NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Standard Authorization Request Form

| | |
|---|---|
| **Title of Proposed Standard:** | Cyber Security Ninety-day Response |
| **Request Date:** | October 2, 2009 |
| **SC Approval Date:** | October 7, 2009 |

| **SAR Requester Information** | | **SAR Type** (*Check a box for each one that applies.*) | |
|---|---|---|---|
| **Name:** | NERC Staff | ☐ | New Standard |
| **Primary Contact:** | David Taylor | X | Revision to existing Standards |
| **Telephone:**<br>**Fax:** | (609)651-5089 | ☐ | Withdrawal of existing Standard |
| **E-mail:** | David.Taylor@NERC.net | ☐ | Urgent Action |

116-390 Village Boulevard
Princeton, New Jersey 08540-5721
609.452.8060 | www.nerc.com

**Purpose:**

To modify certain Critical Infrastructure Protection (CIP) Reliability Standards and associated Implementation Plan in respond to the directives issued in the Federal Energy Regulatory Commission's (FERC) September 30, 2009 Order Approving Revised Reliability Standards For Critical Infrastructure Protection And Requesting Compliance Filing.

**Industry Need:**

On May 22, 2009, NERC in its capacity as the Electric Reliability Organization (ERO) filed eight revised CIP Reliability Standards for approval with the Commission, to protect the Bulk-Power System from malicious or unintentional cyber events. They require Bulk-Power System users, owners, and operators to establish a risk-based assessment methodology to identify critical assets and the associated critical cyber assets essential to the critical assets' operation. Once the critical cyber assets are identified, the CIP Reliability Standards require, among other things, that the Responsible Entities establish plans, protocols, and controls to safeguard physical and electronic access, to train personnel on security matters, to report security incidents, and to be prepared for recovery actions. The eight Reliability Standards are as follows:

CIP-002-2 – Cyber Security – Critical Cyber Asset Identification: Requires a Responsible Entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.

CIP-003-2 – Cyber Security – Security Management Controls: Requires a Responsible Entity to develop and implement security management controls to protect critical cyber assets identified pursuant to CIP-002-1.

CIP-004-2 – Cyber Security – Personnel and Training: Requires personnel with access to critical cyber assets to have identity verification and a criminal check. It also requires employee training.

CIP-005-2 – Cyber Security – Electronic Security Perimeter(s): Requires the identification and protection of an electronic security perimeter and access points. The electronic security perimeter is to encompass the critical cyber assets identified pursuant to the methodology required by CIP-002-1.

CIP-006-2 – Cyber Security – Physical Security: Requires a Responsible Entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

CIP-007-2 – Cyber Security – Systems Security Management: Requires a Responsible Entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.

CIP-008-2 – Cyber Security – Incident Reporting and Response Planning: Requires a Responsible Entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets.

CIP-009-2 – Cyber Security – Recovery Plans for Critical Cyber Assets: Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

On September 30, 2009 the Commission approved Version 2 of the CIP Reliability Standards with an effective date of April 1, 2010. In its September 30, 2009 Order the Commission directed NERC to make additional changes to two of the Standards (CIP-006-2 and CIP-008-2) and the associated Implementation Plan. The Order directed NERC to file the modified standards and Implementation Plan within 90 days.

The modifications to the NERC set of reliability standards and associated Implementation Plan requested in this SAR will enable NERC to comply with the FERC directives issued on September 30, 2009 and will ensure the protection of the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operation of the North American bulk power system.

**Brief Description:**

The Commission's September 30, 2009 Order directs NERC to submit a compliance filing within 90 days of the Order (i.e., by December 28, 2009) which, among other things, includes the following modifications:

- A modification to Reliability Standard CIP-006-2 – Cyber Security — Physical Security to add a requirement on visitor control programs, including the use of visitor logs to document entry and exit.
- A modification to Reliability Standard CIP-008-2 – Cyber Security — Incident Reporting and Response Planning, Requirement R1.6 to remove the last sentence of CIP-008-2 Requirement R1.6.
- A revised Version 2 Implementation Plan addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to the September 30 Order.

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

The documents recommended to be modified and the associated specific modifications are attached. Please refer to the attached documents for the detailed changes.

Although the Commission directed changes to only two of the eight CIP-002-2 thru CIP-009-2 reliability standards, conforming changes are proposed for the remaining six CIP Reliability Standards (CIP-002-2 thru CIP-005-2, CIP-007-2, CIP-009-2) to correct the cross references within the set of standards. If left untouched, the Purpose statements, and many requirements within the set of standards would be incorrect as they all reference CIP-002-2 through CIP-009-2.

***Reliability Functions***

| **The Standard will Apply to the Following Functions** *(Check box for each one that applies.)* | | |
|---|---|---|
| ☐ | Reliability Assurer | Monitors and evaluates the activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the bulk power system within a Reliability Assurer Area and adjacent areas. |
| ☒ | 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. |
| ☒ | 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. |
| ☒ | Interchange Authority | Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas. |
| ☒ | Planning Coordinator | Assesses the longer-term reliability of its Planning Coordinator Area. |
| ☐ | Resource Planner | Develops a >one year plan for the resource adequacy of its specific loads within its portion of the Planning Coordinator's Area. |
| ☒ | Transmission Owner | Owns and maintains transmission facilities. |
| ☒ | Transmission Operator | Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area. |
| ☐ | Transmission Planner | Develops a >one year plan for the reliability of the interconnected Bulk Electric System within the Transmission Planner Area. |
| ☒ | Transmission Service Provider | Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff). |
| ☐ | Distribution Provider | Delivers electrical energy to the End-use customer. |
| ☒ | Generator Owner | Owns and maintains generation facilities. |
| ☒ | Generator Operator | Operates generation unit(s) to provide real and reactive power. |
| ☐ | Purchasing-Selling Entity | Purchases or sells energy, capacity, and necessary reliability-related services as required. |
| ☒ | Load-Serving Entity | Secures energy and transmission service (and reliability-related services) to serve the End-use Customer. |

***Reliability and Market Interface Principles***

| **Applicable Reliability Principles** *(Check box for all that apply.)* | |
|---|---|
| ☐ | 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. |
| ☐ | 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. |
| ☐ | 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. |
| ☒ | 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented. |
| ☒ | 5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems. |
| ☒ | 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions. |
| ☒ | 7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis. |
| ☒ | 8. Bulk power systems shall be protected from malicious physical or cyber attacks. |

| **Does the proposed Standard comply with all of the following Market Interface Principles?** *(Select 'yes' or 'no' from the drop-down box.)* |
|---|
| 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 |

***Related Standards***

| Standard No. | Explanation |
|---|---|
| CIP–002–2 | Cyber Security — Critical Cyber Asset Identification – Conforming changes |
| CIP–003–2 | Cyber Security — Security Management Controls – Conforming changes |
| CIP–004–2 | Cyber Security — Personnel and Training – Conforming changes |
| CIP–005–2 | Cyber Security — Electronic Security Perimeter(s) – Conforming changes |
| CIP-006-2 | Cyber Security — Physical Security – FERC directed modifications |
| CIP–007–2 | Cyber Security — Systems Security Management – Conforming changes |
| CIP–008–2 | Cyber Security — Incident Reporting and Response Planning – FERC directed modifications |
| CIP–009–2 | Cyber Security — Recovery Plans for Critical Cyber Assets – Conforming changes |

***Related SARs***

| SAR ID | Explanation |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

***Regional Variances***

| Region | Explanation |
|---|---|
| ERCOT | |
| FRCC | |
| MRO | |
| NPCC | |
| SERC | |
| RFC | |
| SPP | |
| WECC | |