Standard Authorization Request Form

Title of Proposed Standard	Cyber Security
Request Date	May 2, 2003

SAR Requestor Information

Name	Charles Noble (on behalf of CIPAG)	**SAR Type** (Check box for one of these selections.)	
Company		☒	New Standard
Telephone		☐	Revision to Existing Standard
Fax		☐	Withdrawal of Existing Standard [1]
E-mail		☐	Urgent Action

Purpose/Industry Need (Provide one or two sentences.)

To reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets (computers, software and communication networks) that support those systems.

Brief Description

This standard will require that critical cyber assets related to the reliable operation of the bulk electric systems are identified and protected. Requirements will be included in the standard to identify the responsible person(s), create and implement programs and procedures, perform a thorough assessment of cyber security, and implement appropriate and technically feasible security improvements.

Reliability Functions

The Standard will Apply to the Following Functions *(Check box for each one that applies.)*		
☒	Reliability Authority	Ensures the reliability of the bulk transmission system within its Reliability Authority area. This is the highest reliability authority.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within its metered boundary and supports system frequency in real time
☒	Interchange Authority	Authorizes valid and balanced Interchange Schedules
☐	Planning Authority	Plans the bulk electric system
☒	Transmission Service Provider	Provides transmission services to qualified market participants under applicable transmission service agreements
☐	Transmission Owner	Owns transmission facilities
☒	Transmission Operator	Operates and maintains the transmission facilities, and executes switching orders
☐	Distribution Provider	Provides and operates the “wires” between the transmission system and the customer
☒	Generator	Owns and operates generation unit(s) or runs a market for generation products that performs the functions of supplying energy and Interconnected Operations Services
☐	Purchasing-Selling Entity	The function of purchasing or selling energy, capacity and all necessary Interconnected Operations Services as required
☒	Load-Serving Entity	Secures energy and transmission (and related generation services) to serve the end user

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check box for all that apply.)*	
☐	1. Interconnected bulk electric 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 electric 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 electric 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 electric 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 electric systems.
☒	6. Personnel responsible for planning and operating interconnected bulk electric systems shall be trained, qualified and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk electric systems shall be assessed, monitored and maintained on a wide area basis.
Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*	
1. The planning and operation of bulk electric systems shall recognize that reliability is an essential requirement of a robust North American economy. Yes	
2. An Organization Standard shall not give any market participant an unfair competitive advantage.Yes	
3. An Organization Standard shall neither mandate nor prohibit any specific market structure. Yes	
4. An Organization Standard shall not preclude market solutions to achieving compliance with that Standard. Yes	
5. An Organization 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	

Detailed Description

1. Recent security incidents have impacted cyber systems that are critical to electric system reliability.

2. The frequency and severity of cyber attacks are increasing.

3. Ongoing world events may lead to further cyber attacks that impact bulk electric system reliability.

4. The standard is based upon guidelines established by the NERC Critical Infrastructure Protection Advisory Group (CIPAG) and approved by the NERC Board of Trustees. These guidelines were submitted to the industry for review and comment. Comments received were reviewed and included in the guidelines, as appropriate.

5. The standard is also based upon the proposed cyber security standard drafted by a NERC-sponsored industry group, approved by CIPAG and the NERC Board of Trustees, and submitted to FERC at its request. Two industry comment periods were included in the development of this proposed cyber security standard.

6. According to the FERC's April 28, 2003 "White Paper, Wholesale Power Market Platform" (FERC Docket No. RM01-12) FERC plans to adopt NERC's Cyber Security Standard.

Reliable electric system operations are highly interdependent, and a failure of one part of the generation, transmission, or grid management system can compromise the reliable operation of a major portion of the regional grid. Similarly, the wholesale electric market as a network of economic transactions and interdependencies relies on the continuing reliable operation of not only physical grid resources, but also the operational infrastructure of monitoring, dispatch, and market software and systems. Because of this mutual vulnerability and interdependence, it is necessary to safeguard the critical cyber assets that support bulk electric system operations by establishing standards to assure that a lack of cyber security for one critical asset does not compromise security and risk grid or market failure.

This standard requires that responsible entities understand the role of cyber security in electric infrastructure reliability, have identified their critical cyber assets related to bulk electric system operations, and have a security program in place. This program should mitigate the impact to bulk electric system operations from acts, either accidental or malicious, that could cause wide-ranging, harmful impacts. A basic cyber security program for bulk electric system operations shall cover governance, planning, prevention, operations, incident response, and business continuity. This standard is intended to ensure that appropriate mitigating plans and actions are in place, recognizing the differing roles of each responsible entity and the differing risks being managed.

This cyber security standard shall primarily focus on electronic systems, which include hardware, software, data, related communications networks, control systems as they impact electric system operations, and personnel. In addition, physical security shall be addressed to the extent that it is necessary to assure a secure physical environment for cyber resources.

This standard will apply to entities performing the Reliability Authority, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Operator, Generator, and Load Serving Entity and functions.

This standard provides definition of terms and the minimum requirements to implement and maintain a

cyber security program to protect cyber assets critical to reliable electric system operations.

Definitions

Critical Cyber Assets: Those computers, including installed software and electronic data, and communication networks that support, operate, or otherwise interact with the bulk electric system operations. This definition currently does not include process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations.

Electronic Security Perimeter: The border surrounding the network or group of sub-networks (the "secure network") to which the critical cyber assets are connected.

Physical Security Perimeter: The border surrounding computer rooms, telecommunications rooms, operations centers, and other clearly defined locations in which critical cyber assets are housed and access is controlled.

Cyber Security Incident: Any event or failure (malicious or otherwise) that disrupts the proper operation of a Critical Cyber Asset.

Incident Response: Responding to, and reporting a cyber security incident.

Compliance Monitor: The organization responsible for monitoring compliance with this standard in accordance with the NERC compliance enforcement program.

Related SARs

SAR ID	Explanation
None	

Regional Differences

Region	Explanation
None	

Related NERC Planning Standards/Operating Policies

Standard No.	Explanation
None	

Industry Representatives who participated in developing this SAR	Charles Noble – ISO New England Jerry Freese – American Electric Power Larry Brown – Edison Electric Institute Ken Hall – Edison Electric Institute Larry Bugh – ECAR Regional Council Scott Mix – Electric Power Research Institute Jim Orcheson – Independent Market Operator (Ontario) Roger Lampila – New York ISO James Strange –American Public Power Association Sergio Guzman – Florida Power & Light Lyman Shaffer – Pacific Gas & Electric John Fridye – Reliant Resources Kurt Muehlbauer – Exelon Jay Cribb – Southern Company Seiki Harada – BC Hydro Greg Fraser – Manitoba Hydro Lewis Griffith – Centerpoint Energy Kevin Perry – Southwest Power Pool