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

Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: sarcomm@nerc.com with "Standard Comments" in the subject line.

Please review the SAR and answer the questions in the yellow boxes.

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to timg@nerc.com.

SAR Commenter Information (For Individual Commenters)	
Name	Seiki Harada
Organization	BC Hydro
Industry Segment	# 1, 3, 5 and 6
Telephone	604 623 3550
E-mail	Seiki.harada@bchydro.com

Key to Industry Segments:

1 – Trans. Owners
2 – RTOs, ISOs, RRCs
3 – LSEs
4 – TDUs
5 - Generators
6 - Brokers, Aggregators, and Marketers
7 - Large Electricity End Users
8 - Small Electricity Users
9 - Federal, State, and Provincial Regulatory or other Govt. Entities

SAR Commenter Information (For Groups Submitting Group Comments)		
Name of Group:	**Group Representative:** **Representative Phone:** **Representative Email:**	
List of Group Participants that Support These Comments:		
Name	**Company**	**Industry Segment #**

Background Information:

Notes to Industry Commenters:

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

1. Do you agree with the definitions included in the SAR?

☐ Yes

x☐ No

According to the present version of the Cyber Asset Definition, a SCADA system may be exempted from the application of the standards if it happens to use a very old networking that is not on a stacked protocol. I would say all SCADA for bulk power system must be included.

Additionally, the detailed description section essentially lists two major purposes for the standards: bulk system reliability and efficient market. Looking at the definitions for Cyber Assets and Critical Cyber Assets, they are defined only for bulk system reliability. If we are truly serving the two purposes, we must include such systems as eTAG, OASIS and other market oriented systems.

The definition of Critical Cyber Assets includes 'black start'. I am not sure if this is pointing to the process to restart the part of the grid that collapsed, or the systems required to start up a generating station that tripped off. Perhaps, we need to qualify the words 'black start'.

2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

☐ Yes

x☐ No

Comments:

44 hours per year is a lot of time to be down for 7x24 critical links. I would say we should shoot for about half of that. Further, the cumulative down time alone is not a good measure. It should be combined with the frequency of the communications link going down. For example, even if the communications link is down for only 10 hours per year, if the link was down five times every day for 10 seconds each randomly, the link would be useless.

3. The SAR does not address the availability of critical cyber assets. Should requirements be included? If so, how would availability be measured, especially for

partial failures? What level of availability should be required?

☐ Yes

x☐ No

Comments:

A good level of availability is a function of 1) implementing adequate security measures, 2) maintaining/patching software, hardware and data, 3) operating the systems safely and properly, and 4) external forces which try to disrupt orderly operation. Similar to the number of cyber incidents an entity may encounter in a year, most external factors are not under the control of the entity in question. For example, if there is an overwhelming attack on the DNS server in one sector of the Internet, all Internet based systems and networks might feel the impact (and thus the degraded availability). It is not reasonable to set a standard over a measure for which the entity does not have total control over.

4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:

a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers

x☐ Yes

☐ No

Comments

b. SCADA master station to RTU communications using peer-to-peer communications protocols

x☐ Yes

☐ No

Comments

c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)

x☐ Yes

☐ No

Comments

d. Data collection servers communications to substation IEDs

x☐ Yes

☐ No

Comments

e. If the above were included, how long would each take to complete?

Comments:

This will take a long time to implement (> 10 years?) and a lot of money. We may consider implementing these new measures only to the new implementations and major upgrades as of a certain future date.

5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?

☐ Yes

x☐ No

Comments:

It makes sense to provide redundancy for key SCADA /EMS systems. However, I am not sure if we should be designing in redundancies in ALL the cyber assets declared as 'critical'. It may not be economically feasible to prodive redundancy for all components of all critical systems. Also, we may find that some 'critical' systems are 'more critical' than others….

6. Please enter any other comments you have regarding this SAR in the space below.

Comments

This set of standards is much more wide-encompassing than the Urgent SAR standards. We will need to give sufficient lead time for all participants to implement the additional requirements.

Comment Form — 2nd Posting of the 'Cyber Security' Standard Authorization Request

Note — This form is to be used to comment on version 2 of the Cyber Security Standard Authorization Request (SAR).

E-mail this form between December 1, 2003–January 21, 2004, to: sarcomm@nerc.com with "Standard Comments" in the subject line.

Please review the SAR and answer the questions in the yellow boxes.

If you have questions, please call Tim Gallagher at 609-452-8060 or send a question to timg@nerc.com.

SAR Commenter Information (For Individual Commenters)	
Name	Joe Weiss
Organization	KEMA
Industry Segment #	8
Telephone	(408) 253-7934
E-mail	jweiss@kemaconsulting.com

Key to Industry Segments:

1 – Trans. Owners
2 – RTOs, ISOs, RRCs
3 – LSEs
4 – TDUs
5 - Generators
6 - Brokers, Aggregators, and Marketers
7 - Large Electricity End Users
8 - Small Electricity Users
9 - Federal, State, and Provincial Regulatory or other Govt. Entities

SAR Commenter Information (For Groups Submitting Group Comments)		
Name of Group:	**Group Representative:** **Representative Phone:** **Representative Email:**	
List of Group Participants that Support These Comments:		
Name	**Company**	**Industry Segment #**

Background Information:

Notes to Industry Commenters:

This standard authorization request will *set the scope* for a NERC standard dealing with cyber security requirements as they pertain to maintaining the integrity and reliability of the interconnected electric systems of North America. When the SAR has been fully developed, the NERC Standards Authorization Committee (SAC) will be contacted for permission to begin drafting the standard.

When completed, the standard will be presented to the NERC registered ballot body for approval. If approved, the standard would replace the urgent action cyber security standard approved by the industry in June 2003.

In developing version 2 of this SAR, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to version 1 of this SAR.

Notable changes made to the SAR in response to industry comments include:

- Revised definitions to added greater clarity
- A reference to the relationship between this SAR and the urgent action standard
- Clarification
- A re-stated purpose
- Addition of new functions to correlate to the recently approved version 2 of NERC's Functional Model
- Removal of 'justification' items that were used in the urgent action SAR
- Clarification regarding third-party vendor requirements
- Clarification regarding requirements for communication links between secure perimeters
- Increased applicability of the standard (both in terms of entities and assets)

1. Do you agree with the definitions included in the SAR?

☐ Yes

X No

Comments:

The Cyber Assets definition states: "This definition applies only to systems or devices that use a network stack protocol for communications." This statement needs to be deleted. Cyber assets are not dependent on specific communication protocols. Cyber assets associated with bulk electric system operation utilize non-network stack (non-TCP/IP) protocols such as Modbus, Profibus, and conventional serial RTU communications. Additionally, dial-up modems and unsecured radio links are obviously cyber vulnerabilities and do not use network stack protocols.

The Security Incident definition states: "…any physical or cyber event of malicious or unknown origin…" This is not inclusive enough. There can be cyber events of known, benign origins that can disrupt functional operation of critical cyber assets and cause security incidents. There have been several confirmed cases of benign origin causing denial of service in the utility and other process industries.

2. The SAR requires that data communications between secure perimeters be engineered to a statistical probability of 99.5% uptime on an annual basis (or, 43.8 hours downtime, per year). Do you agree with this as a reasonable design goal?

☐ Yes

X No

Comments:

The critical need for communications is during an upset event such as August 14th. The requirement should be that communications have a 99.5% availability including during upset events.

3. The SAR does not address the availability of critical cyber assets. Should

requirements be included? If so, how would availability be measured, especially for partial failures? What level of availability should be required?

☐ Yes

X No

Comments:

SCADA specifications often require 99.95% availability for critical functions. It is critical that the function be maintained, not necessarily the asset.

4. The SAR does not require that SCADA or PCS communications be encrypted. Should this requirement be added for:

a. Use of Inter-Control Center Communications Protocol (ICCP), primarily between control centers

☐ Yes

X No

Comments:

Encryption does not guarantee the critical functions of authentication and message integrity. Encryption may not be practical for certain generation of SCADA systems. It may not be possible to implement encryption for current plant controls and substation equipment.

b. SCADA master station to RTU communications using peer-to-peer communications protocols

☐ Yes

X No

Comments: Same

c. SCADA master station to RTU communications over an established communications stack (e.g. TCP/IP)

☐ Yes

X No

Comments: Same

d. Data collection servers communications to substation IEDs

☐ Yes

X No

Comments: Same

e. If the above were included, how long would each take to complete?

Comments: See comment 4a

5. The SAR does not require redundancy of critical cyber assets, but rather their protection. Should redundancy also be required?

☐ Yes

X No

Comments:

Redundancy does not necessarily mitigate cyber vulnerabilities. Two systems on the same compromised network can be equally vulnerable even though there is "traditional" redundancy.

6. Please enter any other comments you have regarding this SAR in the space below.

Comments:

1. Distribution providers should be included since many large transmission substations also include distribution equipment that often communicate with transmission devices (and vice versa) making them equally cyber vulnerable. Additionally, DOE tasked NERC to address the electric utility industry- this includes distribution.
2. Market operators should be included per the second paragraph of the detailed description and also because they are part of the electric industry.
3. Encryption should not be required until is it confirmed by testing that encryption is the appropriate technology to meet the required functional needs. This has not yet occurred.

Cyber Security SAR Drafting Team Roster

Michael Allgeier
Data Security Officer
Lower Colorado River Authority (LCRA)
3700 Lake Austin Blvd.
Austin, TX 78703
Office Telephone: 512 473-3200 ext. 2449
Mobile Telephone: 512 779-6459
Fax:
Michael.allgeier@lcra.org

David Ambrose
SCADA System Manager
Western Area Power Administration – Rocky Mountain Regional Office
5555 E. Crossroads Blvd.
Loveland, Colorado 80538
Office Telephone: 970-461-7354
Mobile Telephone: 970-980-6831
Fax: 970-461-7213
ambrose@wapa.gov

Larry Bugh
Manager, Information Technology
ECAR
220 Market Ave. S., Ste 501
Canton, OH 44702
Office Telephone: 330.580.8017
Mobile Telephone: 330.704.0716
Fax: 330.456.5408
larryb@ecar.org

Greg J. Fraser
Manager, System Support Department
Manitoba Hydro
System Support Department
Box 815
Winnipeg, MB Canada R3C 2P4
Office Telephone: (204) 487-5379
Mobile Telephone:
Fax: (204) 487-5394
gjfraser@hydro.mb.ca

Roger L. Lampila
IT Security Administer
New York Independent System Operator
3890 Carman Road
Schenectady, NY 12303
Office Telephone: 518 356 6043
Mobile Telephone: 518 475 7843
Fax: 518 356 6118
rlampila@nyiso.com

John S.F. Lim, CISSP
Systems Manager
Consolidated Edison Co. of New York, Inc.
4 Irving Place, Room 349-S
New York, NY 10003
Office Telephone: 212-460-2712
Mobile Telephone: 917-690-5406
Fax: 212-387-2100
limj@coned.com

John G. Maguire
Senior Security Analyst
PJM Interconnection, LLC
955 Jefferson Drive
Norristown, PA 19403
Office Telephone: 610-666-4420
Mobile Telephone: 610-633-8109
Fax:
maguij@pjm.com

Paul McClay
Manager of Information Security
Tampa Electric Company
PO Box 111, Tampa, FL 33601
Office Telephone: 813-225-5287
Mobile Telephone: 813-376-2340
Fax: 813-225-5302
pfmcclay@tecoenergy.com

Kurt Muehlbauer
Manager of Information Assurance
Exelon Corporation
227 West Monroe, Room 1056
Chicago, IL 60606
Office Telephone: 312.394.3772
Mobile Telephone:
Fax: 312.394.8888
kurt.muehlbauer@exeloncorp.com

David L. Norton, CISSP
Sr. Information Security Analyst
Entergy Transmission
639 Loyola Avenue, MS: LMOB17A
New Orleans, LA 70113-3125
Office Telephone: 504-310-5763
Mobile Telephone: 504-237-5657
Fax: 504-310-5762
DNORT91@entergy.com

Cyber Security SAR Drafting Team Roster

James Sample
Manager of Information Security Services
California ISO
151 Blue Ravine Road
Folsom, CA 95630
Office Telephone: 916-608-5891
Mobile Telephone: 916-802-7537
Fax:
jsample@caiso.com

Phil Sobol
Cyber Security Specialist
Aquila, Inc.
20 W 9th, Kansas City, MO 64105
Office Telephone: 816-467-3303
Mobile Telephone:
Fax: 816-467-3238
phil.sobol@aquila.com

Howard Tarler
Chief, Bulk Transmission Systems Section
New York State Dept. of Public Service
3 Empire State Plaza
Albany, NY 12223-1350
Office Telephone: 518 486 2483
Mobile Telephone: 518 441 3878
Fax: 518 473 2420
Howard_tarler@dps.state.ny.us

John D. Varnell
Manager of technology
Tenaska Power Services Co.
1701 E. Lamar Blvd.
Arlington, TX 76006
Office Telephone: 817-462-1037
Mobile Telephone: 817-312-7261
Fax: 817-462.1035
jvarnell@tnsk.com

William R. Wagner
IS Director, Information Security and Business Continuity
Calpine Corporation
104 Woodmere Road
Folsom, California 95630
Office Telephone: 916-608-3799
Mobile Telephone: 916-716-2511
Fax: 916-294-0921
wwagner@calpine.com

Bob Wallace
Manager–IT Security
Ontario Power Generation
700 University Avenue
Toronto, Ontario, Canada
M5G 1X6
Mail Stop: H10 D11
Office Telephone: (416) 592-8297
Mobile Telephone: (416) 988-3244
Fax: (416) 592-5514
Bob.wallace@opg.com

Chuck Noble
Requestor
ISO New England
One Sullivan Road
Holyoke, MA 01040
Office Telephone: (413) 540-4232
Fax: (413) 535-4109
cnoble@iso-ne.com

Lou Leffler
Staff Coordinator
North American Electric Reliability Council
116-390 Village Boulevard
Princeton, NJ 08540
Phone: 609-452-8060
Fax: 609-452-9550
Lou.Leffler@nerc.net

Lynn Costantini
Staff Coordinator
North American Electric Reliability Council
116-390 Village Boulevard
Princeton, NJ 08540
Phone: 609-452-8060
Fax: 609-452-9550
Lynn.Costantini@nerc.net