

**SERC**

**Compliance Enforcement Plan**

**Southeastern Electric Reliability Council**

**Revision 18: November 30, 2006**

**EFFECTIVE AS OF JANUARY 1, 2007**

**Approved by SERC Executive Committee  
November 30, 2006**

## Revision History

Revisio n	Date	Comments
0	9-1-1999	Original Issue
1	3-30-2000	Revision 1
2	10-6-2000	Revision 2
3	12-28-2000	Revision 3
4	2-26-2001	Revision 4
5	11-30-2001	Revision 5
6	1-31-2002	Revision 6
7	11-22-2002	<p>Initiated Revision History</p> <p>Changed the name of the plan from “SERC Compliance Program Implementation Plan” to “SERC Compliance Enforcement Plan”</p> <p>Updated Appendix A with the list of standards to be monitored in 2003</p> <p>Updated Appendix B with the list of standards to be monitored in 2003</p> <p>Added Appendix H - ADR Process</p> <p>Modified Appendix D - Mitigation Plan process</p> <p>Modified Appendix G – Audit Process</p> <p>Modified Appendix I – NERC Penalties for Non-Compliance</p> <p>Added confidentiality language</p> <p>Other minor changes</p>
8	1-22-2003	Finalized revision 7 based on comments received and submitted as version 8 to the COG for approval.
9	11-17-2003	<p>Revised Appendix A for 2004 measures</p> <p>Revised Appendix F for filing requirements changes</p> <p>Revised Appendix G and E</p> <p>Revisions to include Cyber Security Compliance in the process.</p> <p>Added Appendix J –Cyber Security Standards</p> <p>Added description of web-based database filing information in Process section.</p> <p>Other minor changes</p>
10	1-27-2004	<p>Revised Appendix A – revised table and text.</p> <p>Revised Appendix G to add EIA 417 review determine if an investigation is necessary.</p> <p>Appendix D – revised mitigation process.</p> <p>Appendix B – Operating Policies. Revised to address measures subject to audit.</p>
11	May 24, 2004	<p>Revised Introduction, added a section on ,"<u>Commitment to the Contractual Compliance Program.</u>"</p> <p>Revised Appendix G (Para. A8) to modify new control are start up requirements.</p> <p>Revised Appendices A and B to include new measures in the revised 2004 program.</p> <p>Added new Appendix K to address reporting requirement to NERC.</p>
12	December 27, 2004	<ol style="list-style-type: none"> <li>1. Addressed auditor independence in Appendix G</li> <li>2. Added Mitigation Closure form to Appendix D</li> </ol>

		<ol style="list-style-type: none"> <li>3. Added criteria for including Independent Power Producers in the compliance program to the Overview.</li> <li>4. Revised Appendix A and B tables to include measures for 2005.</li> <li>5. Revised Appendix K – procedures for reporting violations to NERC to reflect the SERC – NERC agreement and SERC 48 hour reporting rules.</li> </ol>
13	February 4, 2005	<ol style="list-style-type: none"> <li>1. In general changed 2004 to 2005 where appropriate.</li> <li>2. Revisions to the Process section.</li> <li>3. Dropped the Appendix A text from the plan.</li> <li>4. Modified Appendix A table to reference SERC Supplements and drop the measures in the table that will not be a part of version 0.</li> <li>5. Revised Appendix K to address opportunity to make a statement to NERC.</li> <li>6. Appendix I revised to address RCEP.</li> <li>7. Revisions to the timeliness penalties.</li> <li>8. Updated Appendix F to match the Portal.</li> </ol>
14	March 11, 2005	<ol style="list-style-type: none"> <li>1. Revised Appendix K – SERC Procedure for Reporting Violations to NERC</li> <li>2. Appendix A table – IVAM1 not in the 2005 program. Dropped from the table.</li> </ol>
15	December 13, 2005	<ol style="list-style-type: none"> <li>1. Addition of a Cross Reference Matrix To Key Compliance Elements</li> <li>2. Updated Introduction, Background, and Process sections, including Attachments 1 and 2.</li> <li>3. Appendix A – Revised the Planning Standards Measurements for 2006 Compliance Plan, dropped the previous standard designations.</li> <li>4. Appendix B - Revised the Operating Standards Measurements for 2006 Compliance Plan, dropped the previous operating policy designations, and incorporated the current titles for the reliability standards.</li> <li>5. Updated Appendices D, E, F</li> <li>6. Appendix G – Updated the appendix, clarified the timeline for additional materials to be provided in an audit.</li> <li>7. Appendix H – added Executive Signatory to appeal process, added opportunity for oral presentation in appeal to the COG.</li> <li>8. Revised Appendix K – SERC Procedure for Reporting Violations to NERC</li> </ol>
15a	January 19, 2006	<ol style="list-style-type: none"> <li>1. Revised Compliance Manager contact information on page 6.</li> <li>2. Updated flowcharts to current committee designations.</li> <li>3. Replaced Security Coordinator with Reliability Coordinator.</li> </ol>
16	March 20, 2006	<ol style="list-style-type: none"> <li>1. Revision to shift MOD-001 to 009 and PRC-001 from Appendix A to Appendix B.</li> </ol>
17	May 31, 2006	<ol style="list-style-type: none"> <li>1. Appendix A and B to accommodate revision of standards during the compliance program. Reference D. Hilt’s letter of</li> </ol>

		<p>May 31, 2006.</p> <ol style="list-style-type: none"> <li>2. Corrected FAC-002 SERC Supplement column and other minor changes..</li> <li>3. Revised Appendix J to include new Cyber Standards.</li> <li>4. Revised Appendix I to field test ERO Sanction Guidelines</li> </ol>
18	November 16, 2006	<ol style="list-style-type: none"> <li>1. Editorial and style changes ; clarified wording throughout document</li> <li>2. Revised Appendix A, B, and J to reflect 2007 active monitoring of effective standards and indicate the method of compliance monitoring</li> <li>3. Revised Appendix I concerning field test of Sanctions and Penalties Guidelines.</li> </ol>

## **SERC Compliance Enforcement Plan**

Introduction	7
Background	7
Overview	7
Cyber Security Standards	8
Commitment to the Contractual Regional Compliance Enforcement Program (RCEP)	8
Process	8
Attachment 1 - SERC Compliance Review Process Flowchart	11
Attachment 2 - SERC Compliance Review Process Description	13
Appendix A – Planning Standards	17
Appendix B – Operating Standards	21
Appendix C – SERC Planning Standards Data Submittal Information Processes	26
Attachment 3 – Regional Bulk Submittals	27
Attachment 4 – Regional Document Submittal	28
Appendix D – SERC Mitigation Process	29
Attachment 5 – Mitigation Process Flowchart	32
Appendix E – SERC Late Data Submittal Process	33
Appendix F – Compliance Program Filing Format Requirements	36
Appendix G – SERC Audit Procedures	40
Attachment 6 – Audit Process	48
Appendix H - Appeals and Alternate Dispute Resolution Process	49
Attachment 7 – Appeals and Alternate Dispute Resolution Process Flowchart	53
Appendix I – NERC Penalties for Non-Compliance	54
Appendix J – Cyber Security Standards Measurements	58
Appendix K – SERC Procedure for Reporting Compliance Violations to NERC.	60

## Cross Reference Matrix of Key Compliance Elements

<b>Key Compliance Elements</b>	<b>SERC</b>
Applicable Plan	Rev 18 dated November 17, 2006
Defined Compliance Process that includes monitoring of standards in the NERC annual program as a minimum.	Pages 6-25 including Attachment 1 and 2, and Appendix A & B
Mitigation Process for all violations that includes a schedule for completion	Appendix D - Page 29
Dispute Resolution Process	Appendix H – Page 49
Processes and procedures that insure consistent compliance rulings	Attachment 2 Box 11 Page 12 Attachment 2 Box 13 Page 12 Appendix G – Section A Page 42
Audit program with defined team make up criteria for diversity in all audits	Appendix G - Page 43
Processes for conducting investigations	Appendix G - Page 45
Spot check processes.	Appendix G - Page 47
Procedures for disclosure of compliance violations to NERC	Process section - Page 8 and Appendix K – Page 60
Inclusion of penalties for non-compliance (either NERC or other)	Appendix I - Page 54
OPTIONAL - Provision for a contractual regional CEP with enforceable penalties	Commitment to RCEP - Page 8

## **Introduction**

This compliance enforcement plan (CEP) addresses the compliance program that will be used to ensure that SERC and its members are in compliance with the NERC Reliability Standards. It defines accountability, expectations for compliance, mitigation for non-compliance, reporting relationships, process flow, audit procedure, an appeals process, a dispute resolution process, and the steps to be taken to report non-compliances to NERC. This document will be updated as necessary in the course of the program and, along with other documents, self-certification and other forms, reports, schedules, etc. associated with the compliance monitoring and assessment process will be posted on the SERC Website at [www.serc1.org](http://www.serc1.org).

The SERC Compliance Manager, in conjunction with the SERC Compliance Review Steering Committee (CRSC), the SERC Compliance Subcommittee (CS), and the Cyber Security Compliance Review Subcommittee (CSCRS), will be responsible for the update and maintenance of this program. The SERC Compliance Oversight Group (COG) is responsible for final approval of non-compliances, assessing penalties, and determining policy related to the overall SERC compliance program. The Compliance Enforcement Plan (CEP) is approved by the SERC Executive Committee. The single point of contact for the SERC Compliance Program is the SERC Compliance Manager. He can be contacted by calling the SERC office at 205-257-6407.

## **Background**

The SERC implementation plan assumes that the regions will have primary responsibility for ensuring compliance to the standards by all users of the interconnected transmission systems. It is recognized that the organizational structure of NERC and the Regional Reliability Councils are under review and will be changed in the near future. This SERC CEP will be replaced with a new annual plan to address the requirements of the Delegation Agreement and will go into effect at the time the delegation agreement is approved by FERC.

## **Overview**

The overall review process is shown on a flowchart in Attachment 1. Further description of the activities is outlined in Attachment 2, which presents the basic program concepts, delineates actions required and assigns responsibility for each step of the process. The process provides that SERC will have the responsibility to promote, support, and comply with the purposes and policies of NERC. SERC has adopted the NERC Reliability Standards, which provide the primary requirements for the SERC Compliance program. To fulfill the regional filing requirements to NERC, SERC will solicit the necessary information from reporting entities via letters of certification, reporting forms, etc. However, some of the NERC Standards do not require reporting entities to supply all the information necessary for SERC to fulfill Regional requirements to NERC. In these instances, SERC will also solicit the necessary information from reporting entities via letters of certification, reporting forms, etc. Where necessary SERC Compliance Templates have been developed to support the regional filings to NERC. Reporting entities are expected to fulfill these additional data requests. In addition, SERC Supplements/Procedures to some of the standards have been developed which include specific member compliance requirements. These supplements/procedures are available on the SERC website.

Member filing requirements for the Planning Standards and for the Operating Standards are contained in Appendices A and B respectively, and in the document "SERC 2007 Compliance Filing Requirements" (available on SERC website). Independent Power Producers (IPP) are subject to being included in the Compliance Filing Requirements document if they have an interconnection agreement and have started commercial operation. The Appendices will be modified as necessary during the compliance year. A schedule that shows timeframes, milestones, and key dates needed to meet the deadlines set by the NERC Compliance Program is included in the spreadsheet document: "SERC 2007 Compliance Program Matrix" (available on the SERC website). The Program Matrix document will be updated as necessary. The compliance program schedule will be posted on the SERC Portal homepage for each master account.

### **Cyber Security Standards**

Cyber Security Standards were approved by the NERC Board on an urgent basis August 13, 2003. They have been re-approved for 2007 and will continue to have a limited compliance program. Reporting by the appropriate entities will be in accordance with Tables 1-3 in the implementation plan

Compliance with the standard will be used to determine the overall level of cyber security preparedness in the industry. Individual self-certification results will be reported by SERC to NERC. This data will illustrate whether the industry is substantially compliant with the standard

### **Commitment to the Contractual Regional Compliance Enforcement Program (RCEP) and Obligations of the Entities Assessed**

**The following paragraph applies only to those members who have signed the SERC Contractual Agreement.**

The SERC Board of Directors approved a Regional Compliance Enforcement Program (RCEP) on April 28, 2004. Those SERC member entities who have signed the RCEP are known as Participating Compliance Entities. These Participating Compliance Entities agree to accept sanctions for failure to comply with certain Designated Reliability Standards that may be more stringent than sanctions applicable to other members of SERC. The Designated Reliability Standards (DRS) in the 2007 Regional Compliance Enforcement Program are identified in Appendix B of this document. More details about the voluntary RCEP are found in the "Agreement Between Southeastern Electric Reliability Council and its Members for Regional Compliance and Enforcement Programs" document (available on the SERC website). Procedures for amending this Compliance Enforcement Plan per article IV. 3. are provided in Attachment 2 Box 1 of this document.

### **Process**

Compliance monitoring will be accomplished by peer team audits, spot reviews, investigations, and committee reviews of self assessments, letters of certification, and data submittals. Operating and Planning audits will be conducted to ensure each responsible entity is audited in accordance with NERC Standards, including SERC Supplements, and at the intervals required. Audit teams will consist of experienced personnel from member systems. SERC may elect to utilize independent auditors for some or all audits to facilitate staffing of audit teams and to ensure an unbiased and consistent compliance monitoring program.

Self-assessment forms and reporting timetables will be modified as revisions are made to the Reliability Standards. Lessons learned from prior years will be utilized to improve the current year's program. The SERC Office will schedule an annual Compliance Seminar to keep members abreast of compliance requirements. Reporting timetables and plans will be communicated to members at the annual seminar, and by e-mail. This information will be maintained and posted on the SERC Portal for each entity that has a master account. Compliance filings will be made on-line via web-based forms. The information will be stored in a secure database.

All compliance assessment data, information, reports and records will be maintained by the SERC Staff on a confidential basis in accordance with the SERC Policy Regarding the Confidentiality of Data Submitted by SERC Members. The on-line database will be located at a secure site managed by a SERC-selected vendor. Access to this information will be restricted to members of the CRSC, CS, CSCRS, COG, Region Review Groups, Responsible SERC subgroups, Audit Teams, and SERC Staff. Access to compliance status reports to NERC will be in accordance with Appendix K. Release of information designated confidential will be in accordance with the SERC Policy Regarding the Confidentiality of Data Submitted by SERC Members and the SERC Agreement Regarding Disclosure dated November 1, 2004.

Compliance Program data/information will be stored electronically. All compliance submittals will be via the web-based forms. Authorization signatures by company officer(s) can be submitted on summary report cover letters. These reports can be downloaded in either Microsoft Word or Acrobat PDF or printed directly from the web-based system. Authorization signatures on summary report cover letters may be submitted electronically via email ([support@serc1.org](mailto:support@serc1.org)) or as a paper copy sent directly (fax or US mail) to the SERC Office. The submittals will be stored in electronic form with a few exceptions, such as maps, etc., that may only be available in a paper form. These exceptions are few and will be established on a case by case basis. The database will allow for automatic processing of submittals without placing an undue burden on the submitting entities. The instructions for filing submittals are outlined in Appendix F.

The SERC Compliance Program uses the NERC Penalty/Enforcement Matrix; however, monetary penalties/sanctions are not currently assessed, with the exception of the Designated Reliability Standards for Participating Compliance Entities. Letters will be sent to non-compliant members and to the SERC committees. Members will, however, be notified of the penalties/sanctions that would have resulted if the program had financial penalties been in effect. Violations of NERC standards will be provided to NERC in accordance with the NERC procedures.

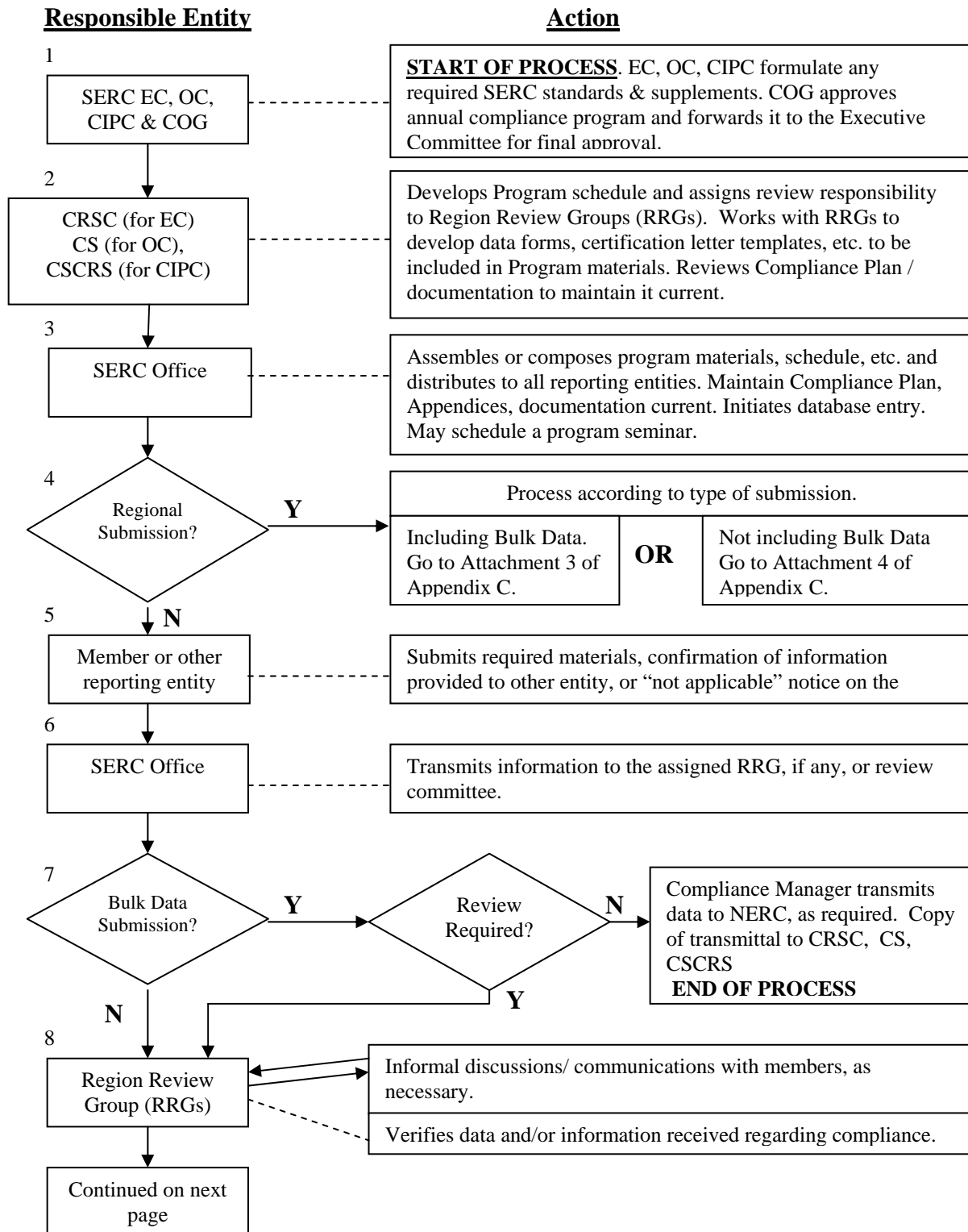
The SERC Compliance Review Steering Committee (CRSC) and the Compliance Subcommittee (CS) have developed a Late Submittal Process to meet NERC's requirements. The Late Data Submittal Process is shown in Appendix E.

Mitigation for non-compliance will be closely monitored by the CRSC, CS, COG and the SERC Compliance Manager to ensure plans are sufficient for achieving compliance. Mitigation is described in Appendix D.

Members who have questions regarding the Compliance Program or specific compliance measurements can send them to the SERC Compliance Manager. The SERC Compliance Manager will be responsible for obtaining answers to the questions (which may involve consultation with the CRSC, the CS, or CSCRS) and communicating them back to the affected members.

**SERC COMPLIANCE REVIEW PROCESS**

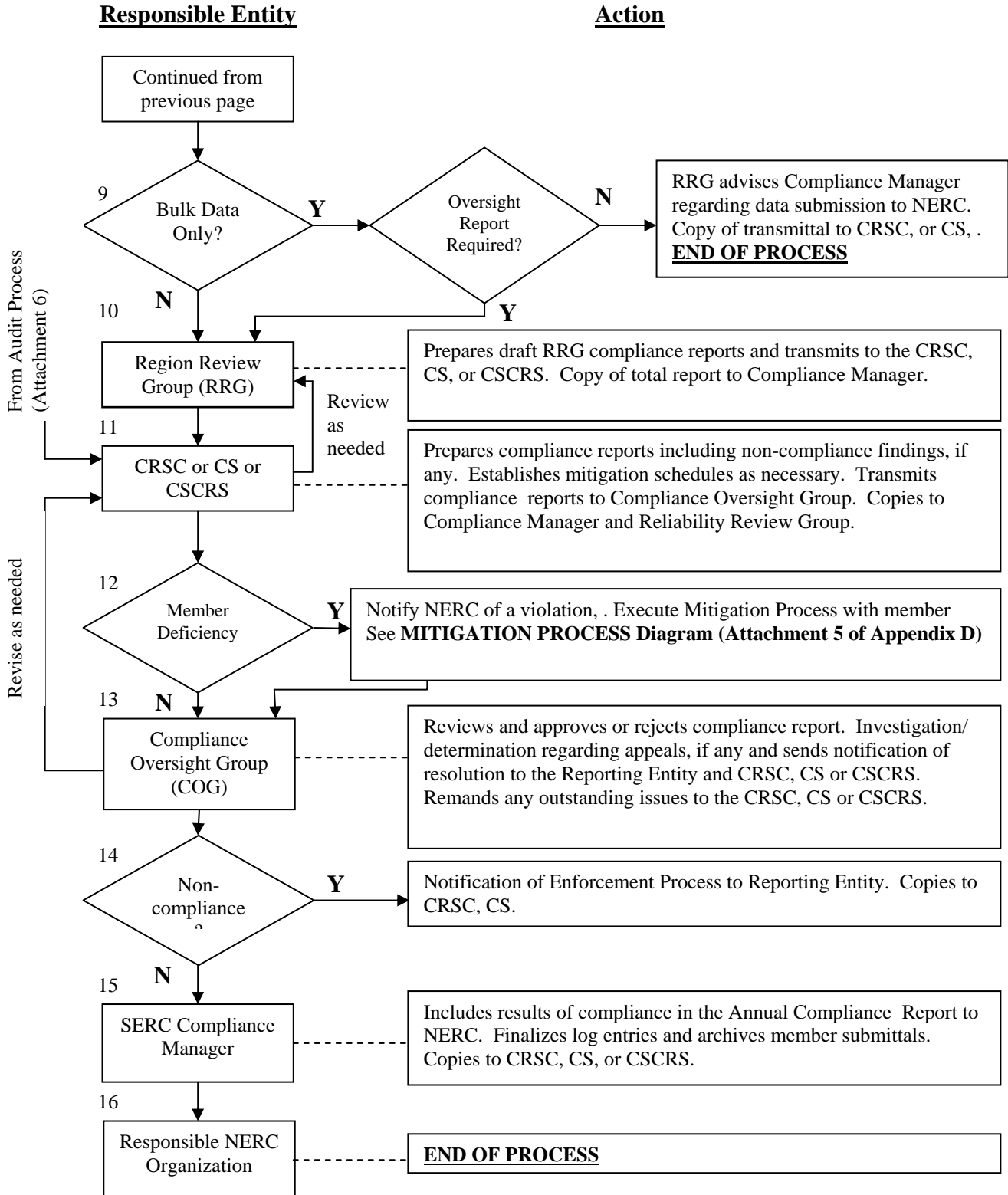
**PROCESS REVIEW DIAGRAM – PAGE 1 OF 2**



**Attachment 1**

**SERC COMPLIANCE REVIEW PROCESS**

**PROCESS REVIEW DIAGRAM – PAGE 2 OF 2**



## **Attachment 2**

### **Overview of SERC Compliance Review Process**

The following is a summary of the activities identified in Attachment 1:

#### **Box 1. SERC Engineering Committee (EC), Operating Committee (OC), Cyber Security Compliance Review Subcommittee (CSCRS) and Compliance Oversight Group (COG)**

In those cases where the NERC Standards require additions or a regional program, appropriate SERC Supplements will be developed by the EC, OC, or CIPC. These SERC Supplements must be:

- Specific, measurable, adequate, and appropriate,
- Written in such a manner that they are clearly understood and enforceable,
- Free of unnecessary barriers to commercial activity,
- Clear in defining what constitutes non-compliance, and
- Consistent, with appropriate differences between the Sub-Regions.

All market participants conducting business in the SERC Region shall have the opportunity to be members of SERC and to participate in the development of reliability standards.

At this time, SERC has adopted the NERC Reliability Standards

For changes to those portions of the plan that address the SERC RCEP, 30 days notice will be provided to the Participating Compliance Entities, with an opportunity to comment to the Compliance Oversight Group (COG) prior to any final action. The COG approves the plan, and forwards it to the Executive Committee for approval.

In the absence of any amendments that address the SERC RCEP, the Compliance Oversight Group (COG) reviews, makes any changes it determines are needed, and approves the annual Compliance Enforcement Plan and forwards it to the Executive Committee for final approval.

#### **Box 2. CRSC (for EC), CS (for OC), and CSCRS (for CIPC)**

Compliance Review Steering Committee (CRSC) or Compliance Subcommittee (CS) will assign the NERC Standards to existing subcommittees and working groups who will act as the Region Review Group (RRG). RRGs are responsible for the review of compliance submittals associated with their assigned NERC standard. The representatives on these groups are selected from the SERC members based on their knowledge and current work assignments. The representation is distributed among the SERC members, in accordance with the scope documents of the appropriate committees. When a representative's company is being assessed, that representative will not participate in the decision. SERC will use the experience learned in the compliance reviews to determine reviewer qualifications.

The current SERC RRGs may include:

- Operating Committee - Audit Teams, Compliance Subcommittee, Resource Team, Operations Planning Subcommittee(OPS), and SERC Staff.
- Engineering Committee – Audit Teams, Compliance Review Steering Committee (CRSC), Reliability Review Subcommittee (RRS), Available Transfer Capability Working Group (ATCWG), Protection and Control Subcommittee (PCS), Operations Planning Subcommittee(OPS), SERC Representative to the NERC MMWG, Stability Database Working Group(SDWG), and SERC Staff.

CRSC and CS will work with RRGs to develop data forms, certification letter templates, etc., to be included in program materials.

The SERC Critical Infrastructure Protection Committee (CIPC) assigns responsibility for assessing compliance to the Cyber Security Standards to the Cyber Security Compliance Review Subcommittee (CSCRS). The CSCRS functions as a region review group or may assign portions of the review to individual RRG's that report to it.

The schedule for the compliance program will be developed by the appropriate compliance committees, taking into account NERC's schedule..

**Box 3. SERC Office**

SERC has the responsibility to notify its members and users of the bulk electric system of the applicable standards for which compliance is required. Members will be provided a copy of the document "SERC Compliance Filing Requirements" which lists filing dates and which measurements apply to each member. This document will also be posted on the SERC website.

SERC may schedule a Compliance Program Seminar to inform members of compliance requirements.

**Box 4. Regional submission?**

Each measurement is processed according to the type of submission that is specified in the Compliance Program document. Generally, individual SERC members will be the responsible entity, but some measures will require SERC committees, working groups, or SERC representatives to NERC groups to submit reports, data and/or assessments.

If the requirement is for a regional submission and the submittal contains bulk data, go to Attachment 3 of Appendix C. If the requirement is for a regional submission and does not include bulk data, go to Attachment 4 of Appendix C. If the measurement does not apply to the region, continue to Box 5.

**Box 5. Member or other reporting entity**

Members or other reporting entities are required to provide data, conduct requisite analysis, and report the results of reliability assessments to the Region, as appropriate. If they think or believe (pick one) a measure is not applicable to them, a submittal is still required with the appropriate check box marked and justification provided. Members and reporting entities will make their submittals in electronic form. Appendix A, B, and J explain how each measure will be assessed.

**Box 6. SERC Office**

The member or other reporting entity submits the required material on the SERC Portal. A report of the information received is transmitted to the assigned RRG, or compliance review committee.

**Box 7. Bulk data submission?**

If the submittal contains bulk data and no review is required, the Compliance Manager (or SERC staff) transmits the data to NERC as required. A copy of the transmittal is sent to the CRSC or CS. This completes the compliance filing process for that measure.

If the submittal does not contain bulk data or if a review is required, continue to Box 8.

**Box 8. Region Review Group (RRG)**

RRGs compile responses, verify data and information and reconcile any differences, errors, or omissions. Informal discussions and communications are held with members as necessary. RRGs will identify deficiencies, if any.

**Box 9. Bulk Data Only?**

If the submittal contains bulk data only and no oversight report is required then the RRGs advise the Compliance Manager regarding data submission to NERC. A copy is transmitted to the CRSC or CS. This completes the compliance filing process for that measure.

If the submittal does not contain bulk data only or an oversight report is required, continue to Box 10.

**Box 10. Region Review Group (RRG)**

As input to the SERC Compliance Process, each identified RRG has the responsibility to provide a report on its compliance findings. The RRG Compliance Report will provide results of its compliance reviews including recommendations of non-compliance and will be forwarded to the CRSC, CS, or CSCRS and copied to the Compliance Manager.

**Box 11. CRSC, CS, and CSCRS**

The CRSC, CS, and CSCRS is responsible for overseeing the compliance process by reviewing inputs from the following:

- Region Review Group (in the case of an audit, the Audit Team) reports on assessments of member compliance,
- Regional member compliance submittals,
- Reports on data assessments,
- Audits, and
- Investigations.

The CRSC or CS may perform an independent review to ensure compliance with any of the NERC Standards.

The CRSC, CS, or CSCRS will prepare a compliance report including deficiency findings, if any. Mitigation schedules will be established as necessary. The compliance report will be transmitted to the Compliance Oversight Group (COG) and copies sent to the Compliance Manager and the Region Review Group. With regard to cyber security standards, no non-compliance letters will be issued so formal mitigation plans will not be requested.

**Box 12. Member Deficiency?**

The CRSC or CS may also define deficiencies for reporting entities. First, the CRSC or CS may identify deficiencies in the assessments or in the compliance reviews. Second, the CRSC or CS may identify deficiencies in the compliance processes. Any assessment of deficiency by the CRSC or CS responsible for overseeing the compliance process will document the deficiency as well as expectations required to attain compliance. In 2007 the CSCRS will not conduct member deficiency assessments. The CSCRS may identify deficiencies in the compliance process.

If the CRSC or CS determines that the entity is deficient, execute the mitigation process, see Attachment 5 of Appendix D.

If the CRSC or CS determines that the member is compliant, go to Box 13.

**Box 13. Compliance Oversight Group (COG)**

The SERC Compliance Oversight Group is made up of the SERC Engineering Committee and SERC Operating Committee officers, the SERC Compliance Review Steering Committee Chair and Co-Chair,

the SERC Compliance Subcommittee Chair and vice Chair, the Critical Infrastructure Protection Committee Chair and Vice- Chair, the Cyber Security Compliance Review Subcommittee Chair and Vice-Chair, the SERC Compliance Manager, and the SERC President. The COG reviews and approves, or rejects the Oversight Report. If it is rejected, the report will be will sent back to the CRSC, CS, or CSCRS for further development.

The COG will investigate audit reports and make determinations regarding appeals in accordance with the Alternate Disputes Resolution Process in Appendix H. The Compliance Manager sends notification of resolution to the Reporting Entity and CRSC or CS. Any outstanding issues will be sent to the CRSC or CS.

If the SERC Compliance Oversight Group agrees with the findings of the CRSC or CS, go to Box 14. If the SERC Compliance Oversight Group does not agree with the findings of the CRSC or CS, go to Box 11 for further consideration.

**Box 14. Non-Compliance?**

Notification of the enforcement process will be sent to the non-compliant entity. The focus of the Compliance Process is on reliability assurance, and achieving compliance with the NERC Standards. The Enforcement Process is not a buy-through on reliability that relieves a Region/market participant from compliance.

The SERC President will send a formal letter to entities that are non-compliant. The letter will specify each measurement where non-compliance has been found, the level of non-compliance, a justification for the rating, and the penalty/sanction being imposed. For members who have signed the RCEP (see page 8), financial penalties will be imposed. For members who have not signed the RCEP, the letter will specify the penalties that would have been imposed had they been enforceable, The SERC Compliance Oversight Group has the final responsibility and authority for issuing compliance recognition, penalties or sanctions.

**Box 15. SERC Compliance Manager**

The SERC office includes the results of compliance assessments in the regional reports to NERC. Copies will be transmitted to the COG.. Database entries are finalized and Reporting Entity submittals are archived.

**Box 16. END OF PROCESS**

Reset periodic review timer.

# **Appendix A**

## **Planning Standards**

## APPENDIX A – PLANNING STANDARDS

. The table below provides a summary of the requirements SERC will monitor in the compliance program.. A standard is monitored for compliance by letters of certification and / or reporting forms that provide data for compliance assessments. Refer to the Compliance Filing Requirements documents on the [www.serc1.org](http://www.serc1.org) website for the measures each entity is required to file. In the event of a conflict, the Compliance Filing Requirements document takes precedence over this Appendix A. The measures shown with shading are regional measures in which SERC is monitored by NERC. The table below provides a summary of the standards monitored in the current year program. The version in effect at the time it is monitored is the version assessed for compliance.

All the standards in effect are listed on the NERC website at –

[http://www.nerc.com/~filez/standards/Reliability\\_Standards.html](http://www.nerc.com/~filez/standards/Reliability_Standards.html).

Refer to this website for the latest version and the effective date of the requirements. ALL REQUIREMENTS IN ALL STANDARDS IN EFFECT ARE SUBJECT TO AUDIT.

<b>Std #</b>	<b>Requirements</b>	<b>Standard</b>	<b>Applicable to</b>	<b>Purpose</b>	<b>Self-Certification</b>	<b>Monthly/Quarterly Reporting</b>	<b>Data Submission</b>	<b>Exception Reporting</b>	<b>Investigation</b>
FAC-003-1	All	<b>Vegetation Management</b>	TO	To improve the reliability of the electric transmission systems by preventing outages from vegetation located on transmission rights-of-way (ROW) and minimizing outages from vegetation located adjacent to ROW, maintaining clearances between transmission lines	√	Q			
FAC-008-1	All	<b>Facility Ratings Methodology</b>	GO, TO	To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on an established methodology	√				

FAC-009-1	All	<b>Establish and Communicate Facility Ratings</b>	GO, TO	To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.	√				
PRC-004-1	All	<b>Analysis and Mitigation of Transmission and Generation Protection System Misoperations</b>	DP*, GO, TO	Provide trip operation / misoperation information per Regional process	√		√		
PRC-005-1	All	<b>Transmission and Generation Protection System Maintenance and Testing</b>	DP*, GO, TO	Document/implement transmission protection system maintenance/testing/monitoring PROGRAM	√				
PRC-008-0	All	<b>Implementation and Documentation of Underfrequency Load Shedding Equipment Maintenance Program</b>	DP, TO	Document/implement UFLS maintenance/testing PROGRAM	√				
PRC-010-0	All	<b>Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program.</b>	DP, LSE, TO, TOP	ASSESS design and effectiveness of UVLS programs	√				
PRC-011-0	All	<b>UVLS System Maintenance and Testing</b>	DP, TO	Document/implement UVLS maintenance/testing PROGRAM	√				
PRC-016-0	All	<b>Special Protection System Misoperations</b>	DP, GO, TO	DOCUMENT/analyze misoperations	√		√		
PRC-017-0	All	<b>Special Protection System Maintenance and Testing</b>	DP, GO, TO	Document/implement SPS maintenance/testing PROGRAM	√				
PRC-021-1	All	<b>Under-Voltage Load Shedding Program Data</b>	DP, TO	DOCUMENTATION of undervoltage load shedding program	√				

TPL-001-0	All	<b>System Performance Under Normal (No Contingency) Conditions</b>	PA, TPL	System performance under normal conditions	√				
TPL-002-0	All	<b>System Performance Following Loss of a Single Bulk Electric System Element</b>	PA, TPL	System performance under single contingency	√				
TPL-003-0	All	<b>System Performance Following Loss of Two or More Bulk Electric System Elements</b>	PA, TPL	System performance under multiple contingencies	√				
TPL-004-0	All	<b>System Performance Following Extreme Events Resulting in the Loss of Two or More Bulk Electric System Elements</b>	PA, TPL	System performance under extreme contingencies	√				

# **Appendix B**

## **Operating Standards**

## APPENDIX B - OPERATING STANDARDS

A standard is monitored for compliance by letters of certification and /or reporting forms that provide data for compliance assessments. The standards shown with shading are regional measures in which SERC is monitored by NERC. The **BAL-001** and **BAL-002** standards are Designated Reliability Standards and are subject to the RCEP. For those entities in the Balancing Resources and Demand field test program, the CPS2 portion of the BAL-001-0 standard has been waived.

All the approved NERC standards and their effective dates are listed on the NERC website at –

[http://www.nerc.com/~filez/standards/Reliability\\_Standards.html](http://www.nerc.com/~filez/standards/Reliability_Standards.html).

Refer to this website for the latest version and the effective date of the requirements. ALL REQUIREMENTS IN EFFECT ARE SUBJECT TO AUDIT.

<b>Std #</b>	<b>Requirements</b>	<b>Standard</b>	<b>Applicable to</b>	<b>Purpose</b>	<b>Self-Certification</b>	<b>Monthly/Quarterly Reporting</b>	<b>Data Submission</b>	<b>Exception Reporting</b>	<b>Investigation</b>
BAL-001-0	All	<b>Real Power Balancing Control Performance</b>	BA	To maintain Interconnection steady-state frequency within defined limits by balancing real power demand and supply in real-time.		M	√		
BAL-002-0	All	<b>Disturbance Control Performance</b>	BA, RSG	To ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits.		Q	√		
BAL-003-0	All	<b>Frequency Response and Bias</b>	BA	This standard provides a consistent method for calculating the Frequency Bias component of ACE.				√	
CIP-001-1	All	<b>Sabotage Reporting</b>	BA, GOP, LSE, RC, TOP	Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported.	√				

COM-001-1	R2 and R5	<b>Telecommunications</b>	BA, RC, TOP	Each RC, TOP and BA needs adequate and reliable telecommunications facilities internally and with others for the exchange of Interconnection and operating information necessary to maintain reliability.	√					
EOP-001-0	All	<b>Emergency Operations Planning</b>	BA, TOP	Each Transmission Operator and Balancing Authority needs to develop, maintain, and implement a set of plans to mitigate operating emergencies. These plans need to be coordinated with other Transmission Operators and Balancing Authorities, and the Reliability Coordinator.	√					
EOP-003-1	All	<b>Load Shedding Plans</b>	BA, TOP	A Balancing Authority and Transmission Operator operating with insufficient generation or transmission capacity must have the capability and authority to shed load rather than risk an uncontrolled failure of the Interconnection.	√					
EOP-005-1	All	<b>System Restoration Plans</b>	BA, TOP	To ensure plans, procedures, and resources are available to restore the electric system to a normal condition in the event of a partial or total shut down of the system	√					
EOP-006-1	All	<b>Reliability Coordination – System Restoration</b>	RC	The Reliability Coordinator must have a coordinating role in system restoration to ensure reliability is maintained during restoration and priority is placed on restoring the Interconnection.	√					
EOP-008-0	All	<b>Plans for Loss of Control Center Functionality</b>	BA, RC, TOP	Each reliability entity must have a plan to continue reliability operations in the event its control center becomes inoperable.	√					
EOP-009-0	All	<b>Documentation of Blackstart Generating Unit Test Results</b>	GO, GOP	To ensure that the quantity and location of system blackstart generators are sufficient and that they can perform their expected functions.	√					

IRO-001-1	All	<b>Reliability Coordination – Responsibilities and Authorities</b>	BA, GOP, LSE, PSE, RC, TOP, TSP	Reliability Coordinators must have the authority, plans, and agreements in place to immediately direct reliability entities within their Reliability Coordinator Areas to re-dispatch generation, reconfigure transmission, or reduce load to mitigate critical conditions to return the system to a reliable state.	√				
IRO-004-1	All	<b>Reliability Coordination – Operations Planning</b>	BA, GO, GOP, LSE, RC, TO, TOP, TSP	Each Reliability Coordinator must conduct next-day reliability analyses for its Reliability Coordinator Area to ensure the Bulk Electric System can be operated reliably in anticipated normal and Contingency conditions.	√			√	
IRO-014-1	All	<b>Procedures, Processes, or Plans to Support Coordination Between Reliability Coordinators</b>	RC	To ensure that each Reliability Coordinator's operations are coordinated such that they will not have an Adverse Reliability Impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations.	√				
IRO-015-1	All	<b>Notifications and Information Exchange Between Reliability Coordinators</b>	RC	To ensure that each Reliability Coordinator's operations are coordinated such that they will not have an Adverse Reliability Impact on other Reliability Coordinator Areas and to preserve the reliability benefits of interconnected operations.	√				
IRO-016-1	All	<b>Coordination of Real-time Activities Between Reliability Coordinators</b>	RC	that they will not have an Adverse Reliability Impact on other Reliability Coordinator Areas	√				
PER-002-0	All	<b>Operating Personnel Training</b>	BA, TOP	Each Transmission Operator and Balancing Authority must provide their personnel with a coordinated training program that will ensure reliable system operation.	√				

PER-003-0	All	<b>Operating Personnel Credentials</b>	BA, RC, TOP	Certification of operating personnel is necessary to ensure minimum competencies for operating a reliable Bulk Electric System.				√	
PER-004-1	All	<b>Reliability Coordination — Staffing</b>	RC	Reliability Coordinators must have sufficient, competent staff to perform the Reliability Coordinator functions.	√				
TOP-003-0	All	<b>Planned Outage Coordination</b>	BA, GOP, RC, TOP	Scheduled generator and transmission outages that may affect the reliability of interconnected operations must be planned and coordinated among Balancing Authorities, Transmission Operators, and Reliability Coordinators.	√				√
TOP-004-1	R6	<b>Transmission Operations</b>	TOP	To ensure that the transmission system is operated so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single Contingency and specified multiple Contingencies.	√				
TOP-005-1	All	<b>Operational Reliability Information</b>	BA, PSE, RC, TOP	To ensure reliability entities have the operating data needed to monitor system conditions within their areas.	√			√	
TOP-007-0	All	<b>Reporting System Operating Limit (SOL) and Interconnection Reliability</b>	RC, TOP	Ensure SOL and IROL violations are being reported to the Reliability Coordinator so that the Reliability Coordinator may evaluate actions being taken and direct additional corrective actions as needed.				√	
VAR-001-1	All	<b>Voltage and Reactive Control</b>	PSE, TOP	To ensure voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real time to protect equipment and the reliable operation of the Interconnection.	√				

# **Appendix C**

## **SERC Planning Standards Data Submittal Information Processes**

# APPENDIX C

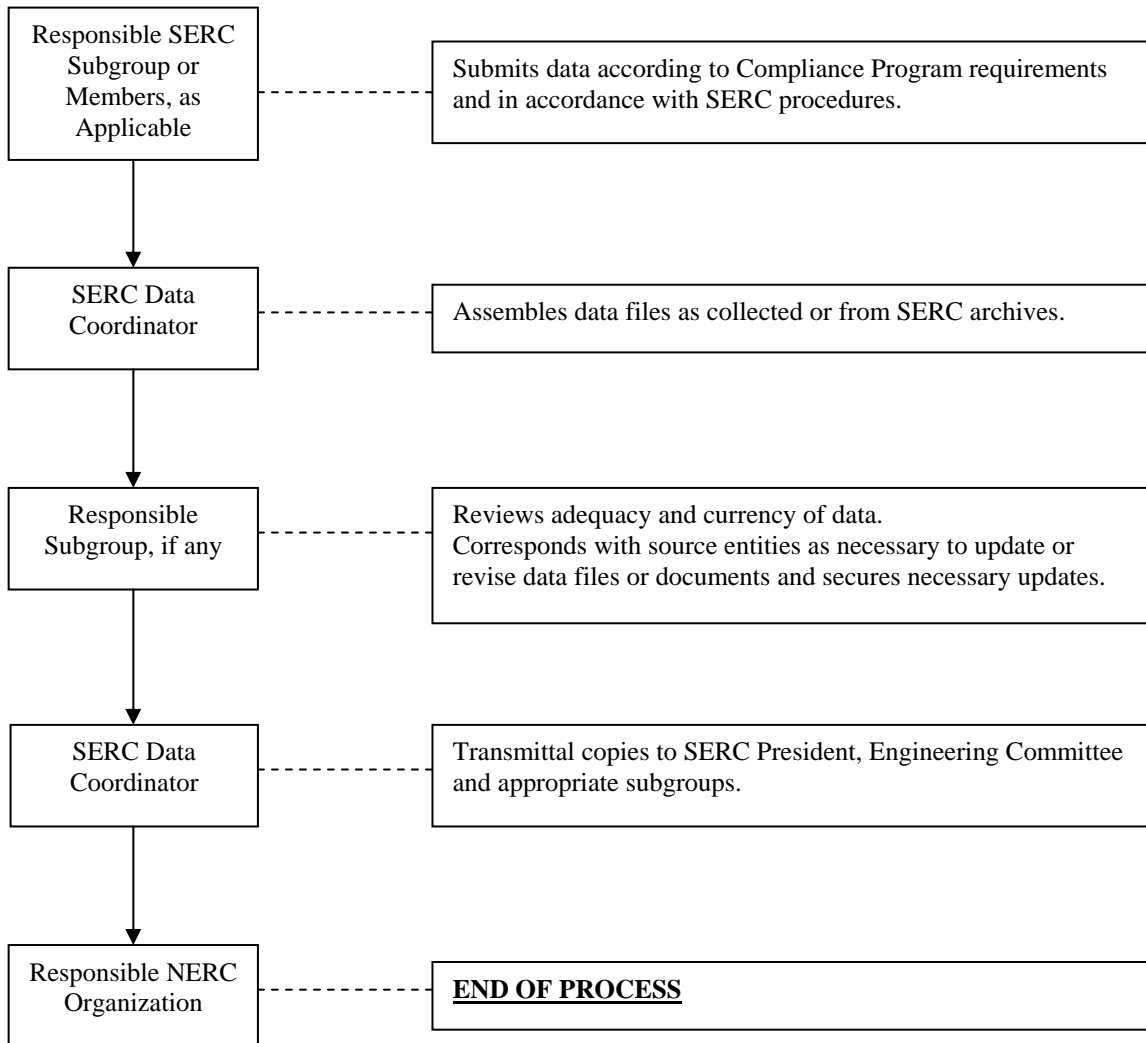
## Attachment 3

### SERC COMPLIANCE REVIEW PROCESS

#### REGIONAL BULK DATA SUBMITTALS

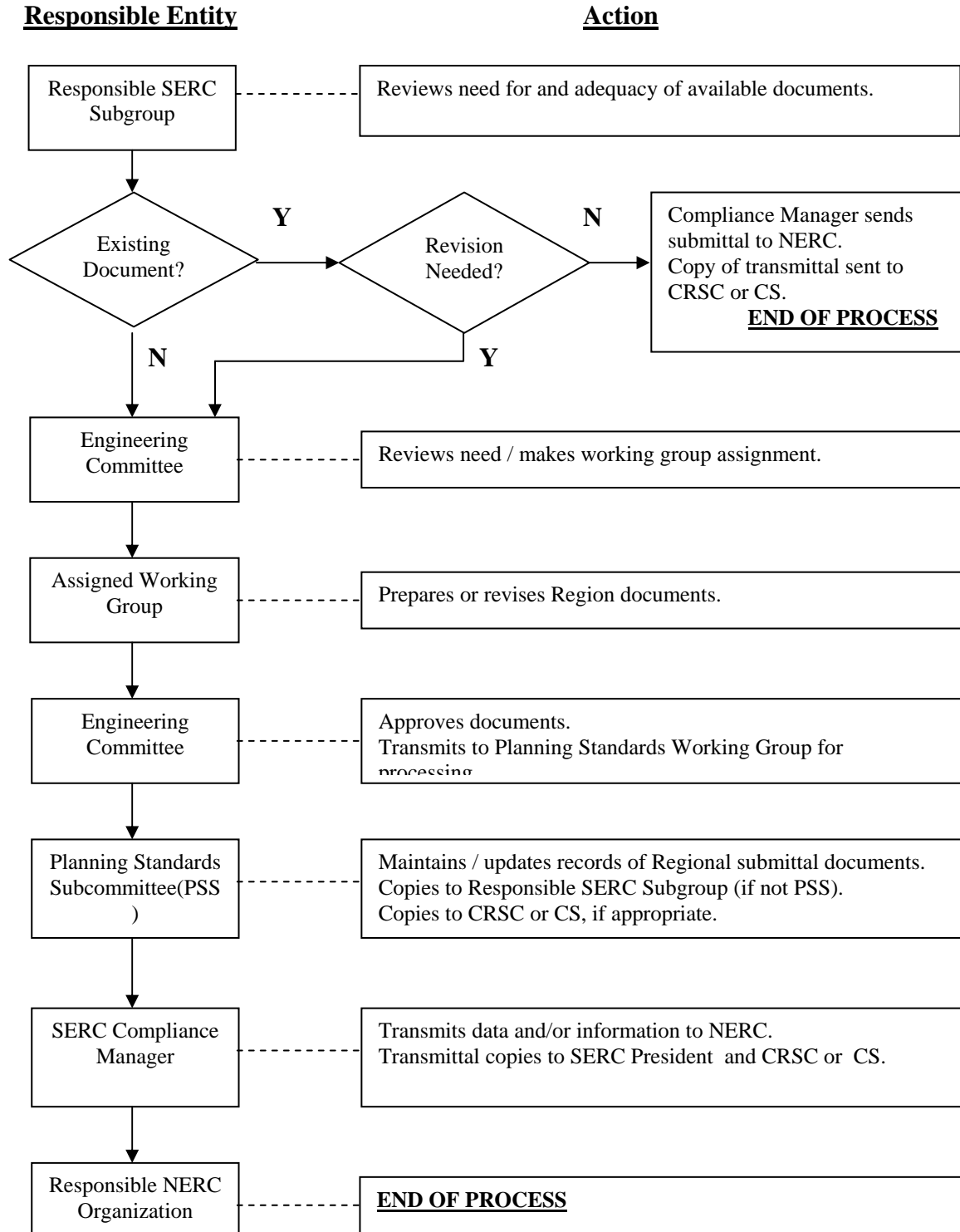
#### Responsible Entity

#### Action



**Attachment 4**

**SERC COMPLIANCE REVIEW PROCESS**  
**FOR REGIONAL DOCUMENT SUBMITTALS**



# **Appendix D**

## **SERC Mitigation Process**

## **APPENDIX D – SERC MITIGATION PROCESS**

The Mitigation Process begins when an entity's filing is assessed as non-compliant by either the Compliance Review Steering Committee (CRSC) for planning standards; or the Compliance Subcommittee (CS) for operating standards. The Entity reporting has a responsibility to become compliant.

Step 1 - At the direction of either the CRSC or CS the Compliance Manager transmits a letter notifying the entity that they have been assessed as non-compliant. The letter specifies the standard judged non-compliant, the reason for non-compliance, and the action to be taken to become compliant. The letter also describes the recourse the entity has in the event there is a disagreement concerning the non-compliance.

Step 2 – The Member or other reporting Entity reviews the letter and either accepts the deficiency or disputes it. If accepted the Entity submits a mitigation plan to correct the deficiency. The mitigation plan is to include a description of the actions to be taken to become compliant, a schedule for completion of those actions, steps to prevent a reoccurrence, and the effect on the reliability of the bulk electric system. In special circumstances the Compliance Manager may ask for additional information to be included in the mitigation plan.

In the event the Entity disputes the deficiency, the Member or other reporting Entity notifies the SERC Office (Compliance Manager) of his request for appeal to the Compliance Oversight Group (COG) in accordance with the appeals process in Appendix H.

Step 3 – The Compliance Manager will maintain a log of the status of mitigation plans. The Compliance Manager will review the record with the Entity to establish that the record is correct. If the dispute cannot be resolved by the Compliance Manager within the schedule timeframe, the appeal will proceed. The CRSC or CS will be notified of Entities that are non-responsive.

Step 4 – Refer to Appendix H – Appeals and Alternate Dispute Resolution Process for a description of the appeals process.

Step 5 – The CRSC or CS resumes the process upon receipt of the mitigation plan. The plan may either be accepted or rejected by the CRSC or CS.

Step 6 – The Compliance Manager communicates the decisions of the CRSC or CS to the Entity, updates the Mitigation Status Log, and provides the status report to the CRSC or CS.

Step 7 – The Member or Reporting Entity completes the mitigation plan. New or revised filings are submitted in the same way as initial filings on the Portal, except that a copy is sent by email directly to the Compliance Manager as well. A mitigation closure certification is filed with the SERC Office using the SERC Portal.

Step 8 – The log of the filings will be updated and the information transmitted to the CRSC or CS by the SERC Office.

Step 9 – The CRSC or CS will update the compliance level as a result of the mitigation plan and incorporate that into the report to the COG. A notification of the results will be sent to the Entity. However, the results of the mitigation plan will not change the initial compliance assessment and penalties that result.

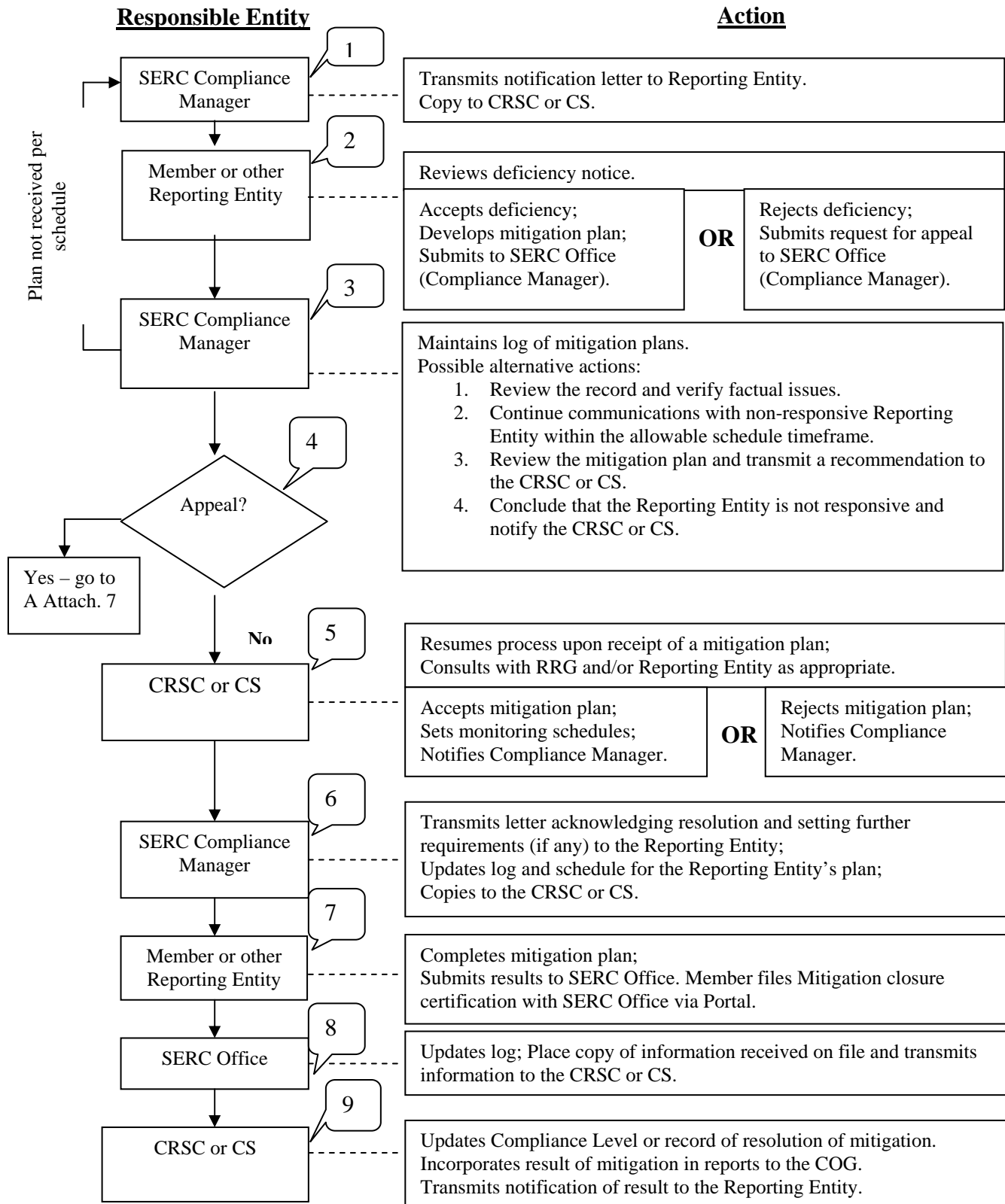
For planning standards, in the event that the mitigation plan schedule exceeds the next self-certification filing or audit date the entity will be considered non-compliant but will not be subject to additional penalties on the measure that is in mitigation. For mitigation plans longer than the next regular compliance filing a status update may be requested to assess whether the mitigation plan is on schedule.

For operating policies, mitigation plan schedules that exceed the next compliance filing will be assessed in accordance with the penalty matrix for re-occurring non-compliances. Findings of non-compliance under an approved mitigation plan will not be penalized again as a result of an audit or annual self-certification.

If, however, the entity fails to meet its mitigation plan schedule and does not provide a revised plan, or has revised its mitigation plan schedule and failed to meet that revised schedule, penalties may be assessed by the COG at the next assessment.

**SERC COMPLIANCE REVIEW PROCESS**

**MITIGATION PROCESS**



# **Appendix E**

## **SERC Late Data Submittal Process**

## APPENDIX E

### Non-Compliance Procedures for Late Submittals

NERC is responsible for reviewing and enforcing compliance of standards applicable to the regions.. NERC also oversees each region's compliance review and enforcement process. The enforcement process relies heavily on the regions to enforce the NERC standards with their members, including the administering of awards and penalties. Regions monitor and enforce NERC Reliability Standards with their members and may impose penalties on entities that do not comply with these standards.

One step in SERC's monitoring of member compliance with NERC standards is committee review of member self-assessments and data submittals. Penalties associated with original late submittals after the due date are evaluated based on the effect the late filing has on the Region Review Group's (RRG's) evaluation efforts and the associated time line activities. Penalties associated with modified filings, based on the RRG review, may be assessed. The RRG will assess and document late filing penalty points on a per measurement basis. Such points will be totaled for each member to determine the appropriate enforcement action (letter and/or fine). The definitions listed below provide guidance for the RRGs in their assessment of the effect of late filings.

### NERC Planning Standards

#### Categories of Late Filing Penalty Points for Planning Standards

- **Late – No Impact** **1.0**  
Received after the due date, but having no impact on the SERC office's distribution of the data to the appropriate RRG for review prior to its compliance assessment meeting. If the submittal contains data required for a SERC filing to NERC, the SERC office's ability to compile the submittal to NERC is not affected.
- **Late – Minimal Impact** **1.5**  
Received after the due date and having some impact on the SERC office's distribution of data to the appropriate RRG for review, but prior to the RRG's meeting to conduct compliance assessments. If the submittal contains data required for a SERC filing to NERC, the SERC office's ability to compile the submittal to NERC is minimally affected.
- **Late – Moderate Impact** **2.0**  
Received after the appropriate RRG's meeting for compliance assessments and before the RRG's Report due date. If the submittal contains data required for a SERC filing to NERC, the submittal is received prior to the NERC filing date, but the SERC office's ability to compile the submittal to NERC is moderately affected.
- **Late – Significant Impact** **2.5**  
Received on or after the appropriate RRG's Report due date or the NERC filing date, where applicable.
  - **No submittal** **10 (Level 4 non-compliance)**

## NERC Operating Standards

The late submittal of a required compliance filing in accordance with the requirements of the NERC Operating Policies to the Region shall be evaluated based on the impact the late filing has on the Region's evaluation efforts and the associated time line. Assessments will be made by the SERC Compliance Subcommittee.

### Categories of Late Filing Penalty Points Applicable to Monthly Submittals )

#### **Late – One Calendar Day**

**1.0**

Received one day after the due date. Since the submittal contains data required for a SERC filing to NERC, the SERC office's ability to compile the submittal to NERC is affected in a minor way.

#### **Late – Two Calendar Days**

**1.5**

Received two calendar days after the due date. Since the submittal contains data required for a SERC filing to NERC, the SERC office's ability to compile the submittal to NERC is affected.

#### **Late – Three Calendar Days**

**2.0**

Received three calendar days after the due date. Since the submittal contains data required for a SERC filing to NERC the SERC office's ability to compile the submittal to NERC is moderately impacted.

#### **Late – Four Calendar Days**

**2.5**

Received four calendar days after the due date. Since the submittal contains data required for a SERC filing to NERC the SERC office's ability to compile the submittal to NERC is seriously impacted.

#### **Late – Five or More Calendar Days (Level 4 non-compliance) 5.0**

Received on or after the appropriate RRG's Report due date or the NERC filing date, where applicable, or no filing received.

### Categories of Late Filing Penalty Points Applicable to Annual Self-Certifications.)

- **Late – No Impact**

**1.0**

Received after the due date, but having no impact on the SERC office's distribution of the data to the Compliance Subcommittee for review prior to its compliance assessment meeting. If the submittal contains data required for a SERC filing to NERC, the SERC office's ability to compile the submittal to NERC is not affected.

- **Late – Minimal Impact**

**1.5**

Received after the due date and having some impact on the SERC office's distribution of data to the Compliance Subcommittee for review, but prior to the RRG's meeting to conduct compliance assessments. If the submittal contains data required for a SERC filing to NERC, the SERC office's ability to compile the submittal to NERC is minimally affected.

- **Late – Moderate Impact**

**2.0**

Received after the Compliance Subcommittee meeting for compliance assessments and before the RRG's Report due date. If the submittal contains data required for a SERC filing to NERC, the submittal is received prior to the NERC filing date, but the SERC office's ability to compile the submittal to NERC is moderately affected.

- **Late – Significant Impact**

**2.5**

Received on or after the Compliance Subcommittee Report due date or the NERC filing date, where applicable.

- **No submittal assessment) 10 (Level 4 non-compliance)**

### **Penalty Point Consequences (Total Point Accumulation of All Occurrences)**

- 10 Points – Letter to member
  - 20 Points – \$1,000
  - 30 Points – \$2,000\*
- \* Repeat this penalty for each 10 point increment of point accrual

#### **Notes:**

1. The letters concerning non-compliance from the Compliance Manager (see Attachment 5 of Appendix D) and the SERC President (see Attachment 2, Box 14) shall detail the penalty associated with late filings. The letters will also reveal late filing penalty points on a per measurement basis in addition to the total point accumulation of all occurrences with associated fines assessed (if applicable).
2. This penalty system does not compound the level of non-compliance associated with the compliance filing's qualitative evaluation by the appropriate RRG.
3. Non-compliance information shall be considered confidential, subject to release in accordance with SERC Policy.
4. For Planning Standards the clock for assessing penalties will reset each compliance filing period (e. g. June 1<sup>st</sup> and December 1<sup>st</sup>). For Operating Standards the clock for assessing penalties will be on a 12 month rolling calendar reflecting the monthly reporting of these measurements. The Region Compliance Manager will be the keeper of record for the accumulation of violations for a given year.
5. Failure to respond to a request for a filing for Planning Standards will result in a 10-point penalty. Failure to respond to a request for a filing for Operating Standards will result in a 5.0-point penalty per measure being reported. This shall apply to each standard/measure that does not receive a response. In addition, level 4 non-compliance will be assessed in these cases.
6. Points shall be applied to each standard/measure that is received late or does not receive a response. Monetary penalties shall be assessed when the participant has 20 points and shall be assessed for every additional 10 points accrued thereafter, for the remainder of the calendar year.
7. The penalty system for Operating Standards applies only to BAL-001 and BAL-002 and is in field test. If additional measures are added, or the program becomes contractual this penalty system will be evaluated to determine if changes need to be made to existing provisions, or if additional provisions need to be added.
8. If a filing date falls on a non-business day, the filing is due on the next business day.

# Appendix F

## Compliance Program Filing Format Requirements

# APPENDIX F- COMPLIANCE PROGRAM FILING FORMAT REQUIREMENTS

## SERC Member Filing Instructions

SERC Compliance Program filings will be entered and submitted electronically via the SERC Web Portal. The Portal is accessed via the SERC home page ([www.serc1.org](http://www.serc1.org)) by clicking the “Member Portal Homepage” link in the top right-hand corner. An entity may have access to the SERC Portal to file the required compliance filings without being a member of the SERC region. In order to access the Portal, users must obtain a login ID and password. (The process for obtaining the login information and permissions is outlined in the section below.) Please note that the login ID is not case sensitive but the password is case-sensitive. Once the user has successfully entered a valid ID and password on the “Member Portal Login Screen,” they are directed to the “Portal Homepage.”

Depending on the user’s permissions, the user will see various menu items on the left-hand side of the screen. For compliance users, “Compliance” will be one option. To submit filings, users should choose “Compliance” and then the appropriate subsection (Planning, Operating, Cyber Security or Vegetation) for a list of outstanding compliance forms for the member they represent. This is the “Compliance Form Search Results Page.” This page summarizes the status of the compliance forms, including due date, lockout date, ready for approval, and certification statement. The due date indicates the last date for submitting without incurring timeliness penalties. The lockout date is the last date the user will be able to access the form to make a filing. The ready for approval column indicates whether the form(s) are finalized and ready to be submitted. The certification statement column contains checkboxes for forms that have been marked “Submit to SERC.”

Once information is entered on a compliance form, the user can save the form. By saving the form, all information entered will be maintained for the next access of the form. This is particularly useful for entering information in stages or for entry by multiple users. Please note that saving the form does not officially submit the form. Once the information on the form is considered finalized by the user, the “Submit to SERC” checkbox at the bottom of the form should be checked and the form saved again.

By checking this box on the form, a checkbox option will appear on the “Compliance Form Search Results Page” under the “Certification Statement” column. When the user is ready for their executive to sign off on the form(s), the checkboxes for each form to be certified by the officer’s signature should be checked. The user should then proceed through the screens to view the certification statement and run the report for the officer to sign. The report can be generated in several formats, including Word and Adobe. If the signature is going to be submitted in hard copy, the user can choose Adobe. In order to submit the signature electronically via email ([support@serc1.org](mailto:support@serc1.org)) Word should be chosen in order to place the electronic signature into the report.

A training document is available on the public website for the compliance process at <http://www.serc1.org/Pages/DocumentSearch.aspx?FN=SERC/Portal%20Training%20Documents>.

For further assistance with any issue above please email a SERC Administrator at [support@serc1.org](mailto:support@serc1.org).

## Directions for Obtaining Portal Login Information

All SERC Portal Members are required to designate a Master Account Administrator. The duties and

responsibilities of this individual are:

*(Note: these responsibilities are Member specific.)*

1. Create new users (Contacts / Member employees assigned to fill out and submit compliance forms) under the Member account (Master Account).
2. Edit existing users (Contacts / Member employees assigned to fill out and submit compliance forms) under the Member account (Master Account).
3. Assign Security Permissions to new and existing users described above to various sections of the system (411/compliance/seasonal assessments, etc.).
4. Reset Passwords for Member users, if necessary.
5. Become the Point Of Contact for Member users (Contacts / Member employees assigned to fill out and submit compliance forms) and for the SERC Web Portal System Administrator.

Master Account Administrators will create accounts for Member key contacts, including among others, those who will be working with Compliance filings (Planning, Operating Cyber Security, and Vegetation areas.) Therefore, to obtain access to the SERC Web Portal for compliance filings, the following information must be provided to either your Master Account Administrator or to the SERC Web Portal System Administrator:

- SERC Master Account
- Master Account Compliance Contact
  - Name
  - Title
  - Address
  - Phone Number
  - Fax Number
  - E-mail Address

Further instructions for filling out submittals are included on the help screens throughout the SERC Web Portal.

# **Appendix G**

## **Compliance Program Practices & Procedures** **For Conducting Reliability Audits / Investigations Of SERC** **Transmission Operators / Generation Owners / Operators And** **Balancing Authorities**

# **APPENDIX G - Compliance Program Practices & Procedures For Conducting Reliability Audits / Investigations Of SERC Transmission Operators / Generation Owners / Operators And Balancing Authorities**

## **INTRODUCTION**

The purpose of this document is to describe the process the SERC Region will use to audit entity compliance with North American Electric Reliability Council (NERC) Reliability Standards and SERC Supplements.

There are two types of reliability reviews that may be conducted by the SERC Region:

1. **Reliability Audits** -- Reliability audits are comprehensive reviews of an entity's compliance with NERC Reliability Standards and SERC Supplements. SERC may elect to utilize independent auditors for some or all subsequent audits to facilitate staffing of audit teams, and to ensure an unbiased and consistent compliance monitoring program. SERC will perform reliability audits of each entity at intervals in accordance with NERC and SERC procedures.
2. **Reliability Investigations** -- Reliability investigations are performed to determine the root cause of an event occurring on one or more SERC member systems. An event is an abnormal condition caused by the loss of generation, load, transmission facilities or a combination thereof that affects the interconnected system in terms of frequency, voltage, transmission line loadings, etc. Such an event is generally investigated with respect to Operating Standards; however, an investigation may include Planning Standards as well.

A reliability investigation may be conducted for any event that requires the implementation of either of the following two (2) NERC Standards:

- 1) NERC Standard EOP-002-0 – Capacity and Energy Emergencies
- 2) NERC Standard EOP-004-0 - Disturbance Reporting.

Implementation of the above will be triggered by the declaration of an Energy Emergency Alert Level 2 or a disturbance requiring the filing of a report (EIA 417) that indicates an implementation of emergency procedures. SERC members should report either of these situations to the SERC office within seventy-two (72) hours of their occurrence. Following notification, the SERC Compliance Manager, and/or Compliance Staff, will review all EIA 417 reports submitted to determine if emergency procedures were implemented and coordinate with the Compliance Subcommittee (CS) to determine the necessity of an investigation.

## **REVIEW PRACTICES AND PROCEDURES**

Reliability reviews (audits and investigations) are coordinated through SERC's Compliance Manager and the SERC Compliance Subcommittee (CS) or the Compliance Review Steering Committee (CRSC).

The Compliance Manager, and Compliance Staff, is responsible for maintaining the history of entities

audits and scheduling reliability audits with the entities to meet the minimum audit cycle consistent with NERC and SERC requirements. SERC member entities may also request reviews more frequently than the minimum requirements.

The Compliance Subcommittee and Compliance Review Steering Committee are responsible to:

- Administer the compliance review process, including assembling review teams and scheduling reviews.
- Develop a detailed and comprehensive compliance review process for the review teams and for the entities being reviewed.
- Recommend penalties for non-compliance.
- Recommending to the SERC COG penalties for specific instances of non-compliance.
- Provide an appellate procedure.
- Recommend Standards changes to the SERC and NERC EC and OC based on reviews.
- Coordinate efforts with EC compliance development.
- Coordinate with and complement Regional compliance review processes.
- Address independence of auditors, non-disclosure of proprietary information and Code of Conduct issues where appropriate.
- Develop an Audit Schedule.

#### **A. Reliability Audits**

SERC will initially select an audit team responsible for assessing an entity's compliance with NERC Standards and SERC Supplements. The audit team members must subject themselves to confidentiality agreements, if required by the entities being audited, for any data that is made available to them through the audit review process. The entity being audited has the authority to approve or reject initially selected audit team members.

The independence of auditors will be guided by the following principles:

- a. Auditors shall not have or seek any outside employment that limits their ability to comply with SERC rules and practices that carry out these principles.
- b. Auditors shall not participate in any capacity in utility-specific audit and compliance review activities involving entities in which a Audit/Compliance Team Member or his immediate family has a direct and/or material financial interest, or an Audit/Compliance Team Member or his immediate family works or has worked as an employee or board director, or works or has worked as a contractor or consultant.
- c. Auditors shall not accept gifts or entertainment that would affect or give the appearance of affecting the performance of their duties.
- d. Members of the CS, CRSC, CSCRS, and COG need to be independent of the entity in violation when such violations are reviewed by the appropriate committee. This can be accomplished by abstaining from voting with regard to the matter.

The audit team make-up will typically be as follows:

- A CS or CRSC appointed team.
- A minimum of three experienced members.
- Members should preferably have at least five years experience in the areas of system operations or planning.
- Members shall be thoroughly familiar with the NERC Reliability Standards.
- For Balancing Authority audits at least one member shall be NERC Operator Certified.
- For planning audits, the team will include RRG (Reliability Review Group) team members.
- Members will not be affiliated with the entities being audited.
- No two members shall be from the same entity.
- One member shall be appointed as Team Leader responsible for overall coordination of the audit.
- One member of the Team shall be from the SERC Regional staff to ensure consistent adherence to SERC's practices and procedures.
- The SERC Regional staff member will assist the Team Leader and be responsible for distributing and collecting the pre-audit questionnaires, arranging the on-site visits, and preparing and distributing the audit report. See step 3 below about pre-audit questionnaires.

### **Audit Team Practices**

- The Audit Team may ask the entity to demonstrate to their satisfaction that the System Operators and responsible personnel are familiar with the Reliability Standards and know how to implement them.
- The Audit Team may ask for an explanation of the process of collecting and reporting compliance data. For example, in reference to compliance with the Control Performance Standards (CPS), the Audit Team should ask the support staffs to explain how the data is reviewed and how erroneous or incomplete data is removed and performance is recalculated. The formula itself should be verified as well.
- An audit includes the verification of data and information, not just a check to see if the end results are available.
- The compliance review on-site visits should be conducted in a manner that minimizes the effect on personnel from the entities being audited as well as the entities that provide the Audit Team
- A free exchange of information is encouraged but lengthy, detailed discussions are discouraged. A balanced approach is suggested.
- The Audit Team shall refrain from making premature judgments or comments until the entire team has had an opportunity to review their notes and reach consensus on their findings. Should there be a disagreement of opinion between the Audit Team members about whether an issue is compliant/non-compliant, the Team Leader will either resolve the disagreement or present both sides of the issue to the respective committees and/or COG for final resolution.
- The Audit Team shall provide an exit briefing to the entity's representatives at the end of the audit of the issues identified during the audit that the team will report as non-compliances.
- The audited entity may provide additional information for audit team review and consideration within 14 days of the audit. Information received after the 14 day period will not be accepted for consideration in the audit report, but will be considered as mitigation of a non-compliance. The audit team will review the entities response, make any necessary revisions to the audit report.
- The audited entity shall respond in writing to the draft audit report findings within 14 days of receiving it.

SERC shall provide all the forms and questionnaires utilized by all entities involved in the audit. These forms and questionnaires will address the audited entity's capabilities and actions as they relate to

previously established entities requirements. The questionnaires are not considered confidential. The compliance committees (CRSC, CS) have the option whether to use neighbor questionnaires in the current year audit program.

For Balancing Authority audits, the following list of entities will receive the designated questionnaires, as each is a source of necessary auditing information and data:

- Balancing Authority being audited – Pre-Audit Questionnaire and Documentation To Be Reviewed.
- Balancing Authority physically interconnected with audited control area – Adjacent Balancing Authority Questionnaire.
- Reliability Coordinators –Reliability Coordinator Questionnaire.

Planning audits may use a similar set of documents including data coordinator and neighboring system questionnaires.

The audit team may conduct an on-site visit to the audited entity's facilities. During a visit, audit team members will:

- Inspect the entity's facilities and equipment,
- Review with the entity the data collected through the questionnaires,
- Review entity's data submittals (may be conducted off-site),
- Interview the entity's operations, engineering and management personnel, and
- Review all other necessary documents and data as considered necessary.

The Audit Team's assessment of the entity's compliance with NERC's Reliability Standards shall be based the results of the audit steps performed as described above. The Audit Team's findings will be documented in a formal report that will include at least the following elements:

- The purpose of the audit,  
(determine whether the Entity complies with NERC Reliability Standards).
- The scope of the audit,  
(listing of NERC Reliability Standards being reviewed).
- Findings,  
(the findings will be based on the Entity's compliance with the NERC Reliability Standards audited and all findings of non-compliance will be clearly described).
- The audited entity's response to the audit report findings  
(includes a clear statement as to whether they agree or disagree with the finding(s). If they agree, the audit report should also include the date they will provide SERC a detailed mitigation plan that corrects any areas of non-compliance. If they disagree, the audit report should include their detailed discussion why they disagree.)

The Audit Team is responsible for developing a draft audit report and presenting it to the entities being audited for their review and written response. As appropriate, any differences of opinion on the audit results should be discussed to ensure both the entity being audited and the audit team clearly understand each other's position. The draft report with the entity's responses shall be reviewed by the CRSC or CS, as appropriate, and sent to the SERC Compliance Oversight Group (COG). Refer to the Audit Process flowchart. The COG is responsible for approving the report and, as necessary, it may remand the audit report back to the audit team for further

clarification, review or verification of the audited entity's compliance. The audit team shall repeat any audit steps as required to ensure the findings are solely based on the audit results. Once the COG approves the audit report, it will notify the entity and audit team members it has approved the report.

### **Audit Timeline**

- Questionnaires shall be sent to all entities involved in an audit at least six (6) weeks prior to the on-site visit at the audited entity.
- Completed Questionnaires shall be returned to the SERC office by all entities involved in an audit at least two (2) weeks prior to the on-site visit at the audited entity.
- An initial draft of the audit report shall be prepared within two (2) weeks following the on-site visit at the audited entity and distributed to the audited entity for review and a written response. The audit team shall review the initial draft of the audit report prior to it being sent to the audited entity.
- The audited entity may provide additional information for audit team review and consideration within 14 days of the audit. Information received after the 14 day period will not be accepted for consideration in the audit report, but will be considered as mitigation of a non-compliance.
- The entity being audited shall respond in writing to the draft audit report findings within 14 days of receiving it. The entity shall send their written response to the Compliance Manager. The audit team will review the entities response, make any necessary revisions to the audit report, and forward the report to the CRSC or CS. The CRSC or CS will review and finalize the audit report and forward the report to the COG.

### **Balancing Authority / Transmission Operator Audit and Certification – Delay in Operating as a Balancing Authority**

- In the event a Balancing Authority is audited and certified, and then delays initiating operation as a Balancing Authority ; the certification expires after one year. Re-auditing and re-certification of the Balancing Authority is required.

Following certification of a new Balancing Authority by the Compliance Subcommittee, the proposed Balancing Authority startup date will be reviewed by the Compliance Subcommittee to evaluate any reliability risks. If the Compliance Subcommittee finds there are reliability risks, the Compliance Subcommittee will then consult with the entity requesting certification to determine a mutually acceptable alternate startup date. The Balancing Authority certification will then be extended for a period up to six (6) months, if necessary, without re-audit.

A single six (6) month extension may be granted by the Compliance Subcommittee, if requested by the entity requesting certification, to avoid Balancing Authority startup during periods of increased risk to the interconnection (such as peak seasons).

### **B. Reliability Investigations**

1. The team membership requirements are the same as identified for the Reliability Audit Team. However, if required, the Investigation Team should be augmented with personnel with specialized technical backgrounds, such as experience in the areas of relaying and system stability.
2. The Investigation Team may elect to conduct an on-site visit to the entity (for example, the control room of the Balancing Authority ) experiencing the event to review data collected, interview operations and

management personnel and verify documentation of procedures followed during the event.

3. The Investigation Team, as appropriate, shall adhere to the Audit Team Practices.
4. The Investigation Team is responsible for developing a draft investigation report and presenting it to the entity experiencing the event for their review and written response. The investigation report shall include: type of emergency, duration of emergency, time and media used to inform external-entity's representatives, actions taken, sequence of events, violations of NERC Reliability Standards, Investigation Team conclusions and recommendations for corrective action. As appropriate, any differences of opinion on the investigation results shall be discussed to ensure both entities clearly understand each other's position. The draft report including the entity's responses shall be sent to the SERC Compliance Oversight Group (COG). The COG is responsible for approving the report and, as necessary it may remand the investigation report back to the investigation team for further clarification, review or verification of the investigated entity's event. The investigation team shall repeat any steps as required to ensure the findings are solely based on the investigation results. Once the COG approves the investigation report, they shall notify the entity and investigation team members they have approved the report.

#### **5. Investigation Timeline:**

SERC entities shall notify the SERC office as soon as possible following an event that required implementation of an emergency energy alert, or load shedding. The Compliance Subcommittee will determine if an investigation of the event is warranted. If so -

- The SERC Compliance Manager shall set the investigation schedule and coordinate data requests with the entities experiencing an event within seven (7) days following notification of the event.
- The entities being investigated shall collect all data related to the event, prepare written answers to questions and return all related data requests to the SERC office within 21 days following notification of the event.
- If necessary, an on-site visit shall be conducted within four (4) weeks following notification of the event.
- An initial investigation report shall be prepared within six (6) weeks following notification of the event and forwarded to the SERC COG.

#### **C. Detailed Compliance Reviews (DCRs)**

Definition: Detailed Compliance Review: A detailed review of member filings conducted at an RRG meeting, typically including the filings of all members for a given measure. Items selected for such reviews will be deemed stand-alone filings, meaning additional supporting documents or discussions should not be necessary, but may be requested as noted within the compliance program. An example might be a facilities connection document which is designed to be all-inclusive.

The CRSC and CS determine whether to conduct DCRs for their respective areas; and if so, what measures will be subject to the DCR process, frequency of the audits, and inclusion into the yearly audit plan.

The review team for DCRs will be made up of representatives of the appropriate SERC Region Review Group (RRG), Compliance Review Steering Committee or Compliance Subcommittee. They will be familiar with the standards in effect and the relevant SERC Supplements. The DCRs will be limited to the documentation required to be submitted by the standard, however if the filing indicates other documentation

would be made available upon request, such documents may be requested.

The Compliance Manager or designated SERC staff will coordinate receipt of the requested documents, disseminate to the review team, and document the results. Results of the Detailed Compliance Reviews will be sent to the members, whether they are compliant or not.

#### **D. Spot Checks**

The CRSC and CS will determine whether to conduct spot checks for their respective areas. Spot checks will be conducted by representatives of the appropriate SERC Region Review Group (RRG), Compliance Review Steering Committee or Compliance Subcommittee. They will be familiar with the standards in effect and the relevant SERC Supplements. The provisions of item A.1 will apply to the make up of the audit team performing the spot check.

The Audit Indicator Status Report is one mechanism to track issues that may require a spot check. The report will be maintained by the Compliance Manager to track issues of concern to the committees. The report is a "SERC Confidential" document. The contents with regard to a member being audited may be shared with that member at the direction of the Chair(s) of the compliance committees (CRSC or CS).

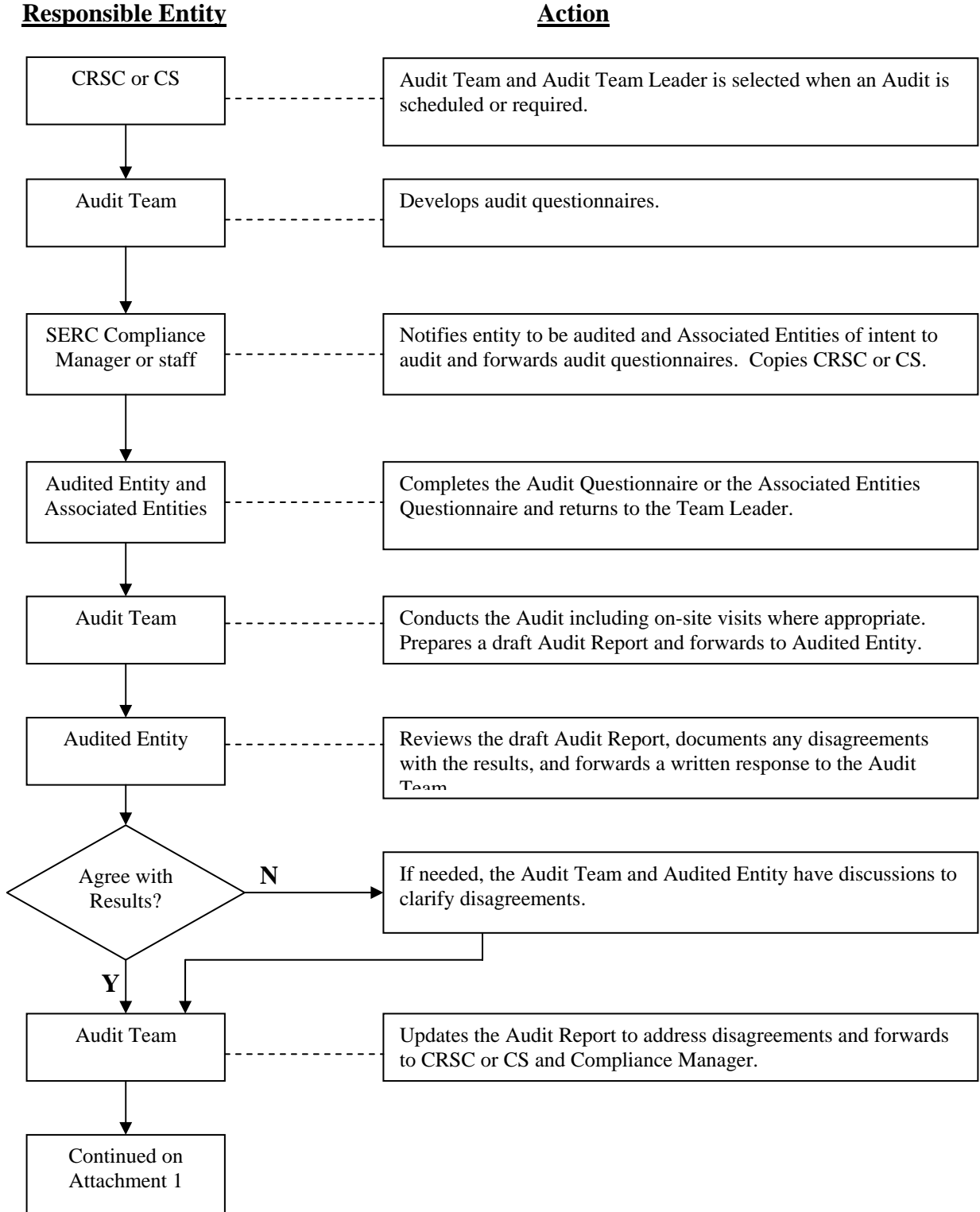
The Audit Indicator Status Report is made up of items that have been identified in performing compliance assessments of the entity, assessments that relate to the entity, and / or other matters that may come to the attention of the compliance committees. They are un-substantiated until such time as they are verified by an audit or spot check of the entity and are considered confidential.

The Compliance Manager or designated SERC staff will coordinate arrangements for the spot check, coordination with the audit team, arrangements with the member, and follow up with a report to the member involved.

**Attachment 6**

**SERC COMPLIANCE REVIEW PROCESS**

**AUDIT PROCESS**



# **Appendix H**

## **Appeals and Alternate Dispute Resolution Process**

## APPENDIX H - APPEALS AND ALTERNATE DISPUTE RESOLUTION PROCESS

The compliance decision process is a three-step sequential process that provides affected entities with the opportunity to participate in and to appeal adverse decisions. The steps are:

1. The Compliance Oversight Group (COG) finding of non-compliance.
2. Appeal to the SERC Executive Committee.
3. Appeal to an Independent Arbitrator.

Appeals at each level are initiated by notifying the Compliance Manager that the affected entity is appealing the non-compliance determination.

### The Compliance Oversight Group

In accordance with the Compliance Review Process (Attachment 1) the Compliance Manager will provide a preliminary finding of non-compliance to an entity. This notification will be made after review by the Compliance Review Steering Committee (CRSC) for planning standards and the Compliance Subcommittee (CS) for operating standards. If upon receipt of that notification, the affected entity wishes to present its position on the matter it may do so, in writing with any supporting documentation, within fourteen days of issuance of the notification. The request to appeal the decision is to be on the organization's letterhead and signed by the officer who certified its filings, or if the result of an audit, the officer who normally signs the annual certification to the standard in question. Responses, if any, to the appellant's submittal must be made no later than seven days following the submittal. The affected entity and the appropriate compliance review committee shall have the opportunity to make oral presentations to the COG, in which case questions may be asked only by members of the SERC COG. This information will form a part of the record upon which the COG will base its decision on compliance or noncompliance and, while the entity may raise any issues it wishes respecting the preliminary finding, it may not challenge the validity of the Reliability Standards.

The COG's decision will be based on each SERC member on the committee having one vote. A quorum shall consist of two thirds of the Compliance Oversight Group membership. A member may be represented by another qualified individual (alternate) provided that the member has provided written authorization for that individual (alternate) to participate. Approval of any action requires a majority of the votes cast.

If no submittal is made by the affected entity within the prescribed 14 day period the preliminary finding of noncompliance made by the CRSC or the CS becomes final, and the Compliance Review Process (Attachment 1) proceeds to an assessment by the COG of financial and other penalties.

Any member of the COG that has an interest in the outcome of the proceeding, specifically including any COG member that is an employee of an affected entity, shall not participate in the consideration of or decision concerning the alleged noncompliance.

### Appeal to the SERC Executive Committee

An affected entity may appeal an adverse COG decision to the SERC Executive Committee. Written notification of the affected entity's intent to appeal must be communicated to the Compliance Manager no later than 14 calendar days after the affected entity receives the COG's final decision and the Compliance Manager shall promptly thereafter transmit such notification to the SERC Executive Committee. The request to appeal the decision is to be on the organization's letterhead and signed by the officer who certified its filings, or if the result of an audit, the officer who normally signs the annual certification to the standard in question. Both the

affected entity and the COG will prepare written statements of their positions on the issues and present them, with any supporting documentation they believe is appropriate, to the SERC Executive Committee within 21 calendar days following the date of the written notification of the appeal. Both the affected entity and the COG may respond to the written presentations within seven days of the submittal of the presentations. The affected entity and the COG shall have the right to make oral presentations to the SERC Executive Committee, in which case questions may be asked only by members of the SERC Executive Committee. Either the affected entity or the COG may raise any issues it wishes respecting the COG decision, such as the factual bases for the decision or the procedural steps involved, but neither may challenge the validity of the Standards, Measurements or Operating Procedures.

If the SERC Staff prepares a report on the disputed matter for the SERC Executive Committee's use in its deliberations, a copy of such report shall be made available to the parties, and the parties shall be afforded a reasonable opportunity to respond to the SERC Staff report.

The SERC Executive Committee will render its decision within 60 calendar days of the date of the affected entity's notification of appeal. The SERC Executive Committee's decision will be based on each SERC member on the committee having one vote. A quorum shall consist of two thirds of the Executive Committee membership. A member may be represented by another qualified individual (alternate) provided that the member has provided written authorization for that individual (alternate) to participate. Approval of any action requires a majority of the votes cast.

Any member of the SERC Executive Committee that has an interest in the outcome of the proceeding, specifically including any SERC Executive Committee member that is an employee of the affected entity, shall not participate in the consideration of or decision concerning the alleged noncompliance. The SERC Executive Committee decision is the final SERC decision on the matter.

#### Appeal to an Independent Arbitrator

An affected entity may appeal an adverse SERC Executive Committee decision to an independent arbitrator acceptable to both the affected entity and the SERC Executive Committee (the "Parties"). The affected entity must notify the Compliance Manager of the affected entity's intent to appeal the SERC Executive Committee's decision not later than 14 calendar days after the SERC Executive Committee issues its decision, and the Compliance Manager shall promptly thereafter transmit such notice to the SERC Executive Committee. The request to appeal the decision is to be on the organization's letterhead and signed by the officer who certified its filings, or if the result of an audit, the officer who normally signs the annual certification to the standard in question.

The arbitration will be conducted in the following manner. The Parties shall prepare a list of proposed arbitrators by each submitting no more than three (3) names for consideration, and within 21 calendar days following the date of the affected entity's notification of its intent to appeal the SERC Executive Committee's decision, the Parties will select a single arbitrator from such list. All arbitrators proposed by the Parties must be knowledgeable with respect to issues related to the reliability and adequacy of the interconnected bulk power supply system, including, but not limited to, issues related to planning and Balancing Authority operations. The Parties will select the arbitrator from such list by (a) agreement, or in the absence of agreement, by (b) alternately striking names from the list in turn (beginning with the Party that wins a coin toss for this purpose) until only the selected arbitrator remains. In lieu of preparing their own list of proposed arbitrators, if the Parties mutually agree to do so, they will select an arbitrator from the list of National Energy Arbitrators maintained by the American Arbitration Association by following the selection process specified in the

preceding sentence.

The arbitrator selected may not be an employee, director, or officer of either Party or any Affiliate of a Party. Potential arbitrators who are employees, directors, or officers of Members of the SERC, but who are not themselves officers of the SERC or members or alternate members of the SERC Executive Committee, will not be considered to be employees, directors, or officers of the SERC. The arbitrator will agree in writing to be bound by the confidentiality obligations applicable to the SERC Staff.

The arbitrator will provide the Parties an opportunity to be heard and, except as otherwise provided herein, will generally conduct the arbitration in accordance with the Commercial Arbitration Rules of the American Arbitration Association. SERC will submit to the arbitrator the report provided by the SERC Staff to the SERC Executive Committee and any other relevant information, and the data and information provided by the affected entity. The affected entity may present whatever additional evidence it believes reasonably supports its position. SERC and the affected entity will be afforded a reasonable opportunity to rebut the evidence presented. The arbitrator will create and maintain an evidentiary record of sufficient detail to document the rationale for his decision.

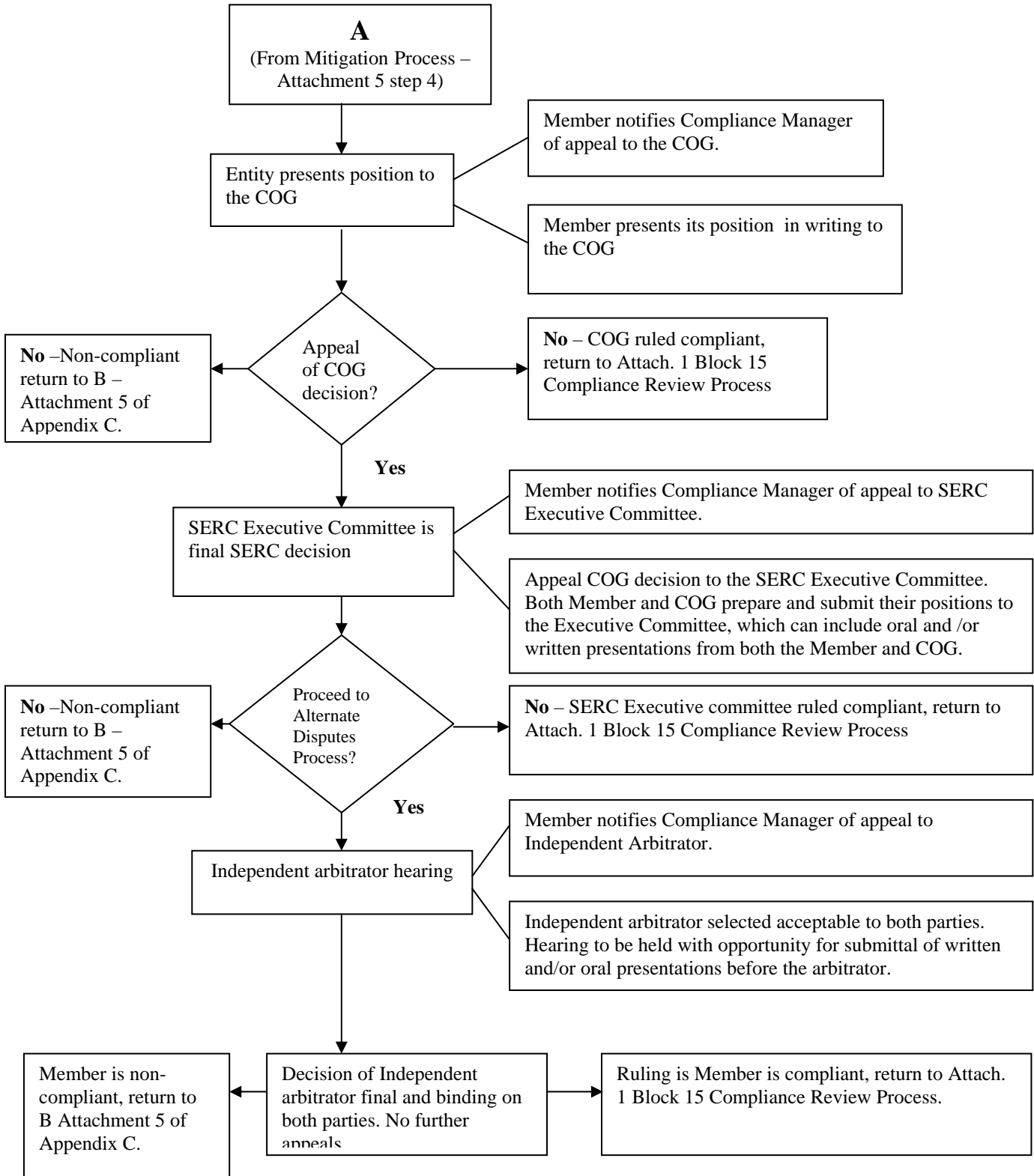
As soon as practicable, but no later than sixty 60 calendar days after the date on which the Parties selected the arbitrator, the arbitrator will issue a written decision resolving the dispute and explaining the basis for his conclusions. Such decision will include findings of fact to support the arbitrator's conclusion(s), and will be final and binding on the parties but will have no precedential effect with respect to any other dispute. During the arbitration process, the Parties will make funds available to the arbitrator as required by the arbitrator to pursue the arbitration. The cost of such funding will be shared equally by the Parties, and at the conclusion of the arbitration will be reimbursed as specified below.

In any arbitration either Party may raise any issue regarding the sanction determination, including the factual basis for the sanction and whether the procedures specified were properly followed. Neither party, however, may dispute the validity of the Reliability Standards.

If an arbitrator hearing a dispute between the Parties determines that data from a SERC Member are relevant to the consideration of such dispute, the arbitrator will so notify such Member, and such Member will have 14 calendar days, or a mutually agreeable extension thereof, to provide the requested data.

Any and all reasonable costs associated with the arbitration (not including attorney and expert witness fees which will be borne by the respective Parties) will be borne by the Party whose arbitration position was not selected by the arbitrator, unless the Parties agree to a different method of allocating costs. If the arbitrator's decision differs from the positions of both the Parties, the arbitrator will specify how the costs are to be allocated. Such cost allocation will include reimbursement of any funds provided to the arbitrator by the Parties. Payment of any such costs will be due at the same time any monetary sanctions would be due or, if no monetary sanctions are due, within 21 days following the final decision of the arbitrator.

## Attachment 7 - Appeals and Alternate Dispute Resolution Process



# **Appendix I**

## **NERC Penalties for Non-Compliance**

## **APPENDIX I – NERC PENALTIES FOR NON-COMPLIANCE**

Confirmed non-compliances will be posted quarterly on the NERC website. ~~The prospective penalty will not be posted.~~ For those members who have signed the RCEP, financial penalties are in effect for the designated reliability standards. Penalties will be determined using the table below.

SERC expects new Penalties and Sanction Guidelines will be field tested in early 2007. If a field test is performed, a letter providing information on the prospective penalties or sanctions will be sent to the Executive Signatory making the compliance filing, the SERC Board representative, the compliance contact and the appropriate compliance review committee and the Compliance Oversight Group.

## NERC Compliance Enforcement Table October 4, 2002

Notes:

- (1) Operating measure violations are subject to **both** monetary fines and sanction letters.
- (2) All monetary penalties will be the greater of the fixed dollars or \$ per MW, shown above.
- (3) Planning measure violations are **only** subject to sanction letters

Number of Violations at a Given Level within Occurrence Period				
No Violations in Occurrence Period	1	2	3	4 or more
<b>2<sup>nd</sup> Consecutive Period of Violations</b>		1	2	3 or more
		\$ Sanction from Table; Letter (C) only if Letter (B) previously sent		
<b>3<sup>rd</sup> Consecutive Period of Violations</b>			1	2 or more
			\$ Sanction from Table; Letter (C) only if Letter (B) previously sent	
<b>4<sup>th</sup> or greater Consecutive Period of Violations</b>				1 or more
				\$ Sanction from Table; Letter (C)
<b>Level of Non-Compliance</b>				
<b>Level 1</b>	Letter (A)	Letter (A)	Letter (B) and \$1000 or \$1 per MW	Letter (B) and \$2000 or \$2 per MW
<b>Level 2</b>	Letter (A)	Letter (B) and \$1000 or \$1 per MW	Letter (B) and \$2000 or \$2 per MW	Letter (B) and \$4000 or \$4 per MW
<b>Level 3</b>	Letter (B) and \$1000 or \$1 per MW	Letter (B) and \$2000 or \$2 per MW	Letter (B) and \$4000 or \$4 per MW	Letter (B) and \$6000 or \$6 per MW
<b>Level 4</b>	Letter (B) and \$2000 or \$2 per MW	Letter (B) and \$4000 or \$4 per MW	Letter (B) and \$6000 or \$6 per MW	Letter (B) and \$10,000 or \$10 per MW

***Letter Distribution:***

Letter (A): Letter to the entity's Vice President Level or equivalent informing the entity of non-compliance, with copies to the data reporting contact, and the entity's highest ranking Regional Council representative.

Letter (B): Letter to the entity's Chief Executive Officer or equivalent, with copies to the data reporting contact, the entity's highest ranking Regional Council representative, and the Vice President over the area in which noncompliance occurred.

Letter (C): Letter to the entity's Chief Executive Officer and Chairman of the Board, with copies to the NERC President, regulatory authorities having jurisdiction over the noncompliant entity if requested by such regulatory authorities, the data reporting contact, the entity's highest ranking Regional Council representative, and the Vice President over the area in which noncompliance occurred.

Notes:

- (1) Letter C is only issued when consecutive repeat violations have occurred and Letter B has previously been sent to the entity's CEO.
- (2) A Region may, at its discretion, distribute sanction letters to regulatory authorities and higher levels of management within the noncompliant organization beyond what is specified by this NERC requirement.

***General:***

The Compliance Enforcement Table is designed to address penalties for violations of the same measure occurring in consecutive reporting periods (e.g. BAL-001 violations in back to back months).

If a participant continues to have non-compliant performance in the next (second) consecutive reporting period, the violation column shifts to the right and the penalties are calculated starting in the second column. If non-compliant performance continues for four or greater reporting periods, the violation column is the farthest to the right.

# **Appendix J**

## **Cyber Security Standards Measurements**

**Appendix J** – All of the Cyber Security Standards contained within this appendix are part of the SERC Compliance Program. The table below provides a summary of the measures SERC will monitor in the compliance program. The version in effect at the time it is monitored is the version assessed for compliance. All the standards in effect are listed on the NERC website at –

[http://www.nerc.com/~filez/standards/Reliability\\_Standards.html](http://www.nerc.com/~filez/standards/Reliability_Standards.html).

Refer to this website for the latest version and the effective date of the requirements.

<b>Std #</b>	<b>Requirements</b>	<b>Standard</b>	<b>Who</b>	<b>Purpose</b>	<b>Self-Certification</b>	<b>Monthly/Quarterly Reporting</b>	<b>Data Submission</b>	<b>Exception Reporting</b>	<b>Investigation</b>
CIP-002-1 through CIP-009-1	All	<b>Critical Infrastructure Protection Standards</b>	BA, GO, GOP, IA, LSE, NERC, RC, TO, TOP, TSP	Cyber Security Standards- Follow revised Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1	√				

## **Appendix K**

### **SERC Procedure for Reporting Compliance Violations to NERC**

## Appendix K - SERC Procedure for Reporting Compliance Violations to NERC

The following description describes the process used for reporting violations to NERC. There are 3 types of compliance activities that are reported to NERC.

- Normal compliance filings that are made by Self-Certification or Letter of Certification (LOC), and monthly filings for operating measures and vegetation outages.
- For standards that fall under the 48 Hour Rule Violation Reporting Form, the initial determination for reporting to NERC of a 48 hour rule filing will be after review by the appropriate committee chair or vice chair (CRSC, CS, or CSCRS). The measure, level and identity of the member, as a minimum, will be reported. Further reporting would be done after the full committee review. This may be done by a meeting or by conference call.
- Initial determination for reporting to NERC of all violations assessed at an audit will be after the full 14 day review and comment period by the member.

The violations will be reported subject to the NERC SERC Confidentiality Agreement terms. Violations still under investigation will be reported on a confidential basis. Violations for which the compliance process has been completed, will be reported as confirmed and complete and under the terms of the agreement can be posted on the NERC website.

For each violation the entity will have the opportunity to provide a statement to accompany the report of the violation to NERC. If the entity desires to provide such a statement it should be in letter format on the entity's letterhead with the name, signature, and title of the person providing the statement. The statement will be posted on the NERC public website and should address the effect on the bulk system reliability, seriousness of the violation, other matters that will assist in explaining the violation to the public, or other statement the member may choose to make.