



Compliance Audit Report Public Version

**Georgia Transmission Corporation
NCR01249
June 18-19, 2008**

**Confidential Information (including
Privileged and Critical Energy Infrastructure
Information) – Has Been Removed**

July 22, 2008

TABLE OF CONTENTS

Executive Summary	3
Audit Process	3
<i>Objectives</i>	3
<i>Scope</i>	4
<i>Confidentiality and Conflict of Interest</i>	4
<i>On-site Audit</i>	4
<i>Methodology</i>	4
<i>Audit Overview</i>	5
<i>Audit</i>	5
<i>Exit Briefing</i>	6
<i>Company Profile</i>	6
<i>Audit Specifics</i>	6
Audit Results	7
<i>Findings</i>	7
<i>Compliance Culture</i>	14

EXECUTIVE SUMMARY

This final compliance audit report is the public version. Confidential information (including privileged and critical energy infrastructure information) has been redacted from this report. The full final compliance audit report was submitted to the audited entity and NERC.

Georgia Transmission Corporation (GTC) was audited on June 18-19, 2008 for compliance with the requirements contained in the currently mandatory and enforceable Reliability Standards in the 2008 NERC Compliance Monitoring and Enforcement Program (CMEP) that are applicable to GTC's registered functions. GTC is registered with SERC Reliability Corporation (SERC) as a Transmission Owner (TO), Transmission Service Provider (TSP), Transmission Planner (TP), Distribution Provider (DP) and Planning Authority (PA). Twenty standards were selected and identified to GTC as subject to review during this audit. The audit focused on documents and other evidence provided to SERC by the staff of GTC, and did not include any evidence obtained through system observation or inspection. The findings of the audit are based on the state of compliance and current mitigation activity at the time of the audit, and do not reflect past compliance activities or activities that will be completed in the future. GTC staff provided an informational presentation on their progress with implementation of Cyber Security Standards CIP-002-1 through CIP-009-1.

GTC staff was requested to provide valid evidence of meeting each and every applicable requirement and sub-requirement contained in each standard that had been previously identified by SERC Compliance staff to GTC as subject to this audit. GTC staff responded by providing evidence in the form of reports, procedures, studies, and other documents. GTC staff then cited specific portions of the evidence that demonstrated compliance. This evidence and the citations were documented and evaluated by the audit team to assess the level of compliance. If all of the requirements and sub-requirements of an audited standard were met, then GTC was judged to be compliant. Likewise, if any of the requirements or sub-requirements were not fully met, then GTC was judged to have a possible violation of the standard. A score of 100% is required for compliance.

The audit team found GTC to be in compliance with all of the NERC Reliability Standards in the audit scope.

AUDIT PROCESS

The compliance audit process steps are detailed in the NERC CMEP. The NERC CMEP generally conforms to the United States Government Accountability Office Government Auditing Standards and other generally accepted audit practices.

Objectives

All registered entities are subject to audit for compliance with all reliability standards applicable to the functions for which the registered entity is registered.¹ The audit objectives are:

- Independently review GTC compliance with the requirements of the reliability standards that are applicable to GTC based on the GTC registered functions.
- Validate compliance with applicable reliability standards from the NERC 2008 Implementation Plan list of actively monitored standards.

¹ North American Electric Reliability Corporation CMEP, paragraph 3.1, Compliance Audits

- Validate evidence of self-reported violations and previous self-certifications, confirm compliance with other requirements of the reliability standard, and review the status of associated mitigation plans.
- Document the GTC compliance culture.

Scope

The scope of the audit of GTC included all monitored standards that are in the NERC 2008 CMEP. Based on the confirmed registration of GTC, the twenty Reliability Standards previously identified were the focus of the compliance audit.

Note: For the 2008 compliance program, the monitoring period for the compliance audit will generally be the past 12 months or periods specified in individual reliability standards. The monitoring period is not limited to the time period for which penalties and sanctions are assessed.

Confidentiality and Conflict of Interest

Code of conduct documentation for the NERC representative and regional entity staff were provided to GTC in advance of the audit. Work history and conflict of interest forms submitted by each audit team member were provided to GTC upon request. SERC has confirmed that confidentiality agreements have been executed by, and are on file for SERC Industry Volunteers. GTC was given an opportunity to object to an audit team member on the basis of a possible conflict of interest or the existence of other circumstances that could interfere with the audit team member's impartial performance of duties. GTC accepted the audit team member participants with no objections.

On-site Audit

GTC was contacted by letter on December 17, 2007 by SERC staff. The letter provided GTC with their initial notification of their upcoming audit in 2008, and the desire to schedule audit dates that would be acceptable to both parties. SERC staff then provided formal acknowledgement of the scheduled audit dates and requested that GTC both verify their currently registered functions and complete and return an attached Pre-Audit Survey within 30 days.

On March 21, 2008, SERC staff forwarded an Audit Detail Letter to GTC, again confirming the scheduled audit dates and confirming GTC's registered functions within SERC. The Audit Detail Letter also provided GTC with notice of the Standards in Audit Scope, Proposed Audit Schedule, Audit Team Roster (with industry affiliations), and requested that GTC Subject Matter Experts (SMEs) responsible for and knowledgeable of compliance submittals be available for interview during the audit. In addition to the Audit Detail Letter, GTC was provided with a Non-Disclosure Agreement Signature Verification for audit team members, a Pre-Audit Questionnaire, a list of Documents to be Provided or Have Available, and Reliability Standard Auditor Worksheets (RSAWs) for each standard to be audited.

Interviews with SMEs were requested, in conjunction with documented evidence, to provide the audit team with additional information or clarification as a basis for professional judgment when validating compliance with reliability standards.

Methodology

A team of auditors and SMEs were identified and conducted the audit of GTC. The standards were grouped and scheduled for review to make the most efficient use of GTC staff's time. The audit team moderator (ATL or designee) initiated dialogue on each standard requirement and

requested compliance evidence. This evidence and GTC's staff response was documented. GTC staff was requested to show valid evidence of meeting each applicable requirement and sub-requirement contained in the twenty standards that had been previously identified by SERC to GTC as subject to this audit. GTC staff responded by providing evidence in the form of reports, procedures, studies, and other documents. GTC staff would then cite specific portions of the evidence that demonstrated compliance.

This evidence and the citations were documented by the scribe on the RSAWs and evaluated by the audit team for the level of compliance and agreement with the requirement. Discrepancies between the requirement and the evidence provided were the subject of dialogue among the team members and GTC staff members until it was determined that each requirement was met by the cited evidence or other evidence offered.

Once all the evidence was presented and discussed, if GTC did not provide sufficient evidence to support a finding of compliance, then a possible violation was identified by the team and GTC staff was informed.

Audit Overview

The audit team arrived at the GTC offices at 3:40 p.m., June 18, 2008. Each member of the audit team was introduced and professional affiliation identified. The staff of GTC was introduced, and general housekeeping matters explained. Steve Gibe, Senior Compliance Auditor and Audit Team Lead (ATL) began the session with an opening presentation. He reviewed the NERC compliance plan for 2008 in general, and how it applied to GTC specifically. The ATL introduced and reviewed the standards to be covered in the audit, and addressed both the expectations of GTC staff and the quality of evidence to be presented. The ATL also covered the basic procedure for the audit, and the bounding rules of conduct. GTC staff made a brief presentation describing GTC's corporate structure, compliance program and an informational overview of progress made toward implementation of the Cyber Security Standard requirements of CIP-002-1 through CIP-009-1. The staff of GTC was excused and the audit team reviewed team assignments and a general overview for preparation of the audit activities starting on the next day.

Audit

The audit team arrived at the GTC at 7:40 a.m., June 19, 2008. The audit began at 8:00 a.m., June 19, 2008. The audit team initially reviewed the registration status of GTC with entity staff to verify applicability of each standard. Each standard's audit began with a recitation of each requirement. GTC staff then presented evidence supporting requirement compliance, or cited evidence previously provided to the audit team. At that point, the evidence was reviewed and discussed until the team reached agreement on the evidence. By audit team consensus a determination of compliance was reached for each of the requirements, and communicated to GTC staff before proceeding to the next requirement. At that point the team scribe would record the evidence presented to satisfy the requirement and the team's recommendation on that requirement using the RSAW.

The review of all applicable standards was completed at 5:01 p.m., June 19, 2008, and the audit team met to review and discuss the findings. Following these discussions, the scribe collected all notes and evidence as needed and began to finalize the RSAWs.

NOTE: Due to the nature of their business relationship, three standards, PRC-010-0, IRO-004-1 and IRO-001-1 were audited from 12:01-1:00 p.m., June 18, 2008, in conjunction with the Georgia System Operations Corporation's audit.

Exit Briefing

The ATL presented an exit briefing to the assembled audit team and entity staff at 5:36 p.m., June 19, 2008. This was followed by an informal response and questions from the GTC staff. The exit briefing summarized the team's preliminary conclusions, including any items of potential noncompliance or possible violation with supporting information, areas of concern, any added information required and the expected timeline for review and issuance of the audit report.

The ATL solicited both informal comments from GTC staff, along with requesting that they fill out formal feedback forms for submission to NERC and SERC.

The audit team left the GTC meeting room at 5:46 p.m., June 19, 2008.

Company Profile

GTC is part of a Family of Companies (FOC) who work together to provide electric service to thirty-nine Georgia EMCs (Electric Membership Corporations). The other entities in the FOC are Georgia System Operations Corporation (GSOC) and Oglethorpe Power Corporation (OPC).

GTC essentially serves as a link between power generation and the EMCs' individual electric distribution systems. Georgia Transmission plans, builds and maintains a transmission system of more than approximately 2900 miles of transmission lines: 161 miles 46 kV, 1112 miles 115 kV, 1192 miles 230 kV and 434 miles 500 kV. In addition, GTC has access to ~17,500 miles of transmission lines on the Georgia Integrated Transmission System (ITS), and is integrated with the facilities of Georgia Power Company, Municipal Electric Authority of Georgia (MEAG), and the City of Dalton, GA.

The GTC system is not a separate contiguous network. The GTC ITS facilities and other ITS facilities are interconnected at very many points within one network within the larger Southern Company footprint. Currently, GTC owns one 230 kV interconnection with the Southeastern Power Administration (SEPA).

Audit Specifics

The compliance audit was conducted on June 18-19, 2008 at the GTC office in Tucker, GA.

Audit Team

Audit Team Role	Name	Title	Company
Lead	Steve Gibe	Senior Compliance Auditor	SERC
Member	James Harrell	Senior Compliance Auditor	SERC
Member	Kevin Berent	Associate Compliance Auditor	SERC
Member	Bob Kenyon	Regional Compliance Program Coordinator	NERC

GTC Audit Participants Title and Organization

Title	GTC Organization
Compliance Manager	GTC
VP, System Planning	GTC
VP, Transmission Policy	GTC

Title	GTC Organization
VP, System Performance	GTC
VP, Operations & Maintenance	GTC
Director, Internal Audit & Compliance	GTC
Manager, System Services	GTC
Senior Engineer, System Services	GTC
Manager T/L Maintenance	GTC
System Forester	GTC
Group Lead, Bulk System Planning	GTC
Senior Engineer, Bulk System Planning	GTC
Principal Engineer, Bulk System Planning	GTC
Manager, Bulk System Planning	GTC
Principal Engineer, Bulk System Planning	GTC
Manager, System Protection & Control	GTC
Principal Engineer, Protection & Control	GTC
Principal Engineer, Protection & Control	GTC
Group Lead T/L Maintenance	GTC
Principal Engineer, Substation Maintenance	GTC
Manager, Substation Maintenance	GTC
Engineer, Protection & Control	GTC
Manager, Control Area Operations	GSOC
Manager, Operations Engineering	GSOC
Principal Engineer	GSOC

AUDIT RESULTS

The audit team found GTC to be in compliance with all of the NERC Reliability Standards in the audit scope. Please see Findings Table below.

Findings

Reliability Standard	Requirement	Finding
BAL-001-0	R1.	N/A
BAL-001-0	R2.	N/A
BAL-001-0	R3.	N/A
BAL-001-0	R4.	N/A
BAL-002-0	R1.	N/A
BAL-002-0	R2.	N/A
BAL-002-0	R3.	N/A
BAL-002-0	R4.	N/A
BAL-002-0	R5.	N/A
BAL-002-0	R6.	N/A
BAL-003-0	R1.	N/A
BAL-003-0	R2.	N/A
BAL-003-0	R3.	N/A
BAL-003-0	R4.	N/A
BAL-003-0	R5.	N/A

Confidential Information (including Privileged and
Critical Energy Infrastructure Information) – Has Been Removed

Reliability Standard	Requirement	Finding
BAL-003-0	R6.	N/A
BAL-004-0	R1.	N/A
BAL-004-0	R2.	N/A
BAL-004-0	R3.	N/A
BAL-004-0	R4.	N/A
BAL-005-0	R1.	N/A
BAL-005-0	R2.	N/A
BAL-005-0	R3.	N/A
BAL-005-0	R4.	N/A
BAL-005-0	R5.	N/A
BAL-005-0	R6.	N/A
BAL-005-0	R7.	N/A
BAL-005-0	R8.	N/A
BAL-005-0	R9.	N/A
BAL-005-0	R10.	N/A
BAL-005-0	R11.	N/A
BAL-005-0	R12.	N/A
BAL-005-0	R13.	N/A
BAL-005-0	R14.	N/A
BAL-005-0	R15.	N/A
BAL-005-0	R16.	N/A
BAL-005-0	R17.	N/A
BAL-006-1	R1.	N/A
BAL-006-1	R2.	N/A
BAL-006-1	R3.	N/A
BAL-006-1	R4.	N/A
BAL-006-1	R5.	N/A
CIP-001-1	R1.	N/A
CIP-001-1	R2.	N/A
CIP-001-1	R3.	N/A
CIP-001-1	R4.	N/A
CIP-002-1 through CIP-009-1		N/A
COM-001-1	R1.	N/A
COM-001-1	R2.	N/A
COM-001-1	R3.	N/A
COM-001-1	R4.	N/A
COM-001-1	R5.	N/A
COM-001-1	R6.	N/A
COM-002-2	R1.	N/A
COM-002-2	R2.	N/A
EOP-001-0	R1.	N/A
EOP-001-0	R2.	N/A

Confidential Information (including Privileged and
Critical Energy Infrastructure Information) – Has Been Removed

Reliability Standard	Requirement	Finding
EOP-001-0	R3.	N/A
EOP-001-0	R4.	N/A
EOP-001-0	R5.	N/A
EOP-001-0	R6.	N/A
EOP-001-0	R7.	N/A
EOP-002-2	R1.	N/A
EOP-002-2	R2.	N/A
EOP-002-2	R3.	N/A
EOP-002-2	R4.	N/A
EOP-002-2	R5.	N/A
EOP-002-2	R6.	N/A
EOP-002-2	R7.	N/A
EOP-002-2	R8.	N/A
EOP-002-2	R9.	N/A
EOP-003-1	R1.	N/A
EOP-003-1	R2.	N/A
EOP-003-1	R3.	N/A
EOP-003-1	R4.	N/A
EOP-003-1	R5.	N/A
EOP-003-1	R6.	N/A
EOP-003-1	R7.	N/A
EOP-003-1	R8.	N/A
EOP-004-1	R1.	N/A
EOP-004-1	R2.	N/A
EOP-004-1	R3.	N/A
EOP-004-1	R4.	N/A
EOP-004-1	R5.	N/A
EOP-005-1	R1.	N/A
EOP-005-1	R2.	N/A
EOP-005-1	R3.	N/A
EOP-005-1	R4.	N/A
EOP-005-1	R5.	N/A
EOP-005-1	R6.	N/A
EOP-005-1	R7.	N/A
EOP-005-1	R8.	N/A
EOP-005-1	R9.	N/A
EOP-005-1	R10.	N/A
EOP-005-1	R11.	N/A
EOP-006-1	R1.	N/A
EOP-006-1	R2.	N/A
EOP-006-1	R3.	N/A
EOP-006-1	R4.	N/A

Confidential Information (including Privileged and
Critical Energy Infrastructure Information) – Has Been Removed

Reliability Standard	Requirement	Finding
EOP-006-1	R5.	N/A
EOP-006-1	R6.	N/A
EOP-008-0	R1.	N/A
EOP-009-0	R1.	N/A
EOP-009-0	R2.	N/A
FAC-003-1	R1.	Compliant
FAC-003-1	R2.	Compliant
FAC-003-1	R3.	Compliant
FAC-003-1	R4.	N/A
FAC-008-1	R1.	Compliant
FAC-008-1	R2.	Compliant
FAC-008-1	R3.	Compliant
FAC-009-1	R1.	Compliant
FAC-009-1	R2.	Compliant
FAC-013-1	R1.	Compliant
FAC-013-1	R2.	Compliant
INT-001-2	R1.	N/A
INT-001-2	R2.	N/A
INT-003-2	R1.	N/A
INT-004-1	R1.	N/A
INT-004-1	R2.	N/A
IRO-001-1	R1.	N/A
IRO-001-1	R2.	N/A
IRO-001-1	R3.	N/A
IRO-001-1	R4.	N/A
IRO-001-1	R5.	N/A
IRO-001-1	R6.	N/A
IRO-001-1	R7.	N/A
IRO-001-1	R8.	Compliant
IRO-001-1	R9.	N/A
IRO-003-2	R1.	N/A
IRO-003-2	R2.	N/A
IRO-004-1	R1.	N/A
IRO-004-1	R2.	N/A
IRO-004-1	R3.	Compliant
IRO-004-1	R4.	Compliant
IRO-004-1	R5.	N/A
IRO-004-1	R6.	N/A
IRO-004-1	R7.	Compliant
IRO-005-1	R1.	N/A
IRO-005-1	R2.	N/A
IRO-005-1	R3.	N/A

Confidential Information (including Privileged and
Critical Energy Infrastructure Information) – Has Been Removed

Reliability Standard	Requirement	Finding
IRO-005-1	R4.	N/A
IRO-005-1	R5.	N/A
IRO-005-1	R6.	N/A
IRO-005-1	R7.	N/A
IRO-005-1	R8.	N/A
IRO-005-1	R9.	N/A
IRO-005-1	R10.	N/A
IRO-005-1	R11.	N/A
IRO-005-1	R12.	N/A
IRO-005-1	R13.	Compliant
IRO-005-1	R14.	Compliant
IRO-005-1	R15.	N/A
IRO-005-1	R16.	N/A
IRO-005-1	R17.	N/A
IRO-006-3	R1.	N/A
IRO-006-3	R2.	N/A
IRO-006-3	R3.	N/A
IRO-006-3	R4.	N/A
IRO-006-3	R5.	N/A
IRO-006-3	R6.	N/A
IRO-014-1	R1.	N/A
IRO-014-1	R2.	N/A
IRO-014-1	R3.	N/A
IRO-014-1	R4.	N/A
IRO-015-1	R1.	N/A
IRO-015-1	R2.	N/A
IRO-015-1	R3.	N/A
IRO-016-1	R1.	N/A
IRO-016-1	R2.	N/A
PER-002-0	R1.	N/A
PER-002-0	R2.	N/A
PER-002-0	R3.	N/A
PER-002-0	R4.	N/A
PER-003-0	R1.	N/A
PER-004-1	R1.	N/A
PER-004-1	R2.	N/A
PER-004-1	R3.	N/A
PER-004-1	R4.	N/A
PER-004-1	R5.	N/A
PRC-004-1	R1.	Compliant
PRC-004-1	R2.	N/A
PRC-004-1	R3.	Compliant

Confidential Information (including Privileged and
Critical Energy Infrastructure Information) – Has Been Removed

Reliability Standard	Requirement	Finding
PRC-005-1	R1.	Compliant
PRC-005-1	R2.	Compliant
PRC-008-0	R1.	Compliant
PRC-008-0	R2.	Compliant
PRC-010-0	R1.	Compliant
PRC-010-0	R2.	Compliant
PRC-011-0	R1.	Compliant
PRC-011-0	R2.	Compliant
PRC-016-0	R1.	Compliant
PRC-016-0	R2.	Compliant
PRC-016-0	R3.	Compliant
PRC-017-0	R1.	Compliant
PRC-017-0	R2.	Compliant
PRC-021-1	R1.	Compliant
PRC-021-1	R2.	Compliant
TOP-002-2	R1.	N/A
TOP-002-2	R2.	N/A
TOP-002-2	R3.	Compliant
TOP-002-2	R4.	N/A
TOP-002-2	R5.	N/A
TOP-002-2	R6.	N/A
TOP-002-2	R7.	N/A
TOP-002-2	R8.	N/A
TOP-002-2	R9.	N/A
TOP-002-2	R10.	N/A
TOP-002-2	R11.	N/A
TOP-002-2	R12.	Compliant
TOP-002-2	R13.	N/A
TOP-002-2	R14.	N/A
TOP-002-2	R15.	N/A
TOP-002-2	R16.	N/A
TOP-002-2	R17.	N/A
TOP-002-2	R18.	Compliant
TOP-002-2	R19.	N/A
TOP-003-0	R1.	N/A
TOP-003-0	R2.	N/A
TOP-003-0	R3.	N/A
TOP-003-0	R4.	N/A
TOP-004-1	R1.	N/A
TOP-004-1	R2.	N/A
TOP-004-1	R3.	N/A
TOP-004-1	R4.	N/A

Confidential Information (including Privileged and
Critical Energy Infrastructure Information) – Has Been Removed

Reliability Standard	Requirement	Finding
TOP-004-1	R5.	N/A
TOP-004-1	R6.	N/A
TOP-005-1	R1.	N/A
TOP-005-1	R2.	N/A
TOP-005-1	R3.	N/A
TOP-005-1	R4.	N/A
TOP-007-0	R1.	N/A
TOP-007-0	R2.	N/A
TOP-007-0	R3.	N/A
TOP-007-0	R4.	N/A
TPL-001-0	R1.	Compliant
TPL-001-0	R2.	Compliant
TPL-001-0	R3.	Compliant
TPL-002-0	R1.	Compliant
TPL-002-0	R2.	Compliant
TPL-002-0	R3.	Compliant
TPL-003-0	R1.	Compliant
TPL-003-0	R2.	Compliant
TPL-003-0	R3.	Compliant
TPL-004-0	R1.	Compliant
TPL-004-0	R2.	Compliant
VAR-001-1	R1.	N/A
VAR-001-1	R2.	N/A
VAR-001-1	R3.	N/A
VAR-001-1	R4.	N/A
VAR-001-1	R5.	N/A
VAR-001-1	R6.	N/A
VAR-001-1	R7.	N/A
VAR-001-1	R8.	N/A
VAR-001-1	R9.	N/A
VAR-001-1	R10.	N/A
VAR-001-1	R11.	N/A
VAR-001-1	R12.	N/A
VAR-002-1	R1.	N/A
VAR-002-1	R2.	N/A
VAR-002-1	R3.	N/A
VAR-002-1	R4.	N/A
VAR-002-1	R5.	N/A

Compliance Culture

Information regarding the compliance culture of GTC was obtained from other sources and has been documented.