

## Standard Authorization Request Form

|  |               |
|--|---------------|
| Title Revisions to Critical Infrastructure Protection Standards (revisions to CIP-002 through CIP-009) |               |
| Request Date   | March 1, 2008 |
| Revision Date  | June 9, 2008  |
| Approved by Standards Committee for standard development on July 10, 2008                              |               |

| SAR Requester Information |                     | SAR Type <i>(Check a box for each one that applies.)</i> |                                 |
|---------------------------|---------------------|--|---------------------------------|
| Name                      | Dave Norton         | <input type="checkbox"/>                                 | New Standard                    |
| Company                   | Entergy             | <input checked="" type="checkbox"/>                      | Revision to existing Standards  |
| Telephone                 | (504) 576-5469      | <input type="checkbox"/>                                 | Withdrawal of existing Standard |
| Fax                       |                     |  |                                 |
| E-mail                    | dnorto1@entergy.com | <input type="checkbox"/>                                 | Urgent Action                   |

## Standards Authorization Request Form

---

**Purpose** (Describe what the standard action will achieve in support of bulk power system reliability.)

To protect the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operations of the bulk power system.

**Industry Need** (Provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

Implement Changes to the following Cyber Security Standards as indicated in FERC Order 706:

|           |  |
|-----------|--|
| CIP-002-1 | Critical Cyber Asset Identification        |
| CIP-003-1 | Security Management Controls               |
| CIP-004-1 | Personnel & Training                       |
| CIP-005-1 | Electronic Security Perimeter(s)           |
| CIP-006-1 | Physical Security of Critical Cyber Assets |
| CIP-007-1 | Systems Security Management                |
| CIP-008-1 | Incident Reporting and Response Planning   |
| CIP-009-1 | Recovery Plans for Critical Cyber Assets   |

**Brief Description** (Provide a paragraph that describes the scope of this standard action.)

This set of revisions in this project includes:

- Modifying the standards so they conform to the latest approved versions of the ERO Rules of Procedure as outlined in the Standard Review Guidelines identified in Attachment 1.
- Addressing the directives issued by FERC, in Order 706 relative to the approved Cyber Security Standards CIP-002-1 through CIP-009-1. Refer to <http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf> for the complete text of the final order. Specific requirements from the Order are identified in Attachment 2.
  - Emphasis on Order 706 directive for NERC to address revisions to the CIP standards considering applicable feature of the NIST Security Risk Management Framework among other resources.
- Incorporating clarifications from the Interpretation of CIP-006-1 Requirement 1.1.

Additional issues identified by stakeholders during the posting of this SAR are listed in Attachment 3.

**Detailed Description** (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR.)

This project requires reviewing each of the standards to ensure that it conforms to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure as outlined in the Standard Review Guidelines (Attachment 1).

This proposed standards drafting project includes addressing all of the directed modifications identified in the FERC Final Order 706. These directives are summarized in Attachment 2.

Revisions will incorporate the clarifications from the Interpretation of CIP-006-1 Requirement 1.1.

Revisions should consider other Cyber-related standards, guidelines and activities:

- Consider adopting the NIST Security Risk Management Framework (includes GAO, OMB and FIPS)
- Consider other cyber security related documents such as NIST, ISO 27000 Family, CIPC WG Risk Assessment Guideline, MITRE corporation technical report, DHS, National Laboratories papers, DOE 417, IEC, ISA, etc.
- Stay apprised of coordination work between FERC, NEI and NRC in regard to the nuclear facility exemption issue with respect to regulatory gaps. As necessary modify the standards to reflect current determinations.

Revisions should consider the additional issues identified by stakeholders in Attachment 3.

**Standards Authorization Request Form**

**Reliability Functions**

| <b>The Standard will Apply to the Following Functions</b> <i>(Check box for each one that applies.)</i> |                               |   |
|---|-------------------------------|---|
| <input checked="" type="checkbox"/>   | Regional Entity               | Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions. |
| <input checked="" type="checkbox"/>   | Reliability Coordinator       | Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.  |
| <input checked="" type="checkbox"/>   | Balancing Authority           | Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.                                       |
| <input checked="" type="checkbox"/>   | Interchange Authority         | Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.                   |
| <input type="checkbox"/>  | Planning Coordinator          | Assesses the longer-term reliability of its Planning Coordinator Area.  |
| <input type="checkbox"/>  | Resource Planner              | Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.   |
| <input type="checkbox"/>  | Transmission Planner          | Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.   |
| <input checked="" type="checkbox"/>   | Transmission Service Provider | Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).   |
| <input checked="" type="checkbox"/>   | Transmission Owner            | Owns and maintains transmission facilities.   |
| <input checked="" type="checkbox"/>   | Transmission Operator         | Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.   |
| <input type="checkbox"/>  | Distribution Provider         | Delivers electrical energy to the End-use customer.   |
| <input checked="" type="checkbox"/>   | Generator Owner               | Owns and maintains generation facilities.   |
| <input checked="" type="checkbox"/>   | Generator Operator            | Operates generation unit(s) to provide real and reactive power.   |
| <input type="checkbox"/>  | Purchasing-Selling Entity     | Purchases or sells energy, capacity, and necessary reliability-related services as required.  |
| <input type="checkbox"/>  | Market Operator               | Interface point for reliability functions with commercial functions.  |
| <input checked="" type="checkbox"/>   | Load-Serving Entity           | Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.   |

**Standards Authorization Request Form**

---

***Reliability and Market Interface Principles***

|  |   |
|--|---|
| <b>Applicable Reliability Principles</b> <i>(Check box for all that apply.)</i>  |   |
| <input type="checkbox"/>   | 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.               |
| <input type="checkbox"/>   | 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.                     |
| <input type="checkbox"/>   | 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably. |
| <input checked="" type="checkbox"/>  | 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.   |
| <input checked="" type="checkbox"/>  | 5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.  |
| <input checked="" type="checkbox"/>  | 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.                  |
| <input checked="" type="checkbox"/>  | 7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.  |
| <input checked="" type="checkbox"/>  | 8. Bulk power systems shall be protected from malicious physical or cyber attacks.  |
| <b>Does the proposed Standard comply with all of the following Market Interface Principles?</b> <i>(Select 'yes' or 'no' from the drop-down box.)</i>  |   |
| 1. A reliability standard shall not give any market participant an unfair competitive advantage. Yes   |   |
| 2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes  |   |
| 3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes  |   |
| 4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes |   |

## Standards Authorization Request Form

---

### *Related Standards*

| <b>Standard No.</b> | <b>Explanation</b>   |
|---------------------|--|
| CIP-001             | Sabotage Reporting (no change proposed)                                |
| CIP-002             | Critical Cyber Asset Identification – FERC directed modifications      |
| CIP-003             | Security Management Controls – FERC directed modifications             |
| CIP-004             | Personnel and Training – FERC directed modifications                   |
| CIP-005             | Electronic Security Perimeter – FERC directed modifications            |
| CIP-006             | Physical Security – FERC directed modifications                        |
| CIP-007             | Systems Security Management – FERC directed modifications              |
| CIP-008             | Incident Reporting and Response Planning – FERC directed modifications |
| CIP-009             | Recovery Plans – FERC directed modifications                           |

### *Related SARs*

| <b>SAR ID</b> | <b>Explanation</b> |
|---------------|--------------------|
| None          |                    |
|               |                    |
|               |                    |
|               |                    |
|               |                    |
|               |                    |
|               |                    |
|               |                    |
|               |                    |

### *Regional Variances*

| <b>Region</b> | <b>Explanation</b> |
|---------------|--------------------|
| ERCOT         | None               |
| FRCC          | None               |
| MRO           | None               |
| NPCC          | None               |
| SERC          | None               |
| RFC           | None               |
| SPP           | None               |
| WECC          | None               |

## **Attachment 1 - Standard Review Guidelines**

### **Technical Basis in Engineering and Operations**

Is this reliability standard based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in that particular field?

### **Purpose**

Does this reliability standard have a clear statement of purpose that describes how the standard contributes to the reliability of the bulk power system? Each purpose statement should include a value statement.

### **Applicability**

Does this reliability standard clearly identify the functional classes of entities responsible for complying with the reliability standard, with any specific additions or exceptions noted? Where multiple functional classes are identified is there a clear line of responsibility for each requirement identifying the functional class and entity to be held accountable for compliance? Does the requirement allow overlapping responsibilities between Registered Entities possibly creating confusion for who is ultimately accountable for compliance?

Does this reliability standard identify the geographic applicability of the standard, such as the entire North American bulk power system, an interconnection, or within a regional entity area? If no geographic limitations are identified, the default is that the standard applies throughout North America.

Does this reliability standard identify any limitations on the applicability of the standard based on electric facility characteristics, such as generators with a nameplate rating of 20 MW or greater, or transmission facilities energized at 200 kV or greater or some other criteria? If no functional entity limitations are identified, the default is that the standard applies to all identified functional entities.

If the applicability is to a set of responsible entities that have criteria other than the criteria used in the compliance registration process, then the applicability section of the standard should include the reliability-related reason for the unique applicability criteria.

### **Effective Dates**

Must be 1<sup>st</sup> day of 1<sup>st</sup> quarter after entities are expected to be compliant – must include time to file with regulatory authorities and provide notice to responsible entities of the obligation to comply. If the standard is to be actively monitored, time for the Compliance Monitoring and Enforcement Program to develop reporting instructions and modify the Compliance Data Management System(s) both at NERC and Regional Entities must be provided in the implementation plan. The effective date should be linked to the applicable regulatory approvals – here is the default sentence to use for standards that should become effective as soon as possible:

First day of first calendar quarter after applicable regulatory approval (or, in those jurisdictions where regulatory approval is not required, the standard becomes effective on the first day of the first calendar quarter after BOT adoption.)

### **Performance Requirements**

Does this reliability standard state one or more performance requirements, which if achieved by the applicable entities, will provide for a reliable bulk power system, consistent with good utility practices and the public interest?

Does each requirement identify who shall do what under what conditions and to what outcome?

### **Fill-in-the-blank Requirements**

Do not include any ‘fill-in-the-blank’ requirements. These are requirements that assign one entity responsibility for developing some performance measures without requiring that the performance measures be included in the body of a standard – then require another entity to comply with those requirements.

Every reliability objective can be met, at least at a threshold level, by a North American standard. If we need regions to develop regional standards, such as in under-frequency load shedding, we can always write a uniform North American standard for the applicable functional entities as a means of encouraging development of the regional standards.

### **Requirements for Regional Reliability Organization**

Do not write any requirements for the Regional Reliability Organization. Any requirements currently assigned to the RRO should be re-assigned to the applicable functional entity. If the requirement can only be performed at a regional level, assign the requirement to the Regional Entity, not the RRO.

### **Violation Risk Factors**

Each requirement must have an associated Violation Risk Factor (VRF). Avoid assigning a VRF to sub-requirements. If a sub-requirement needs a VRF that is different from the VRF assigned to the main requirement, then consider sub-dividing the requirement into multiple requirements. The VRF identifies the reliability-related risk of violating a requirement.

#### **High Risk Requirement**

A requirement 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;

or a requirement in a planning time frame 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.

#### **Medium Risk Requirement**

A requirement that, if violated, 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 medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures;

or a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely 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 medium risk 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.

#### **Lower Risk Requirement**

A requirement that is administrative in nature and, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system.

A requirement that is administrative in nature and is a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk

## Standards Authorization Request Form

---

electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

### Time Horizon

The drafting team should also indicate the time horizon available for mitigating a violation to the requirement using the following definitions:

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

### Measurability

Is each performance requirement stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that requirement?

Does each performance requirement have one or more associated measures used to objectively evaluate compliance with the requirement? Measures should comply with the “Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards” reference document.

If performance results can be practically measured quantitatively, are metrics provided within the requirement to indicate satisfactory performance?

### Violation Severity Levels

The drafting team should indicate a set of violation severity levels that can be applied for the requirements within a standard. (‘Violation severity levels’ replace existing ‘levels of non-compliance.’) The violation severity levels must be applied for each requirement and may be combined to cover multiple requirements, as long as it is clear which requirements are included and that all requirements are included.

The violation severity levels should be based on the following definitions and the latest version of the “Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards”:

- **Lower: mostly compliant with minor exceptions** — The responsible entity is mostly compliant with and meets the intent of the requirement but is deficient with respect to one or more minor details.
- **Moderate: mostly compliant with significant exceptions** — The responsible entity is mostly compliant with and meets the intent of the requirement but is deficient with respect to one or more significant elements.
- **High: marginal performance or results** — The responsible entity has only partially achieved the reliability objective of the requirement and is missing one or more significant elements.
- **Severe: poor performance or results** — The responsible entity has failed to meet the reliability objective of the requirement.

### Compliance Enforcement Authority

Replace, ‘Regional Reliability Organization’ with ‘Regional Entity’

## Standards Authorization Request Form

---

Replace, ‘NERC’ with ‘ERO’

In situations where the Regional Entity is the responsible entity, or where a responsible entity works for the Regional Entity, the Compliance Enforcement Authority is the ERO. In all other situations, the Regional Entity is the Compliance Enforcement Authority.

### **Compliance Monitoring Period and Reset Timeframe**

In all cases, enter, ‘Not applicable.’ (These terms are associated with an older version of the sanctions table. The next time the Reliability Standards Development Procedure is updated, the procedure will be revised to omit references to ‘compliance monitoring period’ and ‘reset timeframe’.)

### **Data Retention**

Use the data retention periods proposed in the “Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards” document unless there is a justifiable reason for proposing other data retention periods.

### **Compliance Monitoring Processes**

The list of compliance monitoring processes used with each standard should comply with the proposed list of processes identified in the “Guidelines for Developing Measures and Compliance Elements in NERC Reliability Standards” reference document. In the standard, list the compliance monitoring processes under ‘Additional Compliance Information.’

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Periodic Data Submittals
- Exception Reporting
- Complaints

### **Associated Documents**

We will delay populating this section of the standard with a list of ‘related’ standards because standards are all being changed and many will have new numbers. We should limit the references to those support documents that are useful in complying with the standard.

### **Functional Model Version 3**

Review the requirements against the latest descriptions of the responsibilities and tasks assigned to functional entities as provided in pages 13 through 53 of the draft Functional Model Version 3.

### **Completeness**

Is this reliability standard complete and self-contained? Does the standard depend on external information to determine the required level of performance?

### **Clear Language**

Is the reliability standard stated using clear and unambiguous language? Can responsible entities, using reasonable judgment and in keeping with good utility practices, arrive at a consistent interpretation of the required performance?

### **Consistent Terminology**

To the extent possible, does this reliability standard use a set of standard terms and definitions that are approved through the NERC reliability standards development process?

If the standard uses terms that are included in the NERC Glossary of Terms Used in Reliability Standards, then the term must be capitalized when it is used in the standard. New terms should not be added unless

## **Standards Authorization Request Form**

---

they have a 'unique' definition when used in a NERC reliability standard. Common terms that could be found in a college dictionary should not be defined and added to the NERC Glossary.

### **Practicality**

Does this reliability standard establish requirements that can be practically implemented by the assigned responsible entities within the specified effective date and thereafter?

### **Consequences for Noncompliance**

In combination with guidelines for penalties and sanctions, as well as other ERO and regional entity compliance documents, are the consequences of violating a standard clearly known to the responsible entities?

**Attachment 2 (this is a large attachment and is in a self-contained file)**

## Attachment 3

### Stakeholder Issues and Recommendations Identified During Initial SAR Posting

#### Industry Education

- Consider what to do with the existing FAQ document e.g., modify, replace.
- Consider how to provide additional guidance in support of these standards, e.g., Technical Reference documents, guidelines, white papers.
- Consider development of a guideline document to address extended LANs over multiple geographically dispersed locations.

#### Balloting and Implementation

- Determine the timing and grouping of revisions to be submitted to industry for comment and ballot, e.g., multi-phase or other approach.
- Determine the optimum implementation plan for revised CIP standards in this project.
- Address when newly identified critical assets or critical cyber assets, newly acquired equipment or assets, etc. must come into compliance with CIP standards.
- Address compliance issue where internal requirements exceed NERC requirements. Clarify in view of language contained in FERC Order 706 paragraph 377.

#### Clarify Existing Requirements

- Consider the need for different requirements for different environments e.g., control center, substation and generation plant.
- Clarify how serial and wireless devices are subject to these standards. Refer to pp 278 and 285 of FERC Order 706.

#### Other Issues

- Consider issues surrounding protection of data in motion.
- Consider the issue of hybrid devices that use both serial and routable protocols.
- Consider the issue of data versus information (electronic and/or hardcopy lists, drawings, etc.) protection including transport and transmittal of such information.
- Consider a clearly defined set of risks which can result in a more focused and effective set of compliance expectations.
- With regard to third-party vendors and contractors, provide clarification and additional guidance as to how much a responsible entity may rely on the processes and procedures of contractors and vendors that support the critical infrastructure of that responsible entity under the CIP standards and still be compliant with the standard.