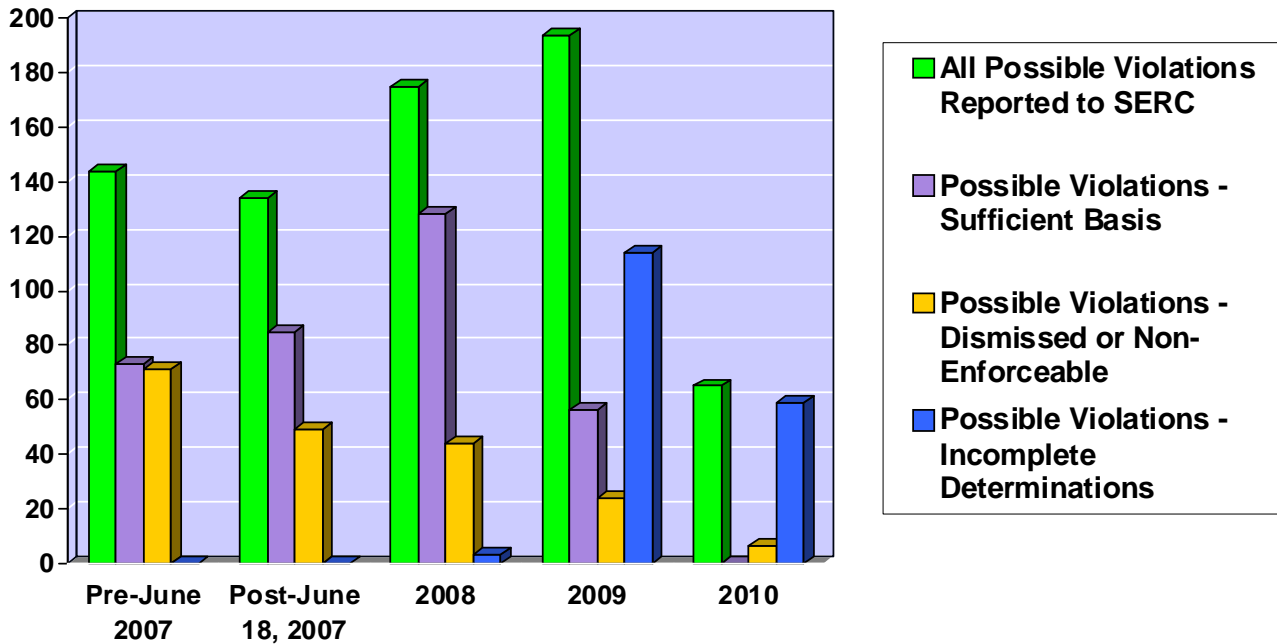


SERC Reliability Corporation

COMPLIANCE STATISTICS (PRE AND POST JUNE 18, 2007 THROUGH FEBRUARY 19, 2010)

*All Possible Violations Reported to Region as of February 19, 2010 **



	Pre-June 18, 2007*	Post June 18, 2007	2008	2009	2010
All Possible Violations Reported to SERC	144	137	175	194	65
Possible Violations Sufficient Basis – Determination Complete	71	84	128	58	0
Possible Violations Dismissed or Non-Enforceable	73	53	44	26	6
Possible Violations with incomplete determinations	0	0	3	110	59

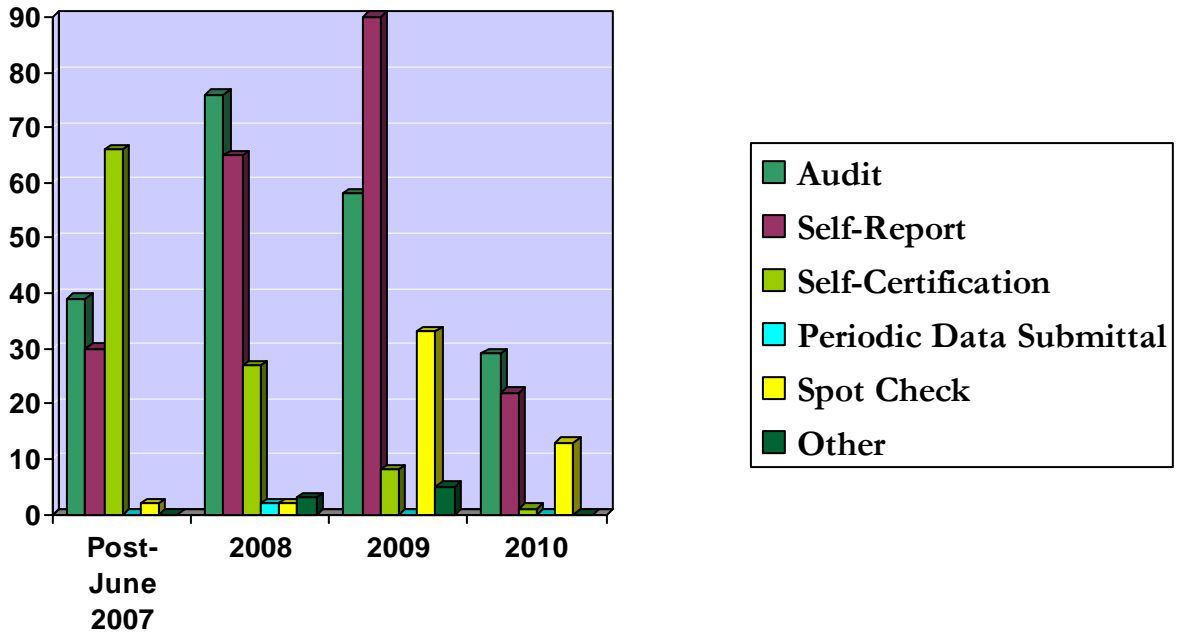
*Pre-June issues are based on a single standard and could have multiple requirements associated with that standard. All other information is reported on a requirement basis.

Of the 169 possible violations with incomplete determinations from 2009 and 2010, almost 50% are possible violations of CIP-002-009 standards.

The three 2008 issues with incomplete determinations are associated with an ongoing investigation which has not yet been completed.

SERC Reliability Corporation

Monitoring Sources for Possible Violations by Requirement as of February 19, 2010*

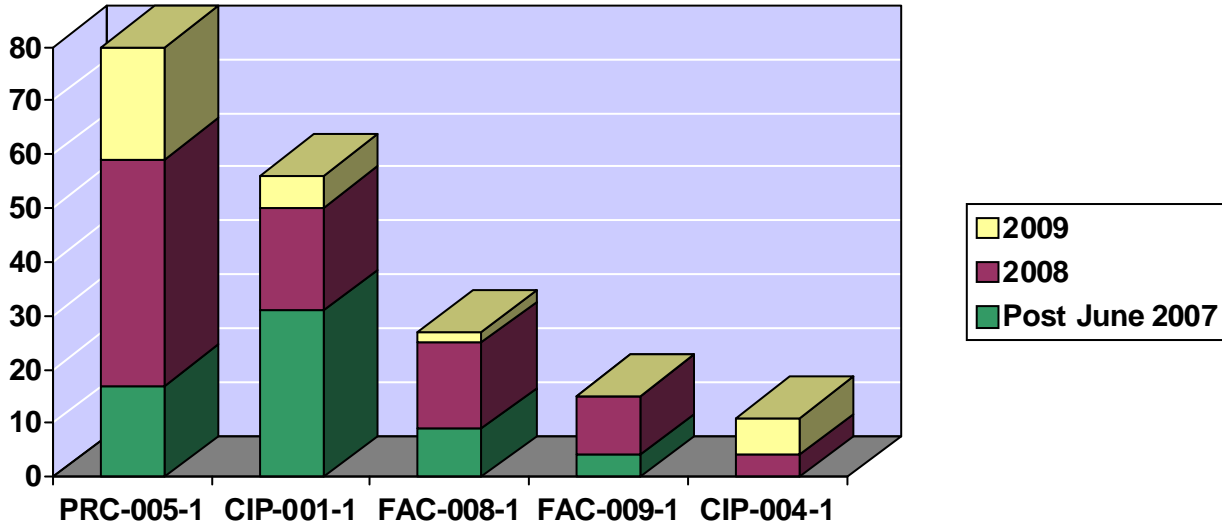


	Post-June 2007	2008	2009	2010
Audit	39	76	58	29
Self-Reporting	30	65	90	22
Self-Certification	66	27	8	1
Periodic Data Submittal	0	2	0	0
Spot Check	2	2	33	13
Other	0	3	5	0
Totals	137	175	194	65

*Pre-June issues are based on a single standard and could have multiple requirements associated with that standard. All other information is reported on a requirement basis.

SERC Reliability Corporation

Possible Violations Reported by Standards

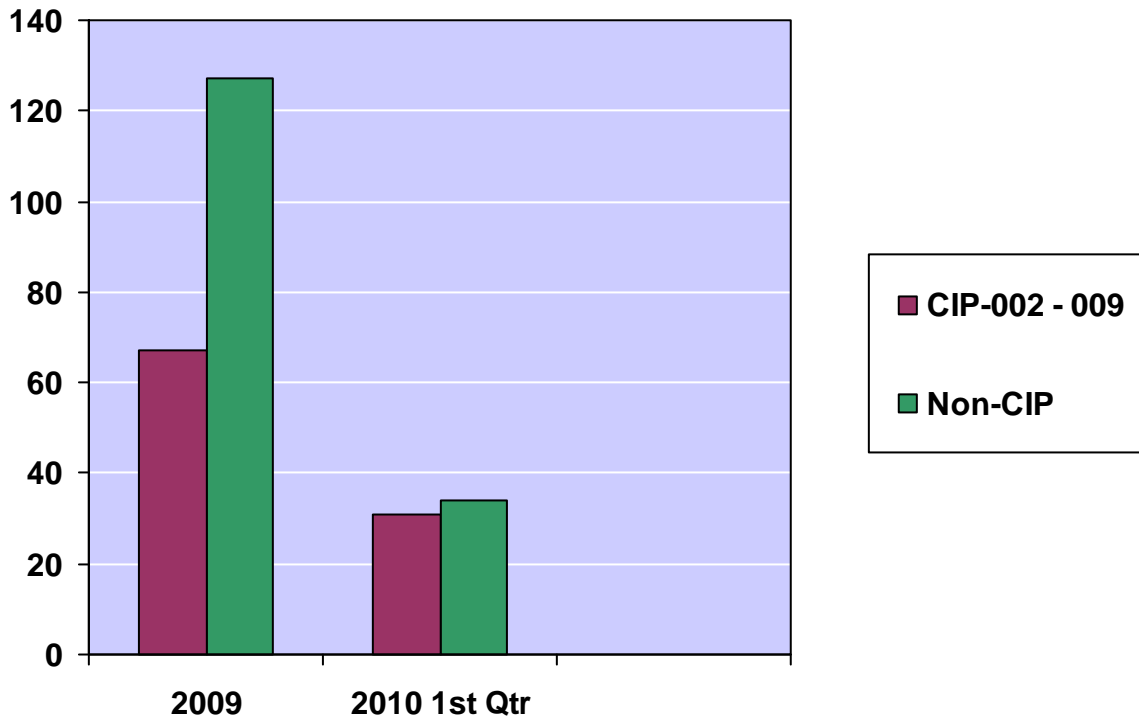


Top 5 Post-June Possible Violations Reported by Standard and Requirement and Deemed to Have Sufficient Basis – Determination Complete as of February 19, 2010

Standard, Requirement	Post-June 2007	2008	2009
CIP-001-1			
R1	7	6	1
R2	7	4	1
R3	7	4	2
R4	10	5	2
PRC-005-1			
R1	14	22	8
R2	3	20	18
FAC-008-1			
R1	9	16	2
FAC-009-1			
R1	3	11	0
R2	1	0	0
CIP-004-1			
R2	0	1	3
R3	0	1	1
R4	0	2	3

SERC Reliability Corporation

Cumulative Possible Violations Reported by Quarter as of February 19, 2010. CIP-002 through CIP-009 versus Non-CIP

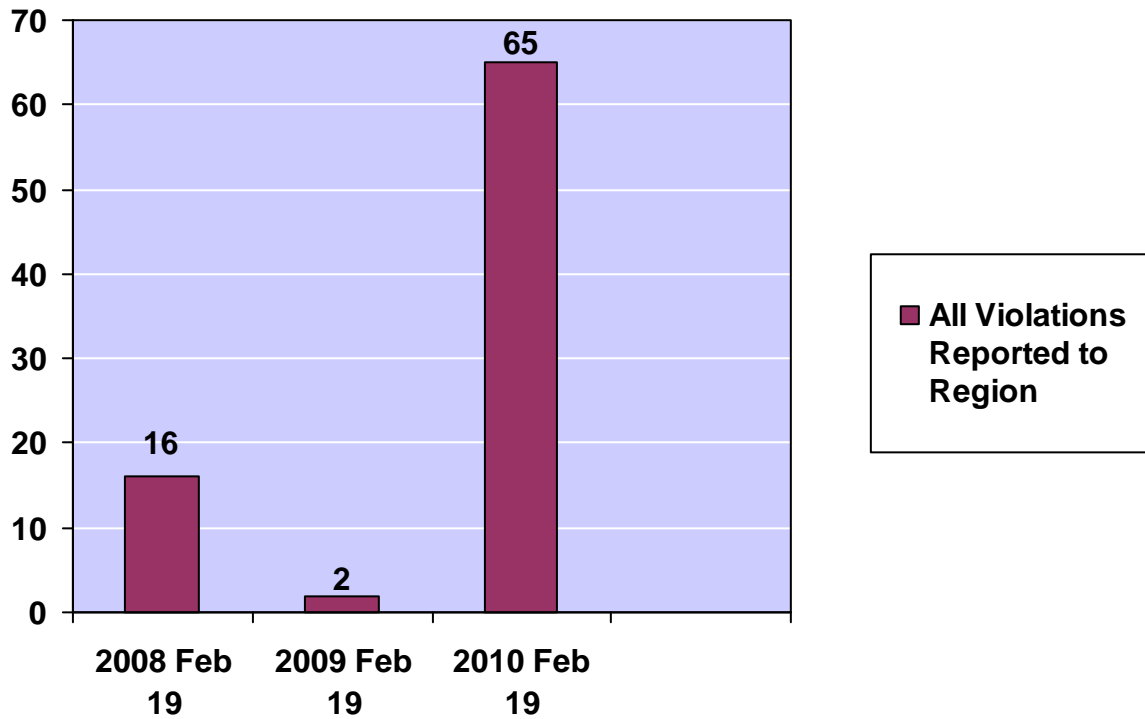


Recently, there has been a large increase of possible violations identified for the CIP Standards (CIP-002 through CIP-009). Of the 194 possible violations reported to SERC in 2009, approximately 34% involved CIP-002 through 009. In 2010, approximately 48% of the possible violations identified involve CIP-002 through 009. Most of the CIP possible violations are still in the “determination” state. These possible violations are more complex and require specific expertise. The scope of CIP possible violations is expected to increase as more entities reach “compliant” dates.

Note that possible violations of CIP-001 are included in the Non-CIP category.

SERC Reliability Corporation

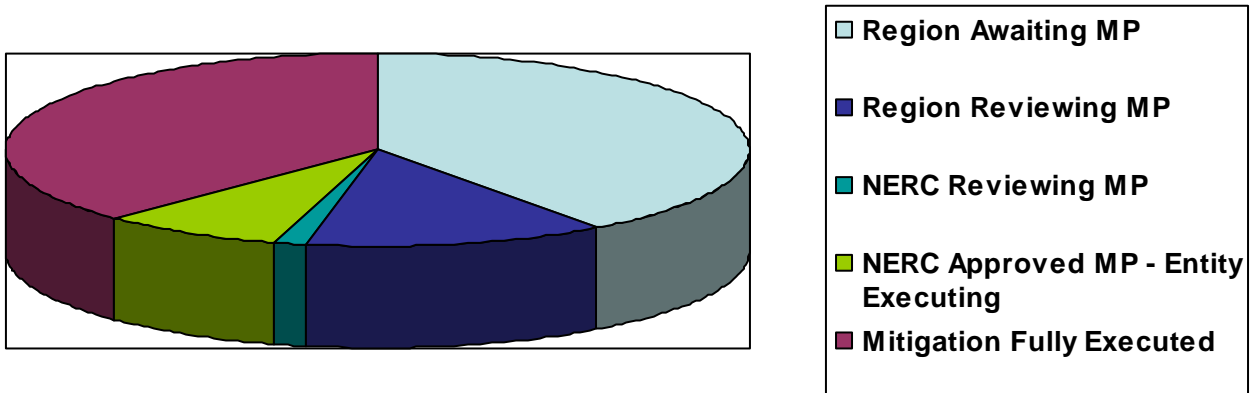
All Possible Violations Identified Year-to-Date



SERC has seen a significant increase in the number of possible violations reported in 2010. To date, approximately 48% of the issues identified in 2010 involve CIP-002 through 009.

SERC Reliability Corporation

Mitigation Plan Status for 2008, 2009, and 2010 Possible Violations Reported to NERC as of February 19, 2010



Region Awaiting MP	Region Reviewing MP	NERC Reviewing MP	NERC Approved MP – Entity Executing	Mitigation Fully Executed	Total MP
143	47	5	29	134	358

This table includes Mitigation Plans that the region has not completed the determination.

SERC Guidelines for Submission of Mitigation Plans

To assist entities in preparation of an acceptable Mitigation Plan, submission guidelines can be found on the SERC public website in the Compliance section under the Mitigation Plan Submittal Form link. The link to the guidance document is listed below:

<http://www.serc1.org/Documents/Compliance/Compliance%20Implementation/SERC%20Guidelines%20for%20Mitigation%20Plan%20Submission.pdf>

Mitigation Plan Completion Dates

SERC Compliance Staff reminds Registered Entities who are preparing or completing Mitigation Plans that there is a high degree of importance attached to the dates the Registered Entity identifies as the date upon which the Mitigation Plan will be completed. The date specified for completion on the Mitigation Plan is deemed a significant contractual obligation of the Registered Entity, reflecting when the possible or alleged violation will be remedied and risk to



SERC Reliability Corporation

reliability of the bulk-power system will be alleviated. Failure to complete the Mitigation Plan on or by that date can result in additional compliance enforcement actions and additional penalties may be applied.

For that reason, care should be taken to establish a completion date that will restore compliance within a reasonable period and also accommodate any internal review and approval processes that will be necessary to complete the plan. SERC Compliance Staff discourages establishing a completion date that falls on a Friday, weekend, or holiday. There have been a number of cases in which a Registered Entity had specified a Friday, weekend or holiday date as its Mitigation Plan completion date and, because of unavailability of individuals to finalize execution of required action or approve required policies or procedural documents, was unable to complete its Mitigation Plan on time. SERC Compliance Staff also reminds Registered Entities not to wait until the last several days prior to the specified Mitigation Plan completion date before finalizing actions, such as conducting required training and obtaining executive sign off of required documents, in the event unexpected absences prevent timely completion.

If, despite appropriate considerations, it appears that an extension of the specified Mitigation Plan closure date is necessary, the extension request must be made at least five business days before the date specified on the Mitigation Plan (see CMEP 6.0). Extension requests must state the basis for the delay in completion. SERC will approve requests for an extension on a case-by-case basis if it determines the need for the extension is justified, taking into account the scope of the issue being mitigated, the length of the requested delay in completion, the evidence in support of extension, and the potential risk to reliability of the bulk-power system.

General Support:

For additional Lessons Learned and other support documents for strengthening your overall compliance program, please visit the Regional Entity Common Web Compliance tab at <http://www.regionaleentities.org/ComplianceHome.aspx>. The lessons learned section is under the CIMG tab and information on attributes of a good compliance program is under the RCIG tab.

General Observations and Lessons Learned for 2010:

February Featured Standard:

Each month, SERC staff will feature a specific Standard or guidance in this section. If there is a Standard that you would like to see featured, please email serccomply@serc1.org.

The February feature is guidance on possible violations of PRC-005 R2. (see page 10 for additional information regarding PRC-005).

If a potential violation of PRC-005 R2 is identified by any discovery method, Entity should be prepared provide to SERC staff assessing the violation, information regarding their Protection System which should include:

- The number of devices in each of the defined elements of the Protection System - Protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry.

SERC Reliability Corporation

- Evidence that all Protection System devices were maintained and tested within the defined intervals (R2.1.). For each type of device, indicate the total number of instances that evidence was missing.
- Evidence of date each Protection System device was last tested/maintained (R2.2.)
- For each test interval missed on each device, describe the condition of the device during the test interval immediately **prior** to the missed test interval. Specifically, was the device working and in good condition during the test interval immediately prior to the missed test interval? In addition, for each test interval missed on each device, describe the condition of the device during the test interval immediately **following** the missed test interval.
- Provide a copy of the Maintenance and Testing Program in place at the time the possible violation occurred.

General Observations and Lessons Learned in 2010:

FAC-008-1 and FAC-009-1

In instances where the audit team finds a flaw in Entity's Facility Rating Methodology (FRM) under FAC-008-1 and that flawed methodology is applied as required in FAC-009-1, the audit team does not flag FAC-009-1 as being in possible violation when a documented FRM has been applied as required by Entity's FRM. The audit team will flag FAC-009-1 as a possible violation if a documented FRM is not applied as written.

Entities found in violation of FAC-008-1 are required to revise their FAC-009-1 ratings to be consistent with their corrected methodology as part of their mitigation of the violation of FAC-008-1.

Entities are strongly encouraged to ensure that their Facility Ratings are properly communicated to the appropriate entities, without request from these entities, after correcting a flawed FRM.

General Observations and Lessons Learned in 2009:

CIP-001-1 (Sabotage Reporting)

- Requirement 1 - Failure to include process for identification of sabotage
- Requirements 1 and 3 – Entity procedures don't address lateral or downward communication of a sabotage event (providing operating personnel with response guidelines and making operating personnel aware of events - communication across organization rather than just to law enforcement authorities and management). Anyone in an organization could receive a threat or notice of a sabotage event. All operating personnel must be aware of the procedure for communicating the threat to the proper personnel. Communication of an event or threat must be made to all operating personnel and to neighboring entities, as applicable.
- Requirement 4 – No evidence that contact has been established with the FBI for purposes of reporting sabotage events. Some entities are confused because their first responders are local authorities (Sheriff, Local Police), not the FBI. Contact must be established with the FBI, as well as the local authorities. The FBI may direct that local authorities be contacted, who will in turn contact the FBI; but this direction must be documented. New guidance has been issued from NERC regarding this requirement.

SERC Reliability Corporation

The guidance is located in the updated Reliability Standard Audit Worksheet (RSAW) for CIP-001-1 R4.

CIP-004-1 (Personnel & Training)

The Regional Compliance Implementation Group (RCIG) has recently posted a white paper detailing the *RCIG Assessment on Monitoring and Implementation of Reliability Standard CIP-004-1 Cyber Security – Personnel and Training*. The white paper is posted on the Regional Entity Common Website at the following link:

<http://www.regionalentities.org/Documents/Compliance/RCIG/RCIG%20Assessment%20CIP-004.pdf>

SERC has reviewed possible violations on CIP-004 R4:

- Several reasons entities have not adequately maintained the physical and electronic access lists and access rights according to the standard are:
 - The official report, that lists who has access, fails to list everyone that has access. Due to the omissions, Entity thought certain individuals did not have access when in fact the individuals still had access.
 - Entity software to automatically remove access to an individual when they no longer worked in a secure area failed to work properly and the access was not revoked on time.
 - Entity failed to consider all access methods into a secured area. Individuals with master keys to gain emergency access to secure areas were not properly accounted for.
 - Entity revoked access by manually confiscating access cards. Due to logistics, not all access cards were confiscated within the time allowed.

Clarification on CIP-004 R4 and the possible overlap of the two sub-requirements

R4.1 states:

“The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets...”

R4.2 states:

“The Responsible Entity shall revoke such access to Critical Cyber Assets ...within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.”

Question: Can an entity rely solely on the quarterly review of the access lists (that is required in R4.1) to identify personnel that no longer require Critical Cyber Access and then revoke their access within seven days of the quarterly review and be compliant with R4.2?

Response: An entity can not rely solely on the quarterly review for identifying personnel that no longer require access. Where the date that an individual no longer needs access is known, e.g. retirement date, resignation date, transfer date, promotion date, etc. then the access to Critical Cyber assets must be revoked within 7 days of that known date.

The quarterly review is intended to identify personnel, who no longer need access, but did not have a specific date associated with no longer needing access. For example, a person was

SERC Reliability Corporation

given physical access to the control center, but during the quarterly review it was discovered that the person has never used that access and per the company's Corporate Security Policy, anyone not using their access during the previous quarter will have that access revoked. This access needs to be revoked within 7 days of the quarterly review.

For an official interpretation a request needs to be submitted to NERC.

FAC-008-1 (Facility Rating Methodology)

Examples of deficiencies identified with respect to FAC-008 include:

- Entity could not produce a written Facility Rating Methodology, for its solely and jointly owned Facilities
- Entity's Facility Rating Methodology did not include a statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility
- The scope of equipment addressed by the Facility Rating Methodology did not include all equipment used to create and transmit electric power (e.g., for Generator Owners, beginning with the generator and considering generator auxiliaries such as excitation equipment, through the facilities point of interconnection or demarcation, whichever is greater)
- The Facility Rating Methodology did not address both the normal and emergency ratings, if applicable, and a statement explaining that both ratings are the same and why
- The Facility Rating Methodology did not identify how the following items (from R1.3 are considered:
 - the source of the ratings for individual equipment (design criteria, nameplate ratings, etc),
 - how equipment ratings are affected by ambient temperatures, or a statement indicating that the equipment is not affected, if applicable
 - operating limitations of the equipment,
 - a listing of other assumptions, or a statement that no assumptions were made

PRC-001-1 — System Protection Coordination

R1. Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of protection system schemes applied in its area.

SERC will enforce this issue at the operator level – expecting the actual operator or an on-shift supervisor to have sufficient knowledge of the purpose and limitations of the protection system schemes applied in its area to ensure an appropriate action or non-action is taken in response to a relay operation in its area.

PRC-005-1 (Transmission and Generation Protection System Maintenance and Testing)

The Regional Compliance Implementation Group (RCIG) has recently posted a white paper detailing the *RCIG Assessment on Monitoring and Implementation of Reliability Standard PRC-005-1 Transmission and Generation Protection System Maintenance and Testing.* The white paper is posted on the Regional Entity Common Website at the following link:

<http://www.regionalentities.org/RegionalComplianceImplementationGroup.aspx>

SERC Reliability Corporation

PRC-005-1- General Guidance

Review your PRC-005 Transmission and Generation Protection System Maintenance and Testing procedure and verify that you have included **all** five of the required elements of a Protection System --- protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry --- or clearly state “not applicable,” and any reasons why not.

Your procedure must also include maintenance and testing intervals and their basis, a summary of maintenance and testing procedures, as well as evidence (including dates) that they were last maintained and tested with-in the defined intervals.

Key issues identified in the implementation of PRC-005

- R1 & R2- Failure to recognize definition of “Protection System” (from Glossary) and failure to include all aspects of all equipment included in definition
- Failure to provide documentation that each class of equipment was receiving maintenance at the specified interval.

Secondary issue identified in the implementation of PRC-005

- R1- Missing summary of maintenance and testing procedures and/or basis for each maintenance interval

Issues to be mindful of in regard to PRC-005-1 R1:

- Maintenance and Testing Intervals- Periodicity
- Basis- Can you document why you picked this particular interval?
 - Manufacturer recommended
 - Experience
 - Other
- Summary of Maintenance and Testing Procedures
 - Synopsis of work to be performed

Issues to be mindful of in regard to PRC-005-1 R2:

- Evidence Protection System devices were maintained and tested
 - Invoices
 - Work management entry
 - Processed work orders
 - Relay and battery test sheets
- Date maintained

PRC-005 Entity Example of Lesson Learned - Relay Review

Details of Review Performed:

Entity conducted a detailed review of the protective relaying systems installed on all generators to ensure that all relays that should be within the scope of the Protection System maintenance and testing program had been identified. This review was conducted in response to a recent discovery that several medium to low voltage transformer protective relays had the ability to trip the generator through unit lockout relays. Typically, this protective relay application would sever the power source to any fault it detects by tripping a medium voltage circuit breaker and would not have the potential to affect the reliability of the bulk-power system. This particular location’s design did not include this disconnect means, so isolation of the faulted section of the power

SERC Reliability Corporation

distribution system monitored by this relay would be accomplished by tripping the generator. The review of the protective relaying systems included specifically looking for any other similarly designed plants to check for any inadvertent omission of protective relays with similar tripping. In addition, every installed protective relay was individually considered to determine if it had the potential to affect the reliability of the bulk-power system. The scope of the review included generator protective relaying, generator step-up transformer protective relaying, and unit auxiliary station service transformer protective relaying which, if operative, will result in the loss of generation. Each relay application was reviewed to determine what equipment may be tripped by the relay. This equipment could include the generator, the main bank, the running bank, or the station service buses. Where the tripping schematics, relay connection, or relay functions were not clearly known, research into the plant/unit specific elementary diagrams was conducted. Plant and transmission single line diagrams for all units mentioned above were reviewed where there was uncertainty as to their configuration to ensure that the protective relay listing is complete.

A team of six electrical engineers spent 600 hours reviewing the single line diagrams, elementary diagrams, relay applications, PEDs databases and relay indices. The goal of the review was to ensure that the relay classifications are consistent with Protection System maintenance and testing program. Protective relays are classified pursuant to the Protection System maintenance and testing program in accordance with their potential to affect the reliability of the bulk-power system. A secondary goal of the review was to ensure that the basis for determining the scope of the affected relays is equally applied at all plants.

Lessons Learned:

- Consider any station service protective relaying that can trip the unit either directly or indirectly using lockout relays.
- If there is no isolating circuit device between the equipment being protected and the generator terminals, a study of the tripping elementary diagram is indicated to verify unit lockout and shutdown capability.
- Physical inspection may be necessary to confirm the drawing accuracy.
- Be sure to read the SERC Maintenance and Testing Supplement to determine which Protections Systems are covered by PRC-005.
- Rule of Thumb – If any device can remove generation or transmission capability from the Bulk Electric System without operator action, it probably should be included in the scope of your Protective System program.

Battery Maintenance and PRC-005-1 R2

Recently, SERC Reliability Corporation had seen a spate of self-reports regarding station batteries that are included in the definition of Protection Systems as included in the NERC Glossary. In each case, the batteries at certain facilities (primarily registered Generator Owners) were not being maintained within the intervals specified by entity's maintenance program. In short, the problem appears to be a lack of clear understanding of the reliability requirements at differing levels of the organizations involved.

The NERC Glossary of Terms used in Reliability Standards defines Protection Systems as "Protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry." Typically, maintenance of batteries occurs with multiple periodicity; often weekly, monthly, quarterly, and annually. The subject self-reports all

SERC Reliability Corporation

dealt with entities where maintenance personnel were not performing all or were not performing within the defined intervals all the maintenance required by entity's preventative maintenance program. In other cases the documentation of the battery maintenance performance within the specified intervals was not sufficient to support compliance with the requirements. SERC Staff determined from communications with entity, that apparently the requirements contained within the Reliability Standards were not adequately communicated to individuals actually responsible for the oversight and execution of the maintenance activities, often in locations other than a corporate office.

SERC Staff has observed a mitigating action for these violations has been for the individuals responsible for disseminating the requirements of PRC-005-1 to personnel reiterate to the individuals actually responsible for the oversight and execution of the maintenance activities that the standard requires "Evidence Protection System devices were maintained and tested **within the defined intervals.**" [emphasis added]. These actions also included ensuring the expectations regarding appropriate evidence to demonstrate compliance were communicated to the responsible personnel. Additional mitigating actions have included updates and tighter controls around the entity maintenance tracking software, as well as, shifting responsibility for self-certification sign-off to a person more closely aligned with the assets involved (station superintendent or maintenance manager).

Documentation Suggestions:

A number of alleged violations are a result of insufficient documentation issues. SERC staff has compiled a list of suggestions to assist entities in strengthening Standards documentation.

- Since the burden of proof to show compliance is with the entity being audited, each entity should be ready to show the specific portion of each document that demonstrates their compliance with a Standard. At a minimum, the entity should know and be able to point to these specific sections.
 - As a best-practices technique, consider highlighting the specific words or sections in either a .DOC or .PDF version.
- Entities often provide SERC with documents containing creation and review dates close to the dates of the audits. Compliance auditors will also request previous versions of documentation to verify compliance from the date the standard became enforceable or from the previous audit.
- Incorporate revision numbers and tracking to your documents.
- Consider annual reviews of documents and procedures.