Standard Authorization Request Form

Title of Proposed Standard	Cyber Security
Request Date	May 2, 2003; Revised November 24, 2003; Revised February 19, 2004, Final Revision March 8, 2004

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 (hardware, software, data, 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 approved 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 security programs, perform assessments, and implement appropriate improvements necessary to ensure cyber security. Security programs include the responsible entity's policies, standards, procedures, training, and auditing controls for the implementation of this standard. The intention of this standard is to replace the Urgent Action Cyber Security Standard.

Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.

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. 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

Bulk electric system operations are highly interdependent. The failure of a generation, transmission, or grid management system can potentially compromise the reliable operation of the bulk electric system. 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 the compromise of a critical cyber asset does not compromise system security, and, thus, risk bulk electric system reliability. The purpose of developing this standard is to prevent and/or minimize adverse impact to generation and transmission of electricity through malicious or unethical tampering of computer based communications, control, monitoring, and protection systems.

This standard will define the minimum requirements to implement and maintain a cyber security program to protect cyber assets that are critical to the reliable operation of the bulk electric system. This standard applies to entities performing the Reliability Authority, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity functions.

This standard shall focus primarily on electronic systems, including: hardware, software, data, and related communication devices that use a routable protocol, such as OSI and TCP/IP (Transmission Control Protocol/Internet Protocol), or are dial-up accessible; monitoring and control systems as they impact bulk electric system operations; and, security issues pertaining to all personnel that have access to critical cyber assets. 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. Where 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 requires that the responsible entities to which this standard applies identify and protect themselves from threats from interconnected cyber systems. This standard requires that responsible entities ensure that third parties who support or provide services used to ensure bulk electric system reliability comply with this standard for those services.

This standard requires that responsible entities identify and protect critical cyber assets related to the reliable operation of the bulk electric system, and have an ongoing security program in place to ensure protection of those assets. Responsible entities will identify critical cyber assets using their preferred risk-based assessment methodology.

This program must, at a minimum, meet the requirements set forth in the standard as they relate to governance, planning, prevention, operations, incident response, security incident reporting, and continuity of operations to mitigate the effect of acts of malicious or suspicious 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 will use as its starting point the Urgent Action Cyber Security Standard approved 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.

Definitions

Cyber Assets: Those systems (including hardware, software and data) and communication networks (including hardware, software and data) associated with bulk electric system assets.

Critical Cyber Assets: Those cyber assets that perform critical bulk electric system functions such as telemetry, monitoring and control, automatic generator control, load shedding, blackstart, 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. The loss or compromise of these cyber

assets would adversely impact the reliable operation of bulk electric system assets.

Bulk Electric System Asset: Any facility or combination of facilities that, if unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, or would have a detrimental impact to the reliability or operability of the electric grid, or would cause significant risk to public health and safety.

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 locations in which critical cyber assets are housed and for which access is controlled.

Responsible Entity: The organization performing the reliability function, as identified in the Reliability Function table.

Incident: Any physical or cyber event that:

disrupts the functional operation of a critical cyber asset, or

compromises the electronic or physical security perimeters.

Security Incident: Any incident of malicious or suspicious origin.

Related Standards

SAR ID	Explanation
Urgent Action	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.

Proposed Implementation __ days after Board of Trustees adoption or on (date):

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