

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The standard authorization request (SAR) was posted for industry comment in May 2005.
2. A standard drafting team was selected in September 2005.
3. The standard drafting team received comments on the SAR.
4. The proposed standard documents were posted for comment in January 2005.
5. Draft 1 of the standard posted for a 30-day comment period from February 17–March 18, 2006.

Description of Current Draft:

This is a first draft of the proposed revisions to show stakeholders the proposed approach to completing the missing measures and compliance elements. Comments received on this draft will be used to guide the drafting team in modifying the other 21 Version 0 Standards that are missing either measures or compliance elements. .

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Post response to stakeholder comments, implementation plan and 22 draft Standards for comment.	May 15–June 28, 2006
2. Post revised standards, and revised implementation plan for comment.	August 1–September 15, 2006
3. Post response to stakeholder comments and final draft of standard and implementation plan for 30-day pre-ballot review.	October 1–30, 2006
4. Conduct first ballot.	November 1–10, 2006
5. Post response to comments submitted with first ballot.	November 17, 2006
6. Conduct second ballot.	November 20–30, 2006
7. Post for 30-day board review.	November 1–30, 2006
8. BOT adoption.	December, 2006
9. Proposed effective date.	One month after BOT adoption.

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

No new terms introduced in this standard.

A. Introduction

1. **Title:** **Telecommunications**
2. **Number:** COM-001-~~0~~1
3. **Purpose:** Each Reliability Coordinator, Transmission Operator and Balancing Authority needs adequate and reliable telecommunications facilities internally and with others for the exchange of Interconnection and operating information necessary to maintain reliability.
4. **Applicability**
 - 4.1. Transmission Operators.
 - 4.2. Balancing Authorities.
 - 4.3. Reliability Coordinators.
 - 4.4. NERCNet User Organizations.
5. **Proposed Effective Date:** ~~April 1, 2005~~One month after BOT adoption.

B. Requirements

- R1. Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide adequate and reliable telecommunications facilities the exchange of Interconnection and operating information:
 - R1.1. Internally.
 - R1.2. Between the Reliability Coordinator and its Transmission Operators and Balancing Authorities.
 - R1.3. With other Reliability Coordinators, Transmission Operators, and Balancing Authorities as necessary to maintain reliability.
 - R1.4. Where applicable, these facilities shall be redundant and diversely routed.
- R2. Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall manage, alarm, test and/or actively monitor vital telecommunications facilities. Special attention shall be given to emergency telecommunications facilities and equipment not used for routine communications.
- R3. Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide a means to coordinate telecommunications among their respective areas. This coordination shall include the ability to investigate and recommend solutions to telecommunications problems within the area and with other areas.
- R4. Unless agreed to otherwise, each Reliability Coordinator, Transmission Operator, and Balancing Authority shall use English as the language for all communications between and among operating personnel responsible for the real-time generation control and operation of the interconnected Bulk Electric System. Transmission Operators and Balancing Authorities may use an alternate language for internal operations.
- R5. Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall have written operating instructions and procedures to enable continued operation of the system during the loss of telecommunications facilities.
- R6. Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-~~0~~, “NERCNet Security Policy.”

C. Measures

M1.

Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide evidence that could include, but is not limited to communication-facilities lists or other equivalent evidence to confirm that they meet Requirement 1.

M2.

Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide evidence that could include, but is not limited to communication facility test-procedure documents, records of testing, and maintenance records for communication facilities or other equivalent evidence to confirm that they meet Requirement 2.

M3.

Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide evidence that could include, but is not limited to operator logs, trouble shooting procedures, maintenance records, or other equivalent evidence, to confirm that they meet Requirement 3.

M4.

Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide evidence that could include, but is not limited to operator logs, voice recordings, electronic communications, or other equivalent evidence to confirm that they meet Requirement 4.

M5.

Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide the current written operating instructions and procedures that will be used to confirm that they meet Requirement 5.

M6.

Each NERCnet User Organization shall provide evidence that could include, but is not limited to documented procedures, operator logs, transcripts of voice recordings, electronic communications, etc., to confirm that they adhere to the requirements¹ in Attachment 1-COM-001, as specified in Requirement 6.

~~C.~~Not Specified.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organizations for all entities except the Regional Reliability Organization

NERC for the Regional Reliability Organization

1.2. Compliance Monitoring and Reset Time Frame

The Compliance Monitor may require an annual self-certification or may conduct an annual spot check audit. The Compliance Monitor shall conduct a periodic audit of R1, R2, R3 and R5, at least once every three years.

For a triggered investigation, the Compliance Monitor shall notify the entity being investigated as soon as possible, but no later than 60 days after the event. (R4 and R6). The entity being investigated shall have 30 calendar days from the day of notice, to prepare documentation.

The Performance-Reset Period shall be twelve months from the last finding of non-compliance.

1.3. Data Retention

¹ The requirements referred to in R6 are the same as the responsibilities identified in Attachment 1-COM-001.

If the measure does not define a specific retention requirement for evidence, a Reliability Coordinator, Transmission Operator, Balancing Authority and NERCnet User Organization shall keep evidence of compliance for four rolling years.

Entities shall retain evidence used as proof of compliance from the previous self-certification audit, triggered investigation or spot audit for at least four years. If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for four years, whichever is longer.

The Compliance Monitor shall keep the last periodic audit report and all subsequent compliance records.

1.4. Additional Compliance Information

See Attachment 1-COM-001 — NERCnet Security Policy

2. Levels of Non-Compliance for Transmission Operator, Balancing Authority and Reliability Coordinator

2.1. Level 1 — Used a language other than English without agreement as specified in R4.

2.2. Level 2 — There shall be a separate level-2 non-compliance for every one of the following requirements that is in violation:

2.2.1 Does not have adequate communication facilities internally, or with one or more external entities as specified in R1.

2.2.2 Did not coordinate, investigate, and recommend solutions to telecommunication problems as specified in R3.

2.3. Level 3 — Not applicable.

2.4. Level 4 — There shall be a separate Level 4 non-compliance, for every one of the following requirements that is in violation:

2.4.1 Telecommunication systems are not actively monitored, tested, managed or alarmed as specified in R2.

2.4.2 There are no written operating instructions and procedures to enable continued operation of the system during the loss of telecommunication facilities as specified in R5.

3. Levels of Non-Compliance for NERCnet User Organization

3.1. Level 1 — Not applicable.

3.2. Level 2 — No documentation showing Attachment 1 — COM-001 has been incorporated into telecommunication practices.

3.3. Level 3 — One or two violations of Attachment 1 — COM-001 in the past year.

3.4. Level 4 — Three or more violations of Attachment 1 — COM-001 in the past year.

Not specified.

E. Regional Differences

None Identified.

Version History

Version	Date	Action	Change Tracking
---------	------	--------	-----------------

Standard COM-001-~~0~~1— Telecommunications

0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata

Attachment 1-COM-001-0 — NERCnet Security Policy

Policy Statement

The purpose of this NERCnet Security Policy is to establish responsibilities and minimum requirements for the protection of information assets, computer systems and facilities of NERC and other users of the NERC frame relay network known as “NERCnet.” The goal of this policy is to prevent misuse and loss of assets.

For the purpose of this document, information assets shall be defined as processed or unprocessed data using the NERCnet Telecommunications Facilities including network documentation. This policy shall also apply as appropriate to employees and agents of other corporations or organizations that may be directly or indirectly granted access to information associated with NERCnet.

The objectives of the NERCnet Security Policy are:

- To ensure that NERCnet information assets are adequately protected on a cost-effective basis and to a level that allows NERC to fulfill its mission.
- To establish connectivity guidelines for a minimum level of security for the network.
- To provide a mandate to all Users of NERCnet to properly handle and protect the information that they have access to in order for NERC to be able to properly conduct its business and provide services to its customers.

NERC’s Security Mission Statement

NERC recognizes its dependency on data, information, and the computer systems used to facilitate effective operation of its business and fulfillment of its mission. NERC also recognizes the value of the information maintained and provided to its members and others authorized to have access to NERCnet. It is, therefore, essential that this data, information, and computer systems, and the manual and technical infrastructure that supports it, are secure from destruction, corruption, unauthorized access, and accidental or deliberate breach of confidentiality.

Implementation and Responsibilities

This section identifies the various roles and responsibilities related to the protection of NERCnet resources.

NERCnet User Organizations

Users of NERCnet who have received authorization from NERC to access the NERC network are considered users of NERCnet resources. To be granted access, users shall complete a User Application Form and submit this form to the NERC Telecommunications Manager.

Responsibilities

It is the responsibility of NERCnet User Organizations to:

- Use NERCnet facilities for NERC-authorized business purposes only.
- Comply with the NERCnet security policies, standards, and guidelines, as well as any procedures specified by the data owner.
- Prevent unauthorized disclosure of the data.
- Report security exposures, misuse, or non-compliance situations via Reliability Coordinator Information System or the NERC Telecommunications Manager.

- Protect the confidentiality of all user IDs and passwords.
- Maintain the data they own.
- Maintain documentation identifying the users who are granted access to NERCnet data or applications.
- Authorize users within their organizations to access NERCnet data and applications.
- Advise staff on NERCnet Security Policy.
- Ensure that all NERCnet users understand their obligation to protect these assets.
- Conduct self-assessments for compliance.

User Accountability and Compliance

All users of NERCnet shall be familiar and ensure compliance with the policies in this document.

Violations of the NERCnet Security Policy shall include, but not be limited to any act that:

- Exposes NERC or any user of NERCnet to actual or potential monetary loss through the compromise of data security or damage.
 - Involves the disclosure of trade secrets, intellectual property, confidential information or the unauthorized use of data.
- R7.** Involves the use of data for illicit purposes, which may include violation of any law, regulation or reporting requirement of any law enforcement or government body.