE: NERC will send non-public audit reports to FERC as informational submittals, not a public filing.

Public Audit Report Processing

- **IF** the final Audit Report **DOES NOT** identify any possible violations:
 - The MCA, or his designee, will process the final Non-Public Audit Report to:
 - Redact all confidential, privileged and/or critical energy infrastructure information from the Non-Public Audit Report,
 - Remove cover page statements, all watermarks and header markings indicating that the report is Non-Public
 - Identify the report as “Public Audit Report” and “Confidential Information (Including Privileged and Critical Energy Infrastructure Information) Has Been Removed”
 - The MCA will forward the Public Audit Report and Transmittal Letter to the CD for final approval
- The CD will endorse the report as being the approved Public Audit Report and will forward the approved report to the EA
- The EA will record the date of report approval in the Tracking Database
- The EA will forward a copy of the approved Public Audit Report to the entity and to NERC
 - The EA will record the date the report was forwarded to the entity and NERC in the Tracking Database and save a copy of the email on the S: drive.
 - The EA will save a copy of the Public Report to the S drive
- NERC will review the Public Audit report and will, five days from receipt, post the report on the NERC website
 - NERC will forward the Public Audit report to FERC as a public filing
- **IF** the final Audit Report **DOES** identify possible violation(s), the final Non-Public Audit Report **WILL NOT** be converted to a Public Audit Report until all possible violation(s) are fully processed through the Regional Entity’s CMEP process described in CMEP Implementation Procedure 5.0, Consolidated Compliance Tracking.
- When disposition of all Alleged Violations have been verified complete, the Compliance Enforcement Manager (CEM) will Notify the MCA that all Alleged Violations have been disposition and that the Non-Public Audit Report is to be converted to a Public Audit Report and forwarded to NERC and the entity
 - The MCA will record the date of CEM notification of completion of possible violation processing in the Tracking Database
- The EA will process the Non-Public Audit Report to:
 - Redact all confidential, privileged and/or critical energy infrastructure information from the Non-Public Audit Report,
 - Remove cover page statements, all watermarks and header markings indicating that the report is Non-Public

SERC CMEP Implementation Procedure 3.1: Compliance Audits

- Identify the report as “Public Audit Report” and “Confidential Information (Including Privileged and Critical Energy Infrastructure Information) Has Been Removed”
- The EA will forward the Public Audit Report, Transmittal Letter, Registered Entity Comment Letter, if applicable, and Procedural Summary to the CD for final approval
 - The EA will record the date the report was forwarded to the CD in the Tracking Database and save a copy of the email to the S drive.
- The CD will endorse the report as being the approved Public Audit Report and will forward the approved report to the MCA/EA
 - The EA will record the date of report approval in the Tracking Database
- The EA will forward a copy of the Public Report to the entity and to NERC
 - The EA will record the date the report was forwarded to the entity and NERC in the Tracking Database.
 - The EA will save a copy of the Public Report in both Word and PDF formats to the S drive
 - The EA will save a copy of the email to the S drive
- NERC will review the Public Audit report and will, five days from receipt, post the report on the NERC website
 - NERC will forward the Public Audit Report to FERC as a public filing

4.2 Audit Conduct

4.2.1. Entrance Briefing

ATL leads an entrance briefing that covers:

- Team composition (company, experience, role on team),
- Objective of the audit,
- Expected behaviors for audit team and entity staff,
- Standards considered in-scope to the audit,
- Any specific team focus areas based on advance review,
- Expected audit duration and Registered Entity support required,
- Expected timing of the exit briefing,
- Reliability Standards Audit Worksheets updated with advanced information.

4.2.2. Team Focus / Assignments

- ATL defines team member accountability for audit of specific standards and requirements.
- ATL ensures team resources are allocated commensurate with relative importance of individual audit areas based on actual / potential impact to Bulk Electric System (BES).

SERC CMEP Implementation Procedure 3.1: Compliance Audits

- ATL stresses the need for team members to obtain objective evidence, to the extent practical, in support of determination of compliance / noncompliance for each standard

4.2.3. Completion of Reliability Standard Audit Worksheets (RSAWs)(Q/Rs)

- Team members interface with entity staff, review documents and displays, and take other actions needed to complete Q/Rs for assigned Reliability Standards.
- In those cases where approved RSAWs (Q/Rs) are not available, regional audit guidelines will be used, as appropriate, to promote consistent audits of involved standards.
- The audit team shall ensure that each document reviewed by the team as evidence is accurately and fully documented to identify, as applicable:
 - Document title
 - Document date
 - Document effective date, if applicable
 - Approving signatory
 - Section number of relevant evidence, if applicable
 - Page number of relevant evidence,
 - Other applicable forms of document identification, and
 - Description of Requirement or portion of Requirement evidenced by the identified statement(s).
- The ATL (or his designee) and audit team members shall ensure that all audit documentation is maintained secure and confidential in accordance with SERC Implementation Procedure 9.0. SERC will provide and password protect a secure flash drive for storage of all audit evidence.

4.2.4. Evidence Retention

- The ATL and audit team shall obtain and retain a copy (in electronic format if possible) of all evidence of compliance presented by an entity.
 - Retention of complete document(s) is not required for standards for which the entity is determined compliant. Retain only the document identification information (Cover page with document title, date, effective date and approving signature) and the section(s) and/or page(s) of the document that provide evidence of compliance.
 - Copies of all evidence provided (in electronic format if possible) in relation to a standard for which the entity is found to be in possible violation / non-compliance shall be retained in full (complete document(s)).

4.2.5. Daily Updates

- ATL arranges daily updates with key entity staff, as required, to review status of developing potential noncompliance / possible violation, and to seek added information / clarification.

SERC CMEP Implementation Procedure 3.1: Compliance Audits

- ATL solicits team input on any topic requiring prompt action by the team / entity with respect to potential noncompliance / possible violations identified (relevance to remedial action directives or standards requiring reporting within 48 hour of determination of possible violation).

4.2.6. Team Interaction

- ATL interacts with team members to ensure completion of audit worksheets and to resolve any conflicts.
- ATL solicits team feedback on areas of potential noncompliance or possible violations.
- ATL determines areas of potential noncompliance or possible violations.

4.2.7. Exit Briefing

- ATL conducts an exit briefing that summarizes the team's preliminary conclusions, including any items of potential noncompliance or possible violation with supporting information, areas of concern, any added information required, and the expected timeline for review and issuance of the audit report.
- ATL solicits Registered Entity feedback on any errors or fact, omissions, or other information key to the team's determinations of potential noncompliance / possible violations.

Registered Entity:

The Registered Entity is requested to provide feedback to SERC within 14 business days.

4.3 Post-Exit Actions

- ATL completes a Screening Worksheet for each potential noncompliance / possible violations identified by the team and forwards to the current Screener for entry into the SERC compliance tracking database.
- ATL clearly communicates any in-scope standards that were not fully addressed to allow for follow-up as needed.
- ATL has assigned auditor draft an audit report and arranges for team and Registered Entity review.
- As part of the Exit presentation, a non-binding list of concerns is provided to the Registered Entity by the audit team.
- ATL considers comments received and redrafts Non-Public Audit Reports for MCA approval.
- MCA reviews and redacts Security Sensitive Information from Non-Public Audit Reports. MCA ensures that all "Critical Infrastructure Protection" and other sensitive information are appropriately redacted.
- MCA forwards the Draft Public Audit Reports to the Director of Compliance for review, approval and distribution.

SERC CMEP Implementation Procedure 3.1: Compliance Audits

- A copy of final audit reports forwarded to the Registered Entity and NERC.

NOTE: The final report will not be made public until any Possible Violations are fully settled.

- EA converts the final report to PDF format and transfers a copy and any associated work products to SERC for retention.

4.4 **Unscheduled Audits**

- An unscheduled audit can be conducted if it is reasonably determined to be necessary as concluded by the Compliance Director (CD).
- If the CD determines an unscheduled audit to be reasonably necessary, the CD will notify NERC and FERC (unless NERC prefers to notify FERC, which is normally the case) of the intent to perform an unscheduled audit including the basis, the Registered Entity involved, the scope of the audit, and the schedule (including preparation milestones).
- The CD will direct the MCA to conduct the unscheduled audit.
- The MCA notifies the Registered Entity of its intent to conduct an unscheduled audit.
- In the event of an unscheduled audit, the general sequence described in section 4.1 above will be preserved but under a compressed timeframe.
- The MCA will review notification / start dates to ensure appropriate balance between the benefit of conducting the unscheduled audit and appropriate entity notification to allow for objection to team composition.
- The MCA will notify the Registered Entity at least ten (10) business days in advance that an unscheduled audit is being initiated. This notice will include identification of the audit team members.

Registered Entity:

The Registered Entity may object to the composition of the audit team on the grounds of a conflict of interest or the existence of other circumstances that could interfere with a team member's impartial performance of his or her duties. Objections must be made at least five (5) business days prior to the start of the on-site audit work. Detailed information on Objections is provided in the SERC CMEP Section 3.1.