3rd Quarter 2012 Lessons Learned from Dismissals

Standard	Requirement	Reason for Reporting Violation	Reason for Dismissal	Dismissal Lesson	NERC Violation ID Reference
CIP-006-1	R1	The Entity self-reported a possible violation for CIP-006-1, R1 because as a result of its certification review process the Certification Team did not find the Entity had documented all access points to the Back Up PSP. As a result, Texas RE initially determined the Entity was in violation with CIP-006-2, R1 because the PSP did not include the "identification of all…measures to control entry at those access points", an "update of the physical security plan within thirty days of the completion of any physical security system redesign or reconfiguration, including…monitoring controls", nor a "annual review of the physical security plan".	The Entity provided additional information which indicated on April 28, 2010, the cameras inside the PSP became active and was added to the drawing dated May 11, 2010. Upon review of this evidence, Texas RE determined that the Entity had no finding of non-compliance with CIP-006-2, R1 because the drawing dated May 11, 2010 reflected the addition of the cameras. The drawings were timely updated identifying all measures to control entry at access points, as required by the Standard.	An Entity is able to provide alternative evidence to demonstrate compliance if the evidence is determined to meet the requirement's purpose and intent. If an Entity is unsure whether it complied with a standard, it can self-report and review its compliance with Texas RE. If an entity has discovered additional information after the initial self-report, that information should be provided to Texas RE.	TRE201000174
CIP-001-1	R2	The Entity's documented sabotage response procedures did not include complete information regarding communication of information concerning sabotage events to appropriate parties in the Interconnection.	The Entity provided Texas RE with its "Incident Notification Procedure" as well as its "Bomb Threat and Security Incident Procedure" (in place prior to January 1, 2010). Both of these documents state the Entity shall notify its QSE in the event of sabotage. The Entity was able to provide a QSE procedure (also in place prior to	An Entity is able to provide alternative evidence to demonstrate compliance if the evidence is determined to meet the requirement's purpose and intent. The evidence can include older	TRE2012009950

			January 1, 2010), detailing its process for notifying the local BA, RC and TOP. The Entity was able to provide pictures of the QSE's Operator desks, demonstrating that the local Transmission Operators were available on speed dial.	procedures in place prior to the Requirement enforceable date. If certain duties are contracted, the entity should be able to show the requirement is being met.	
CIP-001-1	R4	The Entity's documented sabotage response procedures did not include contacts and reporting procedures regarding communication of information concerning sabotage events to the Federal Bureau of Investigation.	The Entity followed a procedure developed under other federal guidelines. According to this document, the Entity designated a "Facility Security Officer", who was tasked with contacting the local FBI/Joint Terrorism Task Force. The Entity provided an attestation towards the validity and timeframe of the document referenced above. Furthermore, the Entity was able to provide evidence that it has been in contact with FBI personnel since January 4, 2007.	An Entity is able to provide alternative evidence to demonstrate compliance if the evidence is determined to meet the requirement's purpose and intent. There may be procedures developed under other guidelines and requirements that meet the Standard requirement.	TRE2012009951
PRC-005-1	R1	The Entity submitted a self-report indicating its January 2007 Protection System Maintenance and Testing Program did not document the DC Control Circuitry maintenance and testing procedures. The Entity provided an attestation stating the DC Control Circuitry	Upon further review, Texas RE determined the Entity's Protection System Maintenance and Testing January 2007 Program included DC Control Circuitry maintenance and testing procedures, but the identifying language was not easily identifiable until	An Entity is able to show compliance by communicating with the Regional Entity to address and clarify ambiguous language in their procedures. Procedures should clearly address all the	TRE201100311

		was being tested within 5 year intervals, despite its absence from the procedures. As a result, Texas RE initially determined the Entity was in noncompliance with PRC-005-1, R1.2.	subsequent discussions between the Entity and Texas RE. The Entity revised its Generation Protection System Maintenance and Testing Program document to include clarifying testing and maintenance procedures language for the DC Control Circuitry.	components on the requirements	
CIP-004-3	R4	The Entity submitted a self-report addressing a possible noncompliance of CIP-004-3 R4.2. The Entity assumed that physical access for an IT employee who resigned on March 23, 2012 was not revoked until the automated removal process occurred on April 2, 2012.	After reporting the violation, the Entity discovered the self-report was not necessary since the employee was removed from the system within the required timeframe. It was later determined that physical access for this employee was manually removed on March 28, 2012 when the individual's badge was turned into Security Services. Access was removed five days following resignation.	If an Entity is unsure whether it complied with a standard, it can self-report and review its compliance with Texas RE. If an entity has discovered additional information after the initial self-report, that information should be provided to Texas RE.	TRE2012010576