

## Standard Authorization Request Form

Title of Proposed Standard Cyber Security Violation Severity Levels (Project 2008-14)	
Request Date	11/03/2008
Approved by Standards Committee 12/16/08	
<u>Revised Date</u>	<u>3/13/09</u>

<b>SAR Requester Information</b>	<b>SAR Type</b> ( <i>Check a box for each one that applies.</i> )
Name            Larry Bugh	<input type="checkbox"/> New Standard
Primary Contact    Larry Bugh	<input checked="" type="checkbox"/> Revision to existing Standard
Telephone        (330) 247-3046 Fax                (330) 456-3648 Fx	<input type="checkbox"/> Withdrawal of existing Standard
E-mail <a href="mailto:larry.bugh@rfirst.org">larry.bugh@rfirst.org</a>	<input type="checkbox"/> Urgent Action

## Standards Authorization Request Form

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

The Federal Energy Regulatory Commission (FERC) in Order 706 (Mandatory Reliability Standards for Critical Infrastructure Protection - Issued January 18, 2008) approved eight Critical Infrastructure Protection (CIP) reliability standards and directed NERC to develop modifications to the CIP Reliability Standards CIP-002 thru CIP-009 to address specific concerns. Included in the directives of Order 706 was a directive for NERC to file Violation Severity Levels for reliability standards CIP-002 thru CIP-009 before compliance audits begin on July 1, 2009.

The standards CIP-002 thru CIP-009 were originally filed with "Levels of Non-Compliance" instead of "Violation Severity Levels" and now need to be revised before compliance audits begin in 2009. This is consistent with the Order on Compliance Filing dated June 7, 2007 (Docket #RR06-1-007), which directed NERC to replace the 'Levels of Non-compliance' in the 83 regulatory-approved standards with 'Violation Severity Levels' which also required development of Violation Severity Levels for any new or revised standards.

Proposed project 2008-14 Cyber Security Violation Severity Levels will meet the FERC directives regarding the development of Violation Severity Levels for the cyber group of standards:

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

**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.)

NERC, as the ERO, is required to comply with FERC directives. By developing 'Violation Severity Levels' for the CIP-002 thru CIP-009, NERC and the industry, will be compliant with FERC's directive. By adding VSLs to CIP-002 thru CIP-009 the ERO's Sanctions Guidelines will be able to be used as designed. The Sanctions Guidelines use 'Violation Severity Levels' (along with Violation Risk Factors) as starting points in determining a penalty or sanction.

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

Develop Violation Severity Levels for reliability standards CIP-002 thru CIP-009 [versions 1 and 2 \(under development separately\)](#), using the standard development process in order to obtain stakeholder consensus on the assignment of Violation Severity Levels for this set of standards.

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

The drafting team will develop proposed 'Violation Severity Levels' in accordance with the

## Standards Authorization Request Form

guidelines for assigning VSL developed by the drafting team for Project 2007-23- Violation Severity Levels for the following set of reliability standards:

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

[Version 2 of the standards CIP-002 through CIP-009 is being developed separately. To facilitate prompt completion of version 2 of CIP-002 through CIP-009 including VSLs, the drafting team will draft VSLs for both versions 1 and 2 of standards CIP-002 through CIP-009.](#) While drafting the VSLs for this set of reliability standards, the drafting team will also need to take into consideration FERC's Violation Severity Level Order of June 19, 2008 and any related FERC Orders or Rules.

### 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 Reliability Organization	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"/> <input checked="" type="checkbox"/>	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
<input type="checkbox"/> <input checked="" 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"/> <input checked="" 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	Ensures the real-time operating reliability of the transmission

**Standards Authorization Request Form**

---

	Operator	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"/> <input checked="" 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.

**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 type="checkbox"/>	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
<input type="checkbox"/>	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
<input 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>

***Related SARs***

<b>SAR ID</b>	<b>Explanation</b>

***Regional Variances***

<b>Region</b>	<b>Explanation</b>
ERCOT	
FRCC	
MRO	
NPCC	
SERC	
RFC	
SPP	
WECC	