Standard Authorization Request Form

Title of Proposed Standard	Cyber Security
Request Date	May 2, 2003; Revised November 24, 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 protect the critical cyber assets (computers, software, and communications networks) essential to the reliability of the bulk electric system.

Brief Description

This standard is based on the Urgent Action Cyber Security Standard that was adopted by the NERC Board of Trustees on August 13, 2003. The standard requires 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 for responsible entities to create and implement programs and procedures, perform on-going assessments, and implement appropriate and technically feasible improvements necessary to meet the requirements of this standard. Security programs include the responsible entity's policies, standards, procedures, training, and auditing controls for the implementation of this standard. The standard is intended to replace the Urgent Action Cyber Security Standard.

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.
☐	Resource Planner	Develops a long-term (>1year) plan for the resource adequacy of specific loads within a Planning Authority area.
☐	Transmission Planner	Develops a long-term (>1 year) plan for the reliability of transmission systems within its portion of the Planning Authority area.
☒	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 Owner	Owns and maintains generation unit(s).
☒	Generator Operator	Operates generation unit(s) and 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.
☐	Market Operator	Integrates energy, capacity, balancing, and transmission resources to achieve an economic, reliability-constrained dispatch.
☒	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. A Reliability Standard shall not give any market participant an unfair competitive advantage. Yes
3. A Reliability Standard shall neither mandate nor prohibit any specific market structure. Yes
4. A Reliability Standard shall not preclude market solutions to achieving compliance with that Standard. Yes
5. 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

Detailed Description

This standard identifies the minimum requirements to implement and maintain a cyber security program to protect cyber assets critical to reliable bulk electric system operation. This standard applies to Reliability Authorities, Balancing Authorities, Interchange Authorities, Transmission Service Providers, Transmission Owners, Transmission Operators, Generator Owners, Generator Operators, and Load Serving Entities, as described in NERC's Functional Model.

Reliable bulk electric system operations are highly interdependent, and the failure of key/critical elements of the generation, transmission, or grid management system can potentially compromise the reliable operation of major portions 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 provide a level of assurance that even a single compromise of a critical cyber asset does not compromise system security, and, thus, risk grid or market failure.

This standard shall primarily focus on electronic systems including: hardware, software, data, related communications networks, and control systems as they impact bulk 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 critical cyber assets and their operation. If a network consisting of critical cyber assets also includes non-critical cyber assets, those non-critical cyber assets must comply with the requirements of this standard. This standard shall require that third-party providers of services used to ensure reliability (e.g. Interchange Distribution Calculator data) must comply with the standard for systems providing those services. This standard shall require that the responsible entities that must comply with this standard identify and protect themselves from threats from interconnected cyber systems.

This standard shall require that entities identify and protect critical cyber assets related to the reliable operation of the bulk electric system and have an ongoing program in place to ensure their protection. This program must at a minimum, meet the requirements set forth in the standard as they relate to governance, planning, prevention, operations, incident response, and continuity of operations. As a result, this program will mitigate the effect of acts of malicious or unknown origin that could cause wide-ranging, harmful impact to the bulk electric system.

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 standard shall use as its starting point the Urgent Action Cyber Security Standard adopted by the NERC Board of Trustees on August 13, 2003. Building on that baseline, this permanent standard shall reflect input received during the balloting of the Urgent Action Standard and comments received in response to this SAR that are aimed specifically at the Urgent Action Standard.

Reliable and secure data communications networks are key to continuity of operational control and ongoing management of critical cyber assets. Some organizations own and operate their own data communications infrastructure, others acquire network services from the Telecommunications Sector, and some meld both private and public resources to create the data communications capabilities necessary to reliably operate and control critical cyber assets. Whether the means of data communications are of private or public origin, be they physical or logical in operation, it is incumbent upon owners and/or operators of critical cyber assets to design and provision data communications capabilities to be reliably available. Accordingly, data communication systems joining two or more distinct electronic security perimeters must be provisioned to a level of reliability at least equal to 99.5% availability per annum. Where the data communications capability utilizes shared public network resources (e.g., POTS, frame relay, the Internet, etc.), using either leased-permanent or temporary dial-up methods, all data must be

encrypted to ensure authorized use of the data communications capability through authentication, confidentiality, integrity, and (as appropriate) non-repudiation.

Definitions

Cyber Assets: Those systems (including hardware, software, and data) and communication networks (including hardware, software, and data) associated with bulk electric system operation. This definition applies only to systems or devices that use a network protocol stack for communications.

Critical Cyber Assets: Cyber assets whose loss or compromise could adversely impact the reliability of bulk electric system operations. Cyber assets that perform bulk electric system functions such as telemetry, monitoring and control, automatic generator control load shedding, black start, real time power system modeling, special protection systems, power plant control, substation automation control, and real time inter-utility data exchange are included at a minimum.

Electronic Security Perimeter: The logical border surrounding the network or group of sub-networks (the "secure network") to which the critical cyber assets are connected, and for which access is controlled.

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

Responsible Entity: The organization performing the reliability function to which the standard applies.

Security Incident: Any physical or cyber event of malicious or unknown origin that disrupts the functional operation of a critical cyber asset or compromises the electronic or physical security perimeters.

Related Standards

SAR ID	Explanation
Urgent Action Cyber Security Standard	This standard is based on the Urgent Action Cyber Security Standard (1200) approved by the NERC Board of Trustees on August 13, 2003.

Regional Differences

Region	Explanation
None	

Related NERC Planning Standards/Operating Policies

Standard No.	Explanation
None	

Implementation Plan

Description: *(Provide plans for the implementation of the proposed standard, including any known systems or training requirements.)*

While a formal implementation plan will be developed and published when the standard is drafted, the SAR drafting team suggests consideration of a plan that permits requiring compliance by entities as they certify (where appropriate) to the functional model. The implementation plan must account for the current state of technology and reasonable timeframes to update existing systems.

Industry Representatives who participated in developing this SAR	Chuck Noble — ISO New England Michael Allgeier — Lower Colorado River Authority David Ambrose — Western Area Power Administration Larry Bugh — ECAR Regional Council Greg J. Fraser — Manitoba Hydro Roger L. Lampila — New York Independent System Operator John S.F. Lim — Consolidated Edison Co. of New York, Inc. John G. Maguire — PJM Interconnection, LLC Paul McClay — Tampa Electric Company Kurt Muehlbauer — Exelon Corporation David L. Norton — Entergy Transmission James Sample — California ISO Phil Sobol — Aquila, Inc. Howard Tarler — New York State Dept. of Public Service John D. Varnell — Tenaska Power Services Co. William R. Wagner — Calpine Corporation Bob Wallace — Ontario Power Generation