



Compliance Audit Report Public Version

**Duke Energy Generation Services, Inc.
NCR09007
September 28-30, 2009**

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

January 7, 2010

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> | 5 |
| <i>Company Profile</i> | 6 |
| <i>Audit Specifics</i> | 6 |
| Audit Results | 6 |
| <i>Findings</i> | 8 |
| <i>Compliance Culture</i> | 17 |

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.

Duke Energy Generation Services, Inc. (DEGS) was audited on September 28-30, 2009 for compliance with the requirements contained in the currently mandatory and enforceable reliability standards in the 2009 NERC Compliance Monitoring and Enforcement Program (CMEP) that are applicable to DEGS's registered functions. DEGS is registered with SERC Reliability Corporation (SERC) as a Generator Operator (GOP). Nine standards were selected and identified to DEGS as subject to review during this audit. The audit focused on documents and other evidence provided to SERC by the staff of DEGS, 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. DEGS's staff provided an update on their progress with implementation of Cyber Security Standards CIP-002-1 through CIP-009-1.

DEGS 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 DEGS as subject to this audit. DEGS staff responded by providing evidence in the form of reports, procedures, studies, and other documents. DEGS 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 DEGS was judged to be compliant. Likewise, if any of the requirements or sub-requirements were not fully met, then DEGS was judged to have a possible violation of the standard. A score of 100% is required for compliance.

The audit team found DEGS 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 DEGS's compliance with the requirements of the reliability standards that are applicable to DEGS based on the DEGS registered functions.
- Validate compliance with applicable reliability standards from the NERC 2009 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 DEGS's compliance culture.

Scope

The scope of the audit of DEGS included all monitored standards that are in the NERC 2009 CMEP. Based on the confirmed registration of DEGS, the nine reliability standards previously identified were the focus of the compliance audit.

Note: For the 2009 compliance program, the monitoring period for the compliance audit will generally be the lesser of: 1) Date of registration to current date; 2) Date of last audit or spot check to current date; or, 3) June 18, 2007 to current date. 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 regional entity staff were provided to DEGS in advance of the audit. Work history and conflict of interest forms submitted by each audit team member were provided to DEGS upon request. DEGS 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. DEGS accepted the audit team member participants with no objections.

On-site Audit

DEGS was contacted by letter on April 3, 2009 by SERC staff. The letter provided DEGS with their initial notification of their upcoming audit in 2009, 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 DEGS both verify their currently registered functions and complete and return an attached Pre-Audit Survey within 30 days.

On June 26, 2009, SERC staff forwarded an Audit Detail Letter to DEGS, again confirming the scheduled audit dates and confirming DEGS's registered functions within SERC. The Audit Detail Letter also provided DEGS with notice of the Standards in Audit Scope, Proposed Audit Schedule, Audit Team Roster (with industry affiliations), and requested that DEGS Subject Matter Experts responsible for and knowledgeable of compliance submittals be available for interview during the audit. In addition to the Audit Detail Letter, DEGS was provided with a Non-Disclosure Agreement Signature Verification for audit team members, a list of Documentation and Evidence Requirements, and Questionnaire and Reliability Standard Auditor Worksheets (QRSAs) 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 was identified and conducted the audit of DEGS. The standards were grouped and scheduled for review to make the most efficient use of DEGS staff's time. The Audit Team Leader (ATL) initiated dialogue on each standard requirement and requested compliance evidence. This evidence and DEGS's staff response were documented. DEGS staff was requested to show valid evidence of meeting each applicable requirement and sub-requirement contained in the nine standards that had been previously identified by SERC to

DEGS as subject to this audit. DEGS staff responded by providing evidence in the form of reports, procedures, studies, and other documents. DEGS staff would then cite specific portions of the evidence that demonstrated compliance.

This evidence and the citations were documented by the audit team scribe on the QRSAs, and were 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 DEGS staff until it was determined whether each requirement was met by the cited evidence or other evidence offered.

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

Audit Overview

This audit was executed simultaneously with personnel from both DEGS and KGen Power. The audit team arrived at the KGen Power offices at 3:10 PM, September 28, 2009. At 3:28 PM, the Audit Team Lead (ATL) began the session with an opening presentation. He reviewed the NERC compliance plan for 2009 in general, and how it applied to DEGS specifically. The ATL introduced and reviewed the standards to be covered in the audit, and addressed both the expectations of DEGS 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.

DEGS staff made a brief presentation describing DEGS's corporate structure and compliance program. The staff of DEGS was introduced, and general housekeeping matters explained. The staff of DEGS was excused and the audit team reviewed team assignments and a general overview for preparation of the audit activities. The audit team left the KGen Power offices at 5:12 PM September 28, 2009 to return the next day to start the review of the reliability standards in the audit scope.

Audit

The audit team arrived at the KGen Power offices at 7:48 AM September 29, 2009. The audit team initially reviewed the registration status of DEGS with entity staff to verify applicability of each standard. Each standard's audit began with a recitation of each requirement. DEGS 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 DEGS staff before proceeding to the next requirement. The team scribe would record the evidence presented to satisfy the requirement, and the team's recommendation on that requirement, using the QRSAs.

The review of all applicable standards was completed at 10:40 AM September 30, 2009, 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 QRSAs.

Exit Briefing

The ATL presented an exit briefing to the assembled audit team and entity staff at 11:05 AM September 30, 2009. This was followed by an informal response and questions from the DEGS 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 DEGS staff, along with requesting that they fill out formal feedback forms for submission to NERC and SERC.

The ATL thanked DEGS staff for their cooperation and support of the audit process. DEGS staff expressed their appreciation of the professional manner in which the audit was conducted.

The audit team left the KGen Power offices at 11:21 AM on September 30, 2009.

Company Profile

Duke Energy Generation Services is a subsidiary in Duke Energy's Commercial Business division. As a single source for complete on-site energy services, DEGS currently has approximately 45 projects in their portfolio, including large energy consumers, municipalities, utilities, and industrial facilities. [NOTE: DEGS has operating responsibilities for four facilities owned by KGen Power: KGen Hinds, LLC, KGen Hot Springs, LLC, KGen Murray I & II, LLC, and KGen Sandersville, LLC. These facilities were the focus of this audit.]

Audit Specifics

The compliance audit was conducted on September 28-30, 2009 at the KGen Power offices in Houston, TX.

Audit Team

| Audit Team Role | Title | Company |
|------------------------|---------------------------|----------------|
| Lead | Senior Compliance Auditor | SERC |
| Member | Compliance Auditor | SERC |

DEGS Audit Participants Title and Organization

| Title | Organization |
|------------------------------------|---------------------|
| General Manager – Operations | DEGS |
| Project Coordinator | DEGS |
| Senior Compliance Specialist | Duke Energy |
| President and CEO | KGen Power |
| Senior Vice President – Operations | KGen Power |
| Vice President – Operations | KGen Power |
| Director – Operations | KGen Power |
| Consultant | ZB Solutions |

AUDIT RESULTS

The audit team reviewed documents provided by DEGS prior to the audit, as requested in the Documentation and Evidence Requirements section of DEGS's Compliance Audit Certification Letter. Pre-audit review of these documents, and of currently open or recently closed mitigation plans (none found), helped to establish the audit team's focus during the audit.

The audit team reviewed the evidence provided by DEGS to substantiate compliance with each standard requirement. The team requested clarification and/or additional supporting and

corroborating evidence, as required, to obtain sufficient and appropriate evidence to support a determination of compliance.

In instances where the evidence provided by DEGS represented multiple facilities and/or large quantities of equipment, the audit team haphazardly selected evidence samples, from the different facilities and/or equipment, to facilitate a consensus agreement of the team whether DEGS is, in the team's professional judgment, satisfactorily meeting the requirements of the standard or is in possible violation of the requirement.

If the audit team determined that the evidence provided by DEGS was insufficient or inappropriate to substantiate a determination of compliance, the team immediately informed DEGS' Subject Matter Expert of this fact. Additionally, the Audit Team Lead, through coordination with DEGS' audit coordinator, ensured that DEGS' management was made aware of the potential for a finding of a possible violation in each instance, and of the basis for the team's determination.

The Audit Team Lead clearly identified the team's findings of compliance, the basis for their findings, areas of concern, and available remedies, in an exit presentation to DEGS's management upon completion of the audit.

The audit team documented their review and determination of compliance of each standard requirement on Questionnaire/Reliability Standard Auditor Worksheets. DEGS's policies, procedures, screenshots, operator logs, audio clips, correspondence and other evidence presented, as well as auditor comments and determinations of compliance documented on the QRSAs were used in formulating this report.

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

Prior to being forwarded to SERC's Manager of Compliance Audits, or his designee, for review and approval as SERC's Final Confidential Non-Public Audit Report of DEGS, the content and accuracy of this report:

- Is reviewed and commented on by all audit team members
- Is reviewed by DEGS's management for correction and comment, and
- Is reviewed and approved by the Audit Team Lead.

Upon final disposition of any possible violations determined by the audit team, if any, and redaction of appropriate information contained herein, this report will be reviewed and approved by SERC's Manager, Compliance Programs before being issued as SERC's Final Public Audit Report of DEGS.

Findings

| Reliability Standard | Requirement | Finding |
|-----------------------------|--------------------|----------------|
| BAL-001-0a | R1. | N/A |
| BAL-001-0a | R2. | N/A |
| BAL-001-0a | R3. | N/A |
| BAL-001-0a | 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-003-0a | R1. | N/A |
| BAL-003-0a | R2. | N/A |
| BAL-003-0a | R3. | N/A |
| BAL-003-0a | R4. | N/A |
| BAL-003-0a | R5. | N/A |
| BAL-003-0a | 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-005-0b | R1. | N/A |
| BAL-005-0b | R2. | N/A |
| BAL-005-0b | R3. | N/A |
| BAL-005-0b | R4. | N/A |
| BAL-005-0b | R5. | N/A |
| BAL-005-0b | R6. | N/A |
| BAL-005-0b | R7. | N/A |
| BAL-005-0b | R8. | N/A |
| BAL-005-0b | R9. | N/A |
| BAL-005-0b | R10. | N/A |
| BAL-005-0b | R11. | N/A |
| BAL-005-0b | R12. | N/A |
| BAL-005-0b | R13. | N/A |
| BAL-005-0b | R14. | N/A |
| BAL-005-0b | R15. | N/A |
| BAL-005-0b | R16. | N/A |
| BAL-005-0b | 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 |

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

| Reliability Standard | Requirement | Finding |
|--------------------------------|--------------------|----------------|
| BAL-006-1 | R5. | N/A |
| CIP-001-1 | R1. | Compliant |
| CIP-001-1 | R2. | Compliant |
| CIP-001-1 | R3. | Compliant |
| CIP-001-1 | R4. | Compliant |
| 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. | Compliant |
| COM-002-2 | R2. | N/A |
| EOP-001-0 | R1. | N/A |
| EOP-001-0 | R2. | N/A |
| 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 |

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

| Reliability Standard | Requirement | Finding |
|-----------------------------|--------------------|----------------|
| 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 |
| 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-001-0 | R1. | N/A |
| FAC-001-0 | R2. | N/A |
| FAC-001-0 | R3. | N/A |
| FAC-002-0 | R1. | N/A |
| FAC-002-0 | R2. | N/A |
| FAC-003-1 | R1. | N/A |
| FAC-003-1 | R2. | N/A |
| FAC-003-1 | R3. | N/A |
| FAC-003-1 | R4. | N/A |
| FAC-008-1 | R1. | N/A |
| FAC-008-1 | R2. | N/A |
| FAC-008-1 | R3. | N/A |
| FAC-009-1 | R1. | N/A |
| FAC-009-1 | R2. | N/A |
| FAC-010-1 | R1. | N/A |
| FAC-010-1 | R2. | N/A |
| FAC-010-1 | R3. | N/A |
| FAC-010-1 | R4. | N/A |
| FAC-010-1 | R5. | N/A |
| FAC-011-1 | R1. | N/A |
| FAC-011-1 | R2. | N/A |

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

| Reliability Standard | Requirement | Finding |
|-----------------------------|--------------------|----------------|
| FAC-011-1 | R3. | N/A |
| FAC-011-1 | R4. | N/A |
| FAC-011-1 | R5. | N/A |
| FAC-013-1 | R1. | N/A |
| FAC-013-1 | R2. | N/A |
| FAC-014-1 | R1. | N/A |
| FAC-014-1 | R2. | N/A |
| FAC-014-1 | R3. | N/A |
| FAC-014-1 | R4. | N/A |
| FAC-014-1 | R5. | N/A |
| FAC-014-1 | R6. | N/A |
| INT-001-3 | R1. | N/A |
| INT-001-3 | R2. | N/A |
| INT-003-2 | R1. | N/A |
| INT-004-2 | R1. | N/A |
| INT-004-2 | R2. | N/A |
| INT-005-2 | R1. | N/A |
| INT-006-2 | R1. | N/A |
| INT-007-1 | R1. | N/A |
| INT-008-2 | R1. | N/A |
| INT-009-1 | R1. | N/A |
| INT-010-1 | R1. | N/A |
| INT-010-1 | R2. | N/A |
| INT-010-1 | R3. | 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-002-1 | R1. | N/A |
| IRO-002-1 | R2. | N/A |
| IRO-002-1 | R3. | N/A |
| IRO-002-1 | R4. | N/A |
| IRO-002-1 | R5. | N/A |
| IRO-002-1 | R6. | N/A |
| IRO-002-1 | R7. | N/A |
| IRO-002-1 | R8. | N/A |
| IRO-002-1 | R9. | N/A |

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

| Reliability Standard | Requirement | Finding |
|-----------------------------|--------------------|----------------|
| 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. | N/A |
| IRO-004-1 | R4. | Compliant |
| IRO-004-1 | R5. | N/A |
| IRO-004-1 | R6. | N/A |
| IRO-004-1 | R7. | N/A |
| IRO-005-1 | R1. | N/A |
| IRO-005-1 | R2. | N/A |
| IRO-005-1 | R3. | N/A |
| 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. | N/A |
| 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 |
| MOD-006-0 | R1. | N/A |

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

| Reliability Standard | Requirement | Finding |
|-----------------------------|--------------------|----------------|
| MOD-006-0 | R2. | N/A |
| MOD-007-0 | R1. | N/A |
| MOD-007-0 | R2. | N/A |
| MOD-010-0 | R1. | N/A |
| MOD-010-0 | R2. | N/A |
| MOD-012-0 | R1. | N/A |
| MOD-012-0 | R2. | N/A |
| MOD-016-1 | R1. | N/A |
| MOD-016-1 | R2. | N/A |
| MOD-016-1 | R3. | N/A |
| MOD-017-0 | R1. | N/A |
| MOD-018-0 | R1. | N/A |
| MOD-018-0 | R2. | N/A |
| MOD-019-0 | R1. | N/A |
| MOD-020-0 | R1. | N/A |
| MOD-021-0 | R1. | N/A |
| MOD-021-0 | R2. | N/A |
| MOD-021-0 | R3. | N/A |
| NUC-001-1 | R1. | N/A |
| NUC-001-1 | R2. | N/A |
| NUC-001-1 | R3. | N/A |
| NUC-001-1 | R4. | N/A |
| NUC-001-1 | R5. | N/A |
| NUC-001-1 | R6. | N/A |
| NUC-001-1 | R7. | N/A |
| NUC-001-1 | R8. | N/A |
| NUC-001-1 | R9. | N/A |
| PER-001-0 | R1. | 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-001-1 | R1. | Compliant |
| PRC-001-1 | R2. | Compliant |
| PRC-001-1 | R3. | Compliant |
| PRC-001-1 | R4. | N/A |

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

| Reliability Standard | Requirement | Finding |
|-----------------------------|--------------------|----------------|
| PRC-001-1 | R5. | Compliant |
| PRC-001-1 | R6. | N/A |
| PRC-004-1 | R1. | N/A |
| PRC-004-1 | R2. | N/A |
| PRC-004-1 | R3. | N/A |
| PRC-005-1 | R1. | N/A |
| PRC-005-1 | R2. | N/A |
| PRC-007-0 | R1. | N/A |
| PRC-007-0 | R2. | N/A |
| PRC-007-0 | R3. | N/A |
| PRC-008-0 | R1. | N/A |
| PRC-008-0 | R2. | N/A |
| PRC-009-0 | R1. | N/A |
| PRC-009-0 | R2. | N/A |
| PRC-010-0 | R1. | N/A |
| PRC-010-0 | R2. | N/A |
| PRC-011-0 | R1. | N/A |
| PRC-011-0 | R2. | N/A |
| PRC-015-0 | R1. | N/A |
| PRC-015-0 | R2. | N/A |
| PRC-015-0 | R3. | N/A |
| PRC-016-0 | R1. | N/A |
| PRC-016-0 | R2. | N/A |
| PRC-016-0 | R3. | N/A |
| PRC-017-0 | R1. | N/A |
| PRC-017-0 | R2. | N/A |
| PRC-018-1 | R1. | N/A |
| PRC-018-1 | R2. | N/A |
| PRC-018-1 | R3. | N/A |
| PRC-018-1 | R4. | N/A |
| PRC-018-1 | R5. | N/A |
| PRC-018-1 | R6. | N/A |
| PRC-021-1 | R1. | N/A |
| PRC-021-1 | R2. | N/A |
| PRC-022-1 | R1. | N/A |
| PRC-022-1 | R2. | N/A |
| TOP-001-1 | R1. | N/A |
| TOP-001-1 | R2. | N/A |
| TOP-001-1 | R3. | Compliant |
| TOP-001-1 | R4. | N/A |
| TOP-001-1 | R5. | N/A |
| TOP-001-1 | R6. | Compliant |

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

| Reliability Standard | Requirement | Finding |
|-----------------------------|--------------------|----------------|
| TOP-001-1 | R7. | Compliant |
| TOP-001-1 | R8. | N/A |
| 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. | N/A |
| TOP-002-2 | R13. | Compliant |
| TOP-002-2 | R14. | Compliant |
| TOP-002-2 | R15. | Compliant |
| 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. | Compliant |
| TOP-003-0 | R2. | Compliant |
| TOP-003-0 | R3. | Compliant |
| 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 |
| 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-006-1 | R1. | N/A |
| TOP-006-1 | R2. | N/A |
| TOP-006-1 | R3. | N/A |
| TOP-006-1 | R4. | N/A |
| TOP-006-1 | R5. | N/A |
| TOP-006-1 | R6. | N/A |
| TOP-006-1 | R7. | N/A |

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

| Reliability Standard | Requirement | Finding |
|-----------------------------|--------------------|----------------|
| TOP-007-0 | R1. | N/A |
| TOP-007-0 | R2. | N/A |
| TOP-007-0 | R3. | N/A |
| TOP-007-0 | R4. | N/A |
| TOP-008-1 | R1. | N/A |
| TOP-008-1 | R2. | N/A |
| TOP-008-1 | R3. | N/A |
| TOP-008-1 | R4. | N/A |
| TPL-001-0 | R1. | N/A |
| TPL-001-0 | R2. | N/A |
| TPL-001-0 | R3. | N/A |
| TPL-002-0 | R1. | N/A |
| TPL-002-0 | R2. | N/A |
| TPL-002-0 | R3. | N/A |
| TPL-003-0 | R1. | N/A |
| TPL-003-0 | R2. | N/A |
| TPL-003-0 | R3. | N/A |
| TPL-004-0 | R1. | N/A |
| TPL-004-0 | R2. | N/A |
| 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

The audit team assessed DEGS's Internal Compliance Program in conjunction with the audit. Evidence reviewed in assessing the program included: DEGS's Compliance Pre-Audit Survey, compliance staff organizational charts, interviews with DEGS staff, and observation of staff responses in preparation for and during the audit.

Four factors that characterize a vigorous and effective compliance program are: active engagement and leadership by a company's senior management; preventive measures appropriate to the individual circumstances of the company; promptly detecting, stopping, and reporting a violation; and, ultimately fixing the problem and working to avoid future possible violations.

SERC recognizes that there isn't one standard formula for an effective compliance program, and that there will be variations in each company's program and culture based on countless factors, including the size and age of the company, as well as the nature and extent of its business. Ultimately what matters are the results, and whether the compliance program worked as it should.

The audit team determined that DEGS' Internal Compliance Program documents and their staff's demonstrated compliance culture indicate an effective compliance program.