UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Rule Regarding Critical Energy	)	Docket No. RM02-4-000
Infrastructure Information	)	Docket No. PL02-1-000

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

The North American Electric Reliability Council ("NERC") submits these comments in response to the Notice of Proposed Rulemaking ("NOPR") that the Commission issued on September 5, 2002 on the subject of protecting critical energy infrastructure information. NERC welcomes the Commission's attention to this important issue.

NERC is a not-for-profit organization formed after the Northeast blackout in 1965 to promote the reliability of the bulk electric system that serves North America. It works with all segments of the electric industry, as well as customers, to "keep the lights on" by developing and encouraging compliance with rules that provide for the reliable operation of the electric system and an adequate supply of electrical energy. NERC comprises ten Regional Reliability Councils that account for virtually all of the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico. In addition, NERC serves as the electric industry's designated Information Sharing and Analysis Center working in coordination with the Federal government's National Infrastructure Protection Center. Furthermore, NERC has also been designated the Electric Power Sector Coordinator by the Department of Energy.

The terrorist attacks of September 11 have made it imperative for all of us to reassess the scope and magnitude of the risks we face and the steps necessary to guard against those risks. Access to critical energy infrastructure information ("CEII") must be a part of that reassessment. Within days after September 11, NERC blocked public access to information on its web site that related to critical aspects of the bulk electric

system. NERC adopted a policy of "reasonable access" to information, meaning that the information was no longer available to the general public but was available to participants in the electricity markets, as well as certain others, on a need-to-know basis. An individual could gain access to the information through use of a unique user identification and password. An individual could only obtain a user ID and password by being sponsored or vouched for by a responsible individual of an entity registered on the TSIN Registry.[1] Additionally, the individual must also complete a non-disclosure agreement stating that unwarranted disclosure of the information provided is prohibited.

NERC's Critical Infrastructure Protection Advisory Group ("CIPAG") has the mission of advancing the physical and cyber security of the electric infrastructure of North America. Its mission is accomplished through developing security standards, practices and guidelines as well as promoting, administering and evaluating their effectiveness. NERC CIPAG is supportive of the actions proposed in the Commission's CEII NOPR. The NERC CIPAG applauds the Commission's initiative and offers constructive suggestions on implementing the actions described in the CEII NOPR. Further, the NERC CIPAG supports the prior action taken by the Commission; these actions include:

a) October 11, 2001 decision to remove from easy public access certain documents containing CEII sensitive documents filed by utilities at FERC that had previously been public.
b) January 16, 2002 CEII Notice of Intent ("NOI") requesting responses on what changes, if any, should be made regarding general public access to CEII and FERC's September CEII NOPR.
c) September 5, 2002 CEII NOPR requesting final industry comments on restricting access.

[1] TSIN is the Transmission Services Information Network maintained by NERC as the central registry for entities doing business in the electricity markets. Registration on TSIN is a prerequisite for doing business on OASIS nodes and for tagging interchange transactions.

RECOMMENDATIONS

NERC CIPAG is committed to ensuring that electric grid operators and market participants have fair and non-preferential access to CEII as required for their market functions. To that purpose, NERC CIPAG did develop and the NERC Board of Trustees did release security guidelines[2] on protecting sensitive information, copy attached. Definitions regarding what information should be classified are provided in the guidelines. The development of the guidelines provided active discussions within the industry and assisted NERC CIPAG when discussing the Commission's NOPR. These guidelines, discussions and inputs from the NERC CIPAG members are the basis for NERC's recommendations.

CEII Classification Recommendations:

NERC CIPAG supports the Commission's statement that CEII classification be limited to critical facilities. NERC CIPAG also supports the Commission's statement that the CEII Coordinator, appointed by the Commission, will determine the CEII classification of information provided by a submitter. The NERC CIPAG does make the following recommendations regarding the classification process:

1. NERC recommends that the Commission make available to submitters, not the public, examples of the types of information that might be classified as CEII.
2. NERC recommends that the Commission redesign FERC forms such that CEII data might be restricted/isolated to an attachment as suggested in the NOPR. As such, a submitter would not have to classify the entire document as "Contains Privileged Information – Do Not Release" or "Contains Privileged Critical Energy Infrastructure Information-Do Not Release," only the attachment would be so classified.
3. NERC recommends that the submitter of CEII be given adequate opportunity to respond to any instance when the CEII Coordinator or other Commission members deems data not CEII despite a request for CEII treatment. The

submitters should be given an opportunity to provide additional evidence, or rationale, regarding why CEII classification should be retained.

4. NERC recommends that the submitter be given at least 30 days to respond to a determination by the Commission that it will release the submitter's CEII to a non-governmental requestor. The "at least five days" (Part 388.112 (d)) provided for in the NOPR represents an undue burden.
5. NERC supports the Commission's procedures defined in Part 388.133, (d)(3)(i) where it states that requestors must justify the need and intended use of CEII information and recommends that this Part be modified to explicitly require the execution of a non-disclosure agreement before any CEII information is released.
6. NERC supports proposed Part 388.113(d)(3)(iii), which requires that the submitter be notified when a non-governmental request for CEII data is received. NERC recommends that submitters be advised within five days of the receipt of that request.

Recommendations on CEII Location/Mapping Data:

As a general matter, NERC CIPAG believes that real-time operating data, information about the nature and location of critical facilities and assets, power system restoration plans, and assessment of vulnerabilities should not be made generally available to the public. The Commission's exclusion of the location information from CEII is understandable given the current state of handheld GPS equipment and the visible locations of much of the facilities of electric systems. What the NERC CIPAG asks is that the Commission restrict access by the general public to detailed network topology maps and the details of the interactions performed by Supervisory Control and Data Acquisition ("SCADA") and Energy Management Systems ("EMS").

7. NERC recommends that the CEII definition be expanded to include network topology maps, as well as the relationship and functions of SCADA and EMS between critical facilities.

[2] Security Guidelines for the Electricity Sector: Protecting Potentially Sensitive Information, NERC, June 14, 2002

8. NERC recommends that general public access be restricted to a need-to-know basis for existing network topology maps, as well as the relationship and functions of SCADA and EMS between critical facilities.

Recommendation on Non-Disclosure Agreement:

NERC CIPAG supports the use of a non-disclosure agreement when CEII is released to third parties. Within NERC, access to sensitive data is restricted to a need-to-know basis and as appropriate registration, certification, agreements and passwords are used.

9. NERC recommends that all releases of CEII include a non-disclosure statement that the data is confidential and provided on a need-to-know basis.
10. NERC recommends that when CEII is released to governmental agencies, or agents thereof, that it include a statement, unless a waiver is provided, that governmental agencies (agents) are bound by the same regulations restricting the use of confidential data.

Recommendations of Support for CEII Coordinator:

NERC CIPAG fully supports the establishment of a CEII Coordinator.

11. NERC recommends that the CEII Coordinator position created by the Commission be provided with defined standards for classification and release of CEII data. NERC extends an invitation for the CEII Coordinator to actively participate (as appropriate) as a Commission liaison representative to the NERC CIPAG.

NERC CIPAG is concerned that the Freedom of Information Act may limit the Commission's ability to protect sensitive data filed with the Commission. NERC CIPAG supports the Commission's opinion stated in the NOPR that CEII document release may be restricted to a need-to-know basis. If it should turn out that FOIA does inhibit the Commission's ability to restrict release of CEII, then NERC urges the Commission to seek a legislative solution to give it the ability to protect such information.

NERC will be pleased to work with the Commission to further define the nature of the information to be protected and effective measures for doing so.

If the Commission has any questions related to this filing, please contact the undersigned at the phone numbers and address indicated.

NORTH AMERICAN
ELECTRIC RELIABILITY COUNCIL
By:

David N. Cook
General Counsel
North American Electric Reliability Council
116-390 Village Boulevard
Princeton, New Jersey 08540-5731
Phone: (609) 452-8060
Fax (609) 452-9550
david.cook@nerc.net

Date: November 13, 2002

CERTIFICATE OF SERVICE

I certify that I have caused a copy of these comments to be mailed to each person on the service list for this docket.

David N. Cook

Security Guidelines for the Electricity Sector: Protecting Potentially Sensitive Information

NERC	*Guideline*
Guideline Title: Protecting Potentially Sensitive Information	**Status: 1.0**
Revision Date:	Effective Date: June 14, 2002

Purpose:

Critical infrastructure owners and operators should have an information security or confidentiality policy in place as an integral part of their business-level policies.

The policy should address the production, storage, transmission, and disposal of both physical and electronic information. The policy should define the hierarchical confidentiality classification framework (eg. Public, Market Participant Confidential, Company Confidential, Highly Confidential) as well as the authorization requirements and conditions to permit disclosure.

This guideline is intended to complement such a policy and should not be construed as a guide to formulating the entirety of such a policy.

Critical infrastructure owners and operators are encouraged to consider this guideline when deciding whether information should be made available to government agencies, third parties, or to the public in general. This guideline provides direction to electricity sector management and security personnel responsible for ensuring that potentially sensitive information regarding critical infrastructure is made available, only on a need-to-know basis (ie. only to the extent necessary to enable entities to execute their duties and responsibilities).

Applicability:

This guideline applies to all critical infrastructure owners and operators, and in particular, to personnel responsible for making information available to others outside their company or agency.

Guideline Statement:

Even prior to the September 11, 2001 terrorist attacks, critical infrastructure protection owners and operators expressed great concern that sensitive

information regarding their assets could be used by those intending to damage critical facilities, disrupt operations or harm individuals. Since September 11, that concern has required that companies and government agencies closely examine their policies regarding the release of information to outside parties.

Table of Contents:

Guideline Detail:

Applicability

Information can appear in many forms, including company reports, brochures and other promotional materials, Internet web sites, on-line documents, automated or personally conveyed information, public records, etc. In addition, each company has proprietary information, which it deems to be sensitive in nature and requires protection from inappropriate or inadvertent disclosure.

In this guideline, the term “sensitive information” refers to any information that could be used to select, or gain information about a potential critical infrastructure target by those intending to damage facilities, disrupt operations or harm individuals. The following questions will help identify potentially sensitive information.

- Has the information been cleared and authorized for appropriate release?
- Does the information contain details about critical operating facilities, systems or vulnerabilities?
- What impact could the information have if it inadvertently reached an unintended audience?
- Does the information provide details concerning physical or cyber security measures?
- Does the information contain personnel information such as biographical data, contact information, names, addresses, telephone numbers, etc.?

- How could someone intent on causing harm use the information to his or her advantage?

- What instructions should be given to legitimate users and recipients of sensitive information, (eg. electricity market participants, emergency response personnel, government) with regard to disseminating the information to other parties (eg. contractors, service providers, customers)?

- Could this information be dangerous if it were used in conjunction with other publicly available information?

- Could someone use the information to target personnel, facilities, or operations?

- Does the information increase the attractiveness of a critical infrastructure asset as a target?

Securing Sensitive Information

Companies should consider designating a single person or department as being responsible for reviewing all third party requests for sensitive information and, in particular, reviewing information placed in the public domain . That department will generally have to coordinate closely with the company's legal counsel.

In general, sensitive information should not be provided unless one of the following conditions is met:

1. A government agency is requesting the data and is specifically entitled to it pursuant to its regulatory or statutory authority. Although compelled to provide the information, companies should ask that the agency provide assurances that the information will be kept confidential.

2. A government agency is requesting the data without having specific regulatory authority but can provide a legitimate public safety basis for its request as well as assurances that appropriate safeguards can be provided for ensuring that the information is protected.

3. Third parties, such as energy companies, consultants working for such companies, developers, or others who can demonstrate a legitimate business need to have the information providing that they sign a nondisclosure agreement or other statement agreeing not to distribute the information outside their company or use it for any other purpose.

Responding to Disclosures of Sensitive Information

Companies should have in place processes to respond to disclosures of sensitive information to ensure that they are addressed promptly and appropriately. This process should include informing and involving senior management, market participants, government, regulators, law enforcement, the public and the media, as appropriate.

Training

Critical infrastructure owners and operators are encouraged to conduct ongoing employee awareness sessions to ensure that information is appropriately secured.

Examples of Potentially Sensitive Information

The following table identifies generic categories of information that, if it became available to those intending to do harm, could place critical infrastructure at greater risk from terrorist or other criminal attacks. Critical infrastructure owners and operators are encouraged to use these categories to identify potentially sensitive information relevant to their own critical assets. Such information should be limited to a need-to-know basis, and should not be made publicly available. The term “critical assets” includes the data, communications, energy and operational systems or structures necessary to maintain overall operations of the company.

Type of Information	***Examples***
Locations & Functions:	
Critical assets: function and physical location	• Major generating stations and switchyards • Black start facilities • Extra high voltage (>230 kV) stations • Locations and responsibilities of control and operating entities • Details of critical computer systems (eg. operational systems such as EMS, SCADA, digital control systems, their names and function, CAD/CAM facilities, network configuration and firewall schemes)
Network topology maps	• Ties between control areas, congestion points • GIS data of transmission networks and facilities, etc. • Hierarchical production or process control maps, charts or diagrams
Exposed/unprotected assets	• Bridge and over-surface assets
Unmanned assets	• SCADA-controlled assets • Remotely controlled assets

Hazardous materials	• Fuel, industrial chemicals or waste storage
Contingency facilities	• Emergency coordination centers • Emergency meeting points and stations
Assessments:	
Vulnerability or risk assessments	• Security assessments
Hypothetical impact assessments	• Hypothetical environmental impact assessments • Information that describes areas likely to be affected by a failure (eg. down-stream impact of dam breach)
Drills and exercises	• Detailed exercise scope and objectives • Operating procedures • Findings and lessons-learned
Facility limitations	• Storm or other high-risk limits • Grid constraints and congestion points • Natural hazard high-risk facilities • Single contingency risks
Location/function-specific ranked data	• Quantitative comparisons of assets
Operations:	
Real time operations data	• Real time MW and flows at critical grid locations or transfer points • Hourly forebay water elevations

Physical and cyber security plans	• Facility and information technology security capabilities and procedures
Heightened risk operating procedures	• Critical production processes • Contingency protection measures • Special protection schemes and their operation • Emergency control actions, procedures and status when responding to events • Details of response to NERC Alert Levels
Emergency response and business continuity plans	• Emergency response procedures (eg. steps to be taken at a specific facility) • Facility evacuation criteria • Power system restoration plans • Contingency procedures • Minutes of meetings regarding emergency planning processes and strategies • Post-incident audits or reviews and specific action plans
Interdependencies:	
Personnel information	• Critical operations or emergency personnel names, addresses, telephone numbers, contact information, etc.
Energy and water sources	• Regular or backup energy and water sources

Communications assets and procedures	• Critical communications processes and facilities • Key communications contacts and protocols
Transportation methods	• Key transportation routes for critical services or personnel
Key suppliers or customers	• Supply lines to critical facilities (military installations, hospitals, government facilities, etc.) • Critical key business process partners • Customer supply points • Number of retail customers served by a specific facility or portion of the infrastructure • Emergency and backup services • Information that could be used to identify customers and their critical infrastructure

Related Documents:

— Security Guidelines for the Electricity Sector: Guideline Overview

— Security Guidelines for the Electricity Sector:
- Vulnerability and Threat Assessment
- Threat Response
- Continuity of Business Processes
- Communications
- Physical Security
- Cyber Security
- Employment Background Screening

- *An Approach to Action for the Electricity Sector, Version 1*, NERC, June 2001, http://www.nerc.com
- *Threat Alert Levels and Physical Response Guidelines,* NERC, November 2001, http://www.nerc.com
- *Threat Alert Levels and Cyber Response Guidelines,* NERC, March 2002, http://www.nerc.com

Revision History:

Date	Version Number	Reason/Comments