

These definitions will be posted and balloted along with the standard, but will not be restated in the standard. Instead, once approved, they will be included in a separate “Definitions” glossary on the NERC website containing definitions relevant to all standards that NERC develops.

DEFINITIONS

Operating Plan: A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan.

Operating Procedure: A document that identifies specific steps or tasks that should be taken by one or more specific operating positions to achieve specific operating goal(s). The steps in an Operating Procedure should be followed in the order in which they are presented, and should be performed by the position(s) identified. A document that lists the specific steps to take in removing a specific transmission line from service is an example of an Operating Procedure.

Operating Process: A document that identifies general steps for achieving a generic operating goal. An Operating Process includes steps with options that may be selected depending upon real-time conditions. A guideline for controlling high voltage is an example of an Operating Process.

Scenario: Possible event.

**100 - COORDINATE RELIABILITY AUTHORITY TO RELIABILITY
AUTHORITY OPERATIONS**

- 101 Procedures
- 102 Notifications and Information Exchange
- 103 Coordination

Purpose: To ensure that each Reliability Authority’s operations are coordinated such that they will not have an adverse impact on the reliability of other Reliability Authority and to preserve the reliability benefits of interconnected operations.

Effective Date: To be determined.

Applicability: This standard applies to entities performing the Reliability Authority function, as identified in NERC’s Functional Model. NERC is now developing standards and procedures for the identification and certification of such entities. Until that identification and certification is complete, these standards apply to the existing entities (such as control areas and reliability coordinators) that are currently performing the defined functions.

In this standard, the term “Reliability Authority” refers to the entities performing this function as defined in the Functional Model.

101 Procedures

(a) Requirements

- (1) The Reliability Authority shall have Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or coordination of actions with one or more other Reliability Authorities to support interconnection reliability. These Operating Procedures, Processes or Plans shall address Scenarios that affect other Reliability Authority Areas as well as those developed in coordination with other Reliability Authorities.
 - (i) These shall collectively address, as a minimum, the following:
 - A) Communications and notifications, including the conditions (sabotage attacks, IROL violations, voltage reductions, insufficient resources, etc.) under which one Reliability Authority notifies other Reliability Authorities; the process to follow in making those notifications; and the data and information to be exchanged with other Reliability Authorities.
 - B) Energy and capacity shortages.
 - C) Planned or unplanned outage information.
 - D) Voltage control, including the coordination of reactive resources for voltage control.
 - E) Coordination of information exchange to support reliability assessments.
 - F) Authority to act to prevent and mitigate instances of causing adverse impacts to other Reliability Authority Areas.
 - (ii) Each Reliability Authority's Operating Procedure, Process or Plan that requires one or more other Reliability Authorities to take action (e.g. make notifications, exchange information, or coordinate actions) shall be:
 - A) Agreed to by all the Reliability Authorities required to take the indicated action(s).
 - B) Distributed to all Reliability Authorities that are required to take the indicated action(s).
- (2) A Reliability Authority's Operating Procedures, Processes or Plans developed to support a Reliability Authority to Reliability Authority Operating Procedure, Process or Plan shall include:
 - (i) A reference to the associated Reliability Authority to Reliability Authority Operating Procedure, Process or Plan.
 - (ii) The agreed-upon actions from the associated Reliability Authority to Reliability Authority Operating Procedure, Process or Plan.
- (3) Each of the Operating Procedures, Processes or Plans addressed in requirement 101(a)(1) and each of the internal Operating Procedures, Processes or Plans developed under 101(a)(2) shall:
 - (i) Include version control number or date.
 - (ii) Include a distribution list.

- (iii) Be reviewed, at least once every three years, and updated if needed.

(b) Measures

- (1) The Reliability Authority's system operators shall have available for Real-time use, the latest approved version of Operating Procedures, Processes, or Plans that require notifications, information exchange or the coordination of actions between Reliability Authorities.
 - (i) These Operating Procedures, Processes, or Plans shall address:
 - A) Communications and notifications, including the conditions under which one Reliability Authority notifies other Reliability Authorities; the process to follow in making those notifications; and the data and information to be exchanged with other Reliability Authorities.
 - B) Energy and capacity shortages.
 - C) Planned or unplanned outage information.
 - D) Voltage control, including the coordination of reactive resources for voltage control.
 - E) Coordination of information exchange to support reliability assessments.
 - F) Authority to act to prevent and mitigate instances of causing adverse impacts to other Reliability Authority Areas.
 - (ii) The Reliability Authority shall have evidence that these Operating Procedures, Processes or Plans were:
 - A) Agreed to by all the Reliability Authorities required to take the indicated action(s).
 - B) Distributed to all Reliability Authorities that are required to take the indicated action(s).
- (2) The Reliability Authority's Operating Procedures, Processes or Plans developed (for its system operators' internal use) to support a Reliability Authority to Reliability Authority Operating Procedure, Process or Plan received from another Reliability Authority shall:
 - (i) Be available to the Reliability Authority's system operators for real-time use,
 - (ii) Include a reference to the associated source document, and
 - (iii) Support the agreed-upon actions from the source document.
- (3) The Reliability Authority's Operating Procedures, Processes or Plans that addresses Reliability Authority to Reliability Authority coordination shall each include a version control number or approval date and a distribution list. The Reliability Authority shall have evidence that these Operating Procedures, Processes or Plans were reviewed within the last three years.

(c) Regional Differences

None

(d) Compliance Monitoring

- (1) The Reliability Authority shall demonstrate compliance through the following techniques:
 - (i) The Reliability Authority shall complete an annual self-certification and shall submit this to its Compliance Monitor annually. The self-certification shall include a list of the latest approved version of documents distributed to other Reliability Authorities that include notifications, information exchange or the coordination of actions between Reliability Authorities or that addresses Scenarios in the Reliability Authority Area that may impact other Reliability Authority Areas. The Compliance Monitor shall interview other Reliability Authorities to identify Operating Procedures, Processes or Plans that were distributed to the Reliability Authority being audited to verify that these documents are available for real-time use by the receiving Reliability Authority's system operators.
 - ii) 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.
- (2) The performance-reset period shall be one calendar year. The Reliability Authority shall keep documentation for prior year and current calendar year. The Compliance Monitor shall keep compliance data for a minimum of 3 years or until the Reliability Authority has achieved full compliance, whichever is longer.
- (3) The Reliability Authority shall have the following documents available for inspection during an on-site audit or within five days of a request as part of an investigation upon a complaint:
 - (i) The latest version of its Operating Procedures, Processes or Plans that require notification, exchange of information or coordination of actions with one or more other Reliability Authorities to support Interconnection reliability

(e) Levels of Non-compliance

- (1) Level One: There shall be a level one noncompliance if either of the following conditions is present:
 - (i) The latest versions of Operating Procedures, Processes or Plans (identified through self-certification) that require notification, exchange of information or coordination of actions with one or more other Reliability Authorities to support interconnection reliability do not include version control number or date, and a distribution list, or
 - (ii) The latest versions of Reliability Authority internal documents developed to support action(s) required as a result of other Reliability Authorities, do not include both a reference to the source Operating Procedure, Process or Plan and the agreed-upon actions from the source Operating Procedure, Process or Plan.
- (2) Level Two: No evidence of distribution.
- (3) Level Three: Not applicable.
- (4) Level Four: There shall be a level four non-compliance if either of the following conditions is present:

Standard 100 — Coordinate Operations

- (i) The latest versions of Operating Procedures, Processes or Plans (identified through self-certification) that require notification, exchange of information or coordination of actions with one or more other Reliability Authorities to support interconnection reliability were not available for system operators real-time use.
- (ii) The latest versions of Operating Procedures, Processes or Plans (identified through self-certification) that require notification, exchange of information or coordination of actions with one or more other Reliability Authorities to support interconnection reliability do not address all required topics.

(f) Sanctions

- (1) Apply sanctions consistent with the NERC Compliance and Enforcement Matrix. In places where financial sanctions are applied for non-compliance, these penalties shall be the fixed dollar sanctions listed in the matrix, not the dollars per megawatt sanctions.

102 Notifications and Information Exchange

(a) Requirement

- (1) The Reliability Authority shall follow its Operating Procedures, Processes or Plans for making notifications and exchanging reliability-related information with other Reliability Authorities.
 - (i) The Reliability Authority shall make notifications to other Reliability Authorities of conditions in its Reliability Authority Area that may impact other Reliability Authority Areas.
- (2) The Reliability Authority shall participate in agreed upon conference calls and other communication forums with adjacent Reliability Authorities.
 - (i) The frequency of these conference calls shall be agreed upon by all involved Reliability Authorities and shall be at least weekly.
- (3) The Reliability Authority shall provide reliability related information as requested by other Reliability Authorities.

(b) Measures

- (1) The Reliability Authority shall have evidence (such as operator logs or other data sources) it has followed its Operating Procedures, Processes or Plans for notifying other Reliability Authorities of conditions in its Reliability Authority Area that may impact other Reliability Authority Areas.
- (2) The Reliability Authority 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 Authorities.
- (3) When requested by its Compliance Monitor, each Reliability Authority shall provide evidence (such as operator logs or other data sources) identifying other Reliability Authorities that have:
 - (i) Notified them of conditions in their area that may impact the questioned Reliability Authority Area.
- (4) When requested, the Reliability Authority shall provide the Compliance Monitor with evidence that the requested reliability related information was provided to other Reliability Authorities.

(c) Regional Differences

None

(d) Compliance Monitoring

- (1) The Reliability Authority 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. The Compliance Monitor shall interview other Reliability Authorities within the Interconnection and verify that the Reliability Authority being audited has been

making notifications and exchanging reliability related information according to approved procedures.

- (2) The compliance-reset period shall be one calendar year. The Reliability Authority 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 Authority has achieved full compliance — whichever is longer.
- (3) The Reliability Authority 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:
 - (i) Evidence it has participated in agreed-upon conference calls or other communications forums.
 - (ii) Operating logs or other data sources that document notifications made to other Reliability Authorities.

(e) Levels of Noncompliance

- (1) Level one: Did not participate in agreed upon (at least weekly) conference calls and other communication forums with adjacent Reliability Authorities.
- (2) Level two: Not applicable.
- (3) Level three: Did not provide requested reliability related information to other Reliability Authorities.
- (4) Level four: Did not follow its Operating Procedures, Processes or Plans for notifying other Reliability Authorities of conditions in its Reliability Authority Area that may impact other Reliability Authority Areas.

(f). Sanctions

- (1) Apply sanctions consistent with the NERC Compliance and Enforcement Matrix. In places where financial sanctions are applied for non-compliance, these penalties shall be the fixed dollar sanctions listed in the matrix, not the dollars per megawatt sanctions.

103 Coordination

(a) Requirements

- (1) The Reliability Authority that identifies a potential, expected, or actual problem that requires the actions of one or more other RAs shall contact the other Reliability Authority(s) to confirm that there is a problem and then discuss options and decide upon a solution to prevent or resolve the identified problem.
 - (i) If the involved Reliability Authorities agree on the problem and the actions to take to prevent or mitigate the system condition each involved Reliability Authority shall implement the agreed-upon solution, and notify the involved Reliability Authorities of the action being taken.
 - (ii) If the involved Reliability Authorities cannot agree on the problem each Reliability Authority shall re-evaluate the causes of the disagreement (bad data, status, study results, tools, etc.)
 - A) If time permits, this re-evaluation shall be done before taking corrective actions.
 - B) If time does not permit, then each RA shall operate as though the problem exists until the conflicting system status is resolved.
 - (iii) If the involved Reliability Authorities cannot agree on the solution the more conservative solution shall be implemented.
- (2) The RA shall have evidence (operator logs or other data sources) of the actions taken for either the event or for the disagreement on the problem or for both.

(b) Measures

- (1) For each event that requires Reliability Authority to Reliability Authority coordination, each involved Reliability Authority shall have evidence (operator logs or other data sources) of the actions taken for either the event or for the disagreement on the problem or for both.

(c) Regional Differences

None

(d) Compliance Monitoring Process

- (1) The Reliability Authority shall demonstrate compliance through self-certification submitted to its Compliance Monitor annually. The Compliance Monitor shall use a scheduled on-site review at least once every three years. The Compliance Monitor shall interview other Reliability Authorities within the Interconnection and verify that the Reliability Authority being audited has been coordinating actions to prevent or resolve potential, expected or actual problems that adversely impact the Interconnection. The Compliance Monitor shall conduct an investigation upon a complaint that is received within 30 days of an alleged infraction's discovery date. The Compliance Monitor shall complete the investigation and report back to all involved Reliability Authorities (the Reliability Authority that complained as well as the Reliability Authority that was investigated) within 45 days after the start of the investigation. Entities found non-compliant shall be subject to re-audit every 90 days until found fully compliant.

- (2) The compliance-reset period shall be one calendar year. The Reliability Authority shall keep auditable evidence for the prior year and current calendar year. In addition, entities found non-compliant shall keep information related to the non-compliance until it has been found compliant. The Compliance Monitor shall keep compliance data for a minimum of three years or until the Reliability Authority has achieved full compliance, whichever is longer.
- (3) The Reliability Authority shall have the following available for its Compliance Monitor to inspect during a scheduled, on-site review or within five working days of a request as part of an investigation upon complaint:
 - (i) Evidence (operator log or other data source) to show coordination with other Reliability Authorities.

(e) Levels of Non-compliance

- (1) Level one: For potential, actual or expected events which required Reliability Authority to Reliability Authority coordination, the Reliability Authority did not have evidence that it coordinated with other Reliability Authorities.
- (2) Level two: Not Applicable.
- (3) Level three: Not Applicable.
- (4) Level four: For potential, actual or expected events which required Reliability Authority to Reliability Authority coordination, the Reliability Authority did not coordinate with other Reliability Authorities.

(f) Sanctions

- (1) Apply sanctions consistent with the NERC Compliance and Enforcement Matrix. In places where financial sanctions are applied for non-compliance, these penalties shall be the fixed dollar sanctions listed in the matrix, not the dollars per megawatt sanctions.

Sanctions Matrix

The following matrix of compliance sanctions was developed by the NERC Compliance Subcommittee as part of the NERC Compliance Enforcement Program and has been approved by the NERC Board of Trustees.

Levels of noncompliance are described in this matrix. The matrix is divided into four levels of increasing noncompliance vertically and the number of violations in a defined period at a given level horizontally.

Note that there are three sanctions that can be used: a letter, a fixed fine, and a \$/MW fine.

Letter

This sanction is used to notify company executives, regional officers, and regulators that an entity is noncompliant. The distribution of the letter varies depending on the severity of the noncompliance. The intent of a letter sanction is to bring noncompliance to the attention of those who can influence the actions of an organization to become compliant.

- Letter (A) — Letter to the entity's vice president level or equivalent informing the entity of noncompliance, with copies to the data reporting contact, and the entity's highest ranking Regional Council representative.
- Letter (B) — Letter to the entity's chief executive officer or equivalent, with copies to the data reporting contact, the entity's highest ranking Regional Council representative, and the vice president over the area in which noncompliance occurred.
- Letter (C) — Letter to the entity's chief executive officer and chairman of the board, with copies to the NERC president, regulatory authorities having jurisdiction over the noncompliant entity (if requested by such regulatory authorities), the data reporting contact, the entity's highest ranking Regional Council representative, and the vice president over the area in which noncompliance occurred.

Fixed Dollars

This sanction is to be used when a letter sanction is not sufficient and a stronger message is desired to encourage compliance. Fixed dollars are typically assigned as a one-time fine that is ideal for measures involving planning-related standards. Many planning actions use forward-looking assumptions; if such assumptions prove wrong in the future, yet are made in good faith using good practices, entities should not be harshly penalized for the outcome.

Dollar per MW

Dollar/MW sanctions are intended to be used primarily for operationally based standards. The "MW" can be load, generation, or flow on a line. The reasonableness of the sanction must be considered when assessing \$/MW penalties. NERC's goal is for the industry to achieve compliance, as opposed to collecting large financial penalties.

Standard 100 — Coordinate Operations

Occurrence Period Category	Number of Violations in Occurrence Period at a Given Level			
	1 st Period of Violations (Fully Compliant Last Period)	1	2	3
2 nd Consecutive Period of Violations		1	2	3 or more
		\$ Sanction from Table; Letter (C) only if Letter (B) previously sent		
3 rd Consecutive Period of Violations			1	2 or more
		\$ Sanction from Table; Letter (C) only if Letter (B) previously sent		
4 th or greater Consecutive Period of Violations				1
		\$ Sanction from Table; Letter (C)		

Level of Non-Compliance	Sanctions Associated with Noncompliance			
	Level 1	Letter (A)	Letter (A)	Letter (B) and \$1,000 or \$1 Per MW
Level 2	Letter (A)	Letter (B) and \$1,000 or \$1 Per MW	Letter (B) and \$2,000 or \$2 Per MW	Letter (B) and \$4,000 or \$4 Per MW
Level 3	Letter (B) and \$1,000 or \$1 Per MW	Letter (B) and \$2,000 or \$2 Per MW	Letter (B) and \$4,000 or \$4 Per MW	Letter (B) and \$6,000 or \$6 Per MW
Level 4	Letter (B) and \$2,000 or \$2 Per MW	Letter (B) and \$4,000 or \$4 Per MW	Letter (B) and \$6,000 or \$6 Per MW	Letter (B) and \$10,000 or \$10 Per MW

Interpreting the Tables:

- These tables address penalties for violations of the same measure occurring in consecutive compliance reporting periods.
- If a participant has noncompliant performance in consecutive compliance reporting periods, the sanctions applied are more punitive.