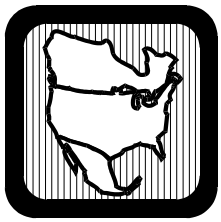

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

# Guidelines for Compliance Information in Support of Reliability Standards White Paper

**October 19, 2005**

A New Jersey Nonprofit Corporation

Phone 609-452-8060 ■ Fax 609-452-9550 ■ URL www.nerc.com

## *Introduction*

This document is intended to guide standard drafting teams in the development of compliance elements within standards and the process for incorporating compliance expertise in the development of the compliance elements of a standard. The goal is to provide the necessary compliance information within reliability standards to meet the needs of the principal users of the standards: reliability stakeholders and compliance enforcement programs. Only a subset of compliance information is provided within the standards; additional compliance process information will be provided through the compliance program.

This procedure is addressing several issues in existing standards:

- The levels of non-compliance within standards indicate a degree to which a standard was not complied with, e.g. a 'percentage' or index of non-compliance. However, these levels of non-compliance alone do not indicate the severity of impacts caused by non-compliance. Thus a Level 3 violation in one standard would not necessarily be comparable to a Level 3 violation in another standard with regard to reliability impacts.
- It has been difficult to provide a uniform, straightforward set of guidelines on setting the levels of non-compliance and drafting teams have used various methods. For example, if a requirement has multiple elements, some drafting teams have used a method in which one missing element is a Level 1 violation, two is a Level 2 violation, etc. Others have distinguished levels by whether information was submitted late.
- It is important to complement the technical expertise on drafting teams with compliance expertise for developing the compliance elements within a standard.

These guidelines are intended to address these issues and improve the quality and consistency of compliance elements within standards, by both instructing drafting teams and by providing procedural safeguards to ensure compliance expertise if provided in the development of standards.

The guidelines introduce a philosophical shift in the compliance elements within a standard. The shift is to ask the drafting team to use a standardized index to indicate the potential severity of violating a requirement within the standard. This moves away from the concept of a level or 'percentage' of non-compliance. This approach allows the drafting team to rank the reliability importance of each requirement. At the same time, it leaves the evaluation of how much the requirement was actually violated (level of non-compliance) to be evaluated based on the actual facts and circumstances found in the compliance investigation. To distiguish between the levels of non-compliance and the indices of potential reliability risk, these new indices are called "Risk Factors." The guidelines also establish a framework for identifying the type and time horizon of each requirement.

## *Approval*

This document will be approved by the Compliance and Certification Committee and the Standards Authorization Committee and will be used as a committee procedure once adopted. Because the guidelines are consistent with the existing Reliability Standards Process Manual, no revision of the manual is anticipated as a result of implementing these guidelines.

## Guidelines for Requirements and Measures within a Standard

The Reliability Standards Process Manual defines *requirements* and *measures* in standards. The following guidelines clarify those definitions:

**Requirements** are explicitly stated technical, performance, and preparedness criteria. Each requirement identifies who is responsible and what action is to be performed, or what outcome is to be achieved for a reliable bulk electric system. Each statement in the requirements section shall be a statement for which compliance is mandatory. Any additional comments or statements, such as background or explanatory information, should be placed in a separate reference document. In short, a requirement defines the minimum acceptable performance or results and provides a clear basis for determining whether an entity meets that threshold or not. A properly constructed requirement does not depend on measures or other compliance information for determining whether acceptable performance or outcomes have been achieved. The measures and other compliance information define how compliance is to be regularly monitored through the compliance enforcement program.

**Measures** — Each requirement is addressed by one or more measures. A measure states what a responsible entity must do to demonstrate compliance to a third party, i.e. the Compliance Monitor. Measures are proxies, or "yardsticks" used to evaluate whether required performance or outcomes have been achieved. Measures do not add new requirements or expand the details of the requirements. Each measure shall be tangible, practical, and objective. A measure should be written so that achieving full compliance with the measure provides the Compliance Monitor with the necessary and sufficient indicators to demonstrate that the associated requirement was met by the responsible entity.

Each measure should clearly refer to the requirement(s) to which it applies and each requirement should clearly indicate which measure(s) apply to that requirement.

## Types of Requirements

In the development of standards, drafting teams should identify a *type* for each requirement. The drafting team should propose the *type* in its proposed draft of the standard and request comment from stakeholders during comment periods regarding the appropriateness of the designation recommended by the drafting team. The drafting team should strive to reach stakeholder consensus on the *type* of each requirement.

The drafting team should identify the *type* of each requirement as one of the following (choosing a best fit realizing the characterization may not be a perfect fit): a) technical, b) performance, or c) preparedness. Organization certification requirements, a fourth *type*, would be used in organization certification standards:

- **Technical requirements** relate to the provision, maintenance, operation, or state of the bulk electric system, and the facilities and tools necessary to reliably operate the bulk electric system; will likely contain measures of physical parameters; and will often be technical in nature (requirements placed on things).
- **Performance requirements** relate to the actions of entities providing for or impacting the reliability of the bulk electric system and will likely contain measures of the results of such actions, or the nature of the performance of such actions (requirements placed on what people or entities do).
- **Preparedness requirements** relate to the actions of entities to be prepared for future events or conditions that are critical to reliability of the bulk electric system. The outcomes of meeting

these requirements include plans, preparations, training, etc. to establish a state of preparedness for events that are expected to occur infrequently.

- **Organization certification requirements** define the essential capabilities needed to perform a reliability function and are used to credential organizations that have the requisite capabilities.

## *Potential Reliability Significance of a Requirement*

In addition to identifying the type of requirement, the drafting team should rate the *potential reliability significance* of each requirement as a Risk Factor 1, 2, or 3, in accordance with the criteria listed below:

A **Risk Factor 1** requirement is administrative in nature. Violation of a Risk Factor 1 requirement would not be expected to affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system.

A **Risk Factor 2** requirement could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a Risk Factor 2 requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.

A **Risk Factor 3** requirement is one that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures.

Because preparedness requirements, such as providing a valid restoration plan, are essential for reliability but may be used infrequently, performance may not be directly observable through compliance monitoring. The following modifications are therefore added to each Risk Factor for preparedness requirements:

A **Risk Factor 1** *preparedness* requirement is administrative in nature. Violation of a Risk Factor 1 requirement would not, *under the emergency, abnorma,l or restorative conditions anticipated by the preparations*, be expected to affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system.

A **Risk Factor 2** *preparedness* requirement could, *under emergency, abnormal or restorative conditions anticipated by the preparations,* directly affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a Risk Factor 2 requirement is unlikely, *under emergency, abnormal, or restoration conditions anticipated by the preparations,* to lead to bulk electric system instability, separation, or cascading failures, *nor to hinder restoration to a normal condition*.

A **Risk Factor 3** *preparedness* requirement is one that, if violated, could, *under emergency, abnormal, or restorative conditions anticipated by the preparations,* directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, *or could hinder restoration to a normal condition*.

Ranking the *potential reliability significance* does not apply to organization certification requirements. The presumption is that all organization certification requirements must be met to merit credentialling for the function. Failing to meet to certification requirements would result in not being certified or possibly de-certification of an entity.

The drafting team should make a best fit selection using the Risk Factors shown above. It is recognized that some selections will be difficult and the drafting team should use its best judgment in each case. The drafting team's recommendation should be vetted with stakeholders throught the public comment process.

The drafting team is also expected to apply good judgment regarding the practicality of the bulk electric system conditions at the time of a violation. One could argue that if the system is outside design criteria, a violation of even the simplest requirement could lead to a cascading failure. When choosing a *potential reliability significance* index, the drafting team should assume worst conditions that are still within regular planning and operating criteria. It is preferable to assume worst case conditions than to allow poor behavior that has no ill effects because system conditions were not stressed. On the other hand, the drafting team should avoid assuming unrealistic conditions that are outside planning criteria and normal or emergency operating criteria. The fact that the system is outside these criteria may itself constitute a violation of one or more requirements, but should not be used as a base assumption for determining the potential severity of violating other requirements. The drafting team should document any specific assumptions made in assigning a *potential reliability significance* index.

If the drafting team is unable to fit a single best *potential reliability significance* to a requirement, it may indicate more than one, but only if the base assumptions distinguishing the different risk rankings are provided within the standard.

## *Temporal Characterization of Requirements*

The drafting team should also identify the time horizon(s) for which each requirement applies. The drafting team should select one or more time horizons for each requirement based on the definitions provided below:

- **Real-time operations** — actions required within one hour or less to preserve the reliability of the bulk electric system.
- **Same-day operations** — routine actions required within the time frame of a day, but not real-time.
- **Operations planning** — operating and resource plans from day-ahead up to and including seasonal.
- **Long-term planning** — a planning horizon of one year or longer.

## *Additional Compliance Information in a Standard*

The following table describes the compliance monitoring process information to be provided in a standard.

| Section Heading | Description |
|---|---|
| **C. Compliance Monitoring Process** | |
| **1. Compliance Monitoring Responsibility** | States which entity(ies) are responsible for monitoring compliance with the standard, typically the Regional Reliability Organization or NERC. |
| **2. Compliance Monitoring** | Compliance Monitoring Period defines a period of time over which compliance will be measured, such as annually, quarterly, monthly, |

| Section Heading | Description |
|---|---|
| **Period** | etc. |
| **3. Reset Period** | The Reset Period defines a duration of time after which a verified violation is reset to zero for the purpose of counting the number of violations by an entity. After the reset period ends, another instance of not meeting the requirement would be counted as a new violation. |
| **4. Data Retention** | Defines a period of time that an entity is required to keep compliance-related information for future review or audit. |
| **5. Additional Compliance Information** | Defines any additional compliance process requirements not addressed above. |

## *Compliance Expertise in the Development of Compliance Elements of a Standard*

The Standards Authorization Committee (SAC) will solicit and seek to appoint at least one compliance expert to each standard drafting team. Given resource limitations, that may not always be possible, but it is a goal.

The standard drafting team, whether or not it has a compliance expert on the team should prepare the compliance elements within a standard and forward the draft standard to the Compliance and Certification Managers Committee (CCMC) for inputs on the compliance elements, prior to the initial posting of the draft standard for stakeholder comment. The standard drafting team should utilize the CCMC inputs in preparing its initial draft for posting.

During the posting of the draft standard for comment, the CCMC should review the compliance information and provide comments through the regular comment process.

Prior to requesting authorization to ballot a standard, the drafting team should request a final verification by the CCMC that the compliance elements within the standard can be implemented as written in the final draft. The SAC should consider this verification and any additional comments of the drafting team when authorizing the standard to go to ballot.

## *Additional Compliance Factors to Be Developed by Compliance Enforcement Program*

With the approach described above of identifying the relative risk index for each requirement in the standards, there are other factors that the Compliance Enforcement Program may consider in fully understanding the severity of violations and appropriate penalites and sanctions. The details of these parameters should be established by the Compliance Enforcement Program:

- The level or percent of non-compliance — by how much did an entity miss the requirement? Did the entity completely miss the entire requirement, or was the entity mostly compliant and missed some minor details? Conceptually, the level of non-compliance could be viewed as a percentage of compliance (i.e. 0% to 100%). However, non-compliance can also be graded in several

categories, such as the index previously used in the standards (i.e. levels of non-compliance 1 to 4).

- Whether there were multiple violations concurrently.
- The duration of the violation(s).
- Whether the violations are repeating from prior violations that should have been previously corrected.
- Whether the entity self-reported the violations and took timely actions to correct the problem.
- Actual events and circumstances that occurred as context around the violation that could serve to either accentuate or mitigate the significance of the violation. For example, if an entity was operating in violation of a requirement and was informed by another party of the violation, but continued to violate the requirement deliberately. Conversely there could be mitigating reasons for the performance that would have caused the violation to be difficult to avoid.
- Evaluation of actual events and conditions, including whether the bulk electric system was at risk for instability, separation, or uncontrolled cascading failures.

The Compliance Enforcement Program should, through due process, develop rules and guidelines for these considerations for use in compliance enforcement actions under the electric reliability organization.

# Sample Standard Showing Compliance Elements

## A. Introduction

**R1. Title: Notifications and Information Exchange Between Reliability Coordinators**

**R2. Number**: IRO-015-1

**R3. Purpose**: 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.

**R4. Applicability**

**R4.1.** Reliability Coordinators

**R5. Proposed Effective Date:** November 1, 2006

## B. Requirements

**R1.** The Reliability Coordinator shall follow its Operating Procedures, Processes or Plans for making notifications and exchanging reliability-related information with other Reliability Coordinators.

Type: Performance
Horizon: Same-day Operations
Risk Factor: 2
Assumptions: None

**R1.1.** The Reliability Coordinator shall make notifications to other Reliability Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas.

**R2.** The Reliability Coordinator shall participate in agreed upon conference calls and other communication forums with adjacent Reliability Coordinators.

Type: Performance
Horizon: Operations Planning
Risk Factor: 2
Assumptions: None

**R2.1.** The frequency of these conference calls shall be agreed upon by all involved Reliability Coordinators and shall be at least weekly.

**R3.** The Reliability Coordinator shall provide reliability related information as requested by other Reliability Coordinators.

Type: Performance
Horizon: Same-day Operations
Risk Factor: 2
Assumptions: None

## C. Measures

**R1.** The Reliability Coordinator shall have evidence (such as operator logs or other data sources) it has followed its Operating Procedures, Processes or Plans for notifying other Reliability Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas.

**R2.** The Reliability Coordinator shall have evidence (such as operator logs or other data sources) that it participated in agreed upon (at least weekly) conference calls and other communication forums with adjacent Reliability Coordinators.

**R3.** The Reliability Coordinator shall have evidence that it provided requested reliability related information to other Reliability Coordinators.

## D. Compliance

**1. Compliance Monitoring Process**

**1.1 Compliance Monitoring Responsibility**

Regional Reliability Organization

### 1.2 Compliance Monitoring Period and Reset Timeframe

The Performance-Reset Period shall be one calendar year.

### 1.3 Data Retention

The Reliability Coordinator shall keep auditable documentation for a rolling 12 months. The Compliance Monitor shall keep compliance data for a minimum of three years or until the Reliability Coordinator has achieved full compliance — whichever is longer.

### 1.4 Additional Compliance Information

The Reliability Coordinator shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor shall also use a scheduled on-site review at least once every three years and investigations upon complaint. The Compliance Monitor shall conduct an investigation upon a complaint within 30 days of the alleged infraction's discovery date. The Compliance Monitor shall complete the investigation within 45 days after the start of the investigation. As part of an audit or an investigation, the Compliance Monitor shall interview other Reliability Coordinators within the Interconnection and verify that the Reliability Coordinator being audited or investigated has been making notifications and exchanging reliability related information according to agreed Operating Procedures, Processes or Plans.

The Reliability Coordinator shall have the following available for its Compliance Monitor to inspect during a scheduled, on-site review or within five days of a request as part of an investigation upon complaint:

**1.4.1.** Evidence it has participated in agreed-upon conference calls or other communications forums.

**1.4.2.** Operating logs or other data sources that document notifications made to other Reliability Coordinators.

## E. Regional Differences

None Identified.