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

THREAT ALERT SYSTEM
AND PHYSICAL RESPONSE GUIDELINES
FOR THE ELECTRICITY SECTOR

Definitions of Physical Threat Alert Levels

A Model for Developing Organization Specific Physical Threat Alert Level Response Plans

Version 2.0
October 08, 2002

Developed by
North American Electric Reliability Council (NERC)
Critical Infrastructure Protection Advisory Group

Approved by
NERC Board of Trustees

Goals

- Define Threat Alert Levels for all alerts issued by the NERC Electricity Sector Information Sharing and Analysis Center (ES-ISAC) in cooperation with the National Infrastructure Protection Center (NIPC) or other government agencies. These Threat Alert Levels and Physical Response Guidelines, however, do not apply to facilities regulated by the Nuclear Regulatory Commission.
- Provide guideline examples of security measures that electric utility organizations may consider taking, based on the Alerts issued.
- Ensure that the application of these electricity infrastructure Alert Levels are appropriate based upon the threat information received by the Electricity Sector Information Sharing and Analysis Center from government sources, Electricity Sector participants, and other ISACs.
- Ensure threat information from the Telecom, Oil/Gas, Information Technology, and other sectors is included, as appropriate, in the formulation of a Threat Alert.
- Note that Threat Alerts could be issued for a specific geographical area, such as "Specific Region Only," or "Specific City Only," or by category, such as "Specific Type of Facility."

Threat Alert Level Definitions

ES-Physical-Green (Low)

ES-Physical GREEN Applies when no known threat exists of terrorist activity or only a general concern exists about criminal activity, such as vandalism, which warrants only routine security procedures. Any security measures applied should be maintainable indefinitely and without adverse impact to facility operations. This level is equivalent to normal daily operations.

ES-Physical-Blue (Guarded)

ES-Physical BLUE Applies when a general threat exists of terrorist or increased criminal activity with no specific threat directed against the electric industry. Additional security measures are recommended, and they should be maintainable for an indefinite period of time with minimum impact on normal facility operations.

ES-Physical-Yellow (Elevated)

ES-Physical YELLOW Applies when a general threat exists of terrorist or criminal activity directed against the electric industry. Implementation of additional security measures is expected. Such measures are anticipated to last for an indefinite period of time.

ES-Physical-Orange (High)

ES-Physical ORANGE Applies when a credible threat exists of terrorist or criminal activity directed against the electric industry. Additional security measures have been implemented. Such measures may be anticipated to last for a defined period of time.

ES-Physical-Red (Severe)

ES-Physical-RED Applies when an incident occurs or credible intelligence information is received by the electric industry indicating a terrorist or criminal act against the electric industry is imminent or has occurred. This condition may apply as a result of an incident in North America outside of the Electricity Sector. Maximum security measures are

necessary. Implementation of such measures could cause hardship on personnel and seriously impact facility business and security activities.

Physical Response Guidelines for the Threat Alert Levels

The following are examples of physical security measures to be considered for each threat alert level. These examples are not an exhaustive or all-inclusive list of possible security measures. The intent is to help define the scope for measures each organization may implement for its specific Alert Level Response Plans, based on its very specific requirements. Not all measures are applicable to all organizations. An organization may decide to re-order the sequence of some measures it deems appropriate to its environment and responsibilities. It also is expected that most organizations may need to develop additional, specific security measures.

ES-Physical-Green (Low)

1. Normal security operating standards and procedures.
2. Occasional workforce awareness messages or tabletop exercises, as appropriate.
3. All Security, Threat, and Disaster Recovery Plans should be routinely reviewed and updated. Recommend an annual review as a minimum.

ES-Physical-Blue (Guarded)

4. Work force awareness messages to be alert to; unusual activities and whom to report such activities.
5. Review operational plans and procedures and ensure they are up-to-date, to include:
   A. Security, Threat, Disaster Recovery, and Fail-Over plans
   B. Other Operation Plans as appropriate, i.e., transmission control procedures
   C. Availability of additional security personnel
   D. Availability of medical emergency personnel
   E. Review all data and voice communications channels to assure operability, user familiarity, and backups function as designed
   F. Review fuel source requirements

ES-Physical-Yellow (Elevated)

6. Implement measures 1-5, if they have not already been implemented.
7. Ensure all gates, security doors, and security monitors are in working order and visitor, contractor, and employee access control are enforced.
8. Notify critical and on-call personnel.
9. Establish/assure communications with law enforcement agencies
10. Identify additional business/site specific measures as appropriate.

ES-Physical-Orange (High)

11. Implement measures 1-10, if they have not already been implemented.
12. Review need to revise plans in measure 3, based on current intelligence, and include additional instructions as appropriate to the Security/Threat Plans.
13. Place all critical and on-call personnel on alert, consider holding tabletop exercises.
14. Enforce safe zones around facilities per Security Plan.
15. Ensure all gates and security doors are locked and actively monitored either electronically or by “random walk-by procedures.”
16. Implement Enhanced screening procedures for:

A. Anyone entering the facility
B. All deliveries and packages

17. Contact and coordinate with fuel suppliers, as necessary.
18. Inspect site fuel storage and HAZ-MAT (hazardous material) facilities.
19. Increase liaison with law enforcement, medical emergency services, and other entities.
20. Coordinate critical facilities security with neighbors:
    A. Virtual neighbors such as other utility organizations
    B. Physical facility neighbors
21. Consider emergency utility operations procedures appropriate to available threat intelligence.
22. Media releases should be reviewed with Security/Alert Level Coordinator prior to release.
23. Review plan for returning to Threat Level-YELLOW, BLUE OR GREEN status.
24. Additional business/site specific measures as appropriate.

ES-Physical-Red (Severe)

25. Implement measures 1-24, if they have not already been implemented.
26. Send non-essential personnel home, per business/site specific procedures.
27. Stop all non-alert related tours and visitors.
28. Consider having medical emergency personnel on-site, if possible.
29. Continuously monitor or otherwise secure all entrances and critical service facilities, such as substations, etc. This step may include use of armed security personnel.
30. Stop all mail and package deliveries directly to site.
31. Inspect all vehicles entering site.
32. Ensure all on-site personnel are fully briefed on emergency procedures.
33. Establish frequent communications with all appropriate law enforcement agencies for two-way updates on threat status.
34. Review plan for returning to Threat Level-ORANGE, YELLOW, BLUE or GREEN status.
35. Additional business/site specific measures as appropriate.

THREAT ALERT SYSTEM AND CYBER RESPONSE GUIDELINES FOR THE ELECTRICITY SECTOR

Definitions of Cyber Threat Alert Levels

A Model for Developing Organization Specific Cyber Threat Alert Level Response Plans

Version 2.0
October 08, 2002

Developed By
North American Electric Reliability Council (NERC)
Critical Infrastructure Protection Advisory Group

Approved by
NERC Board of Trustees

Goals

- Define Information Systems and Services (Cyber) Threat Alert Levels issued by the NERC Electricity Sector Information Sharing and Analysis Center (ES-ISAC) in cooperation with the National Infrastructure Protection Center (NIPC) or other government agencies. These Alert Levels and Physical Response Guidelines, however, do not apply to facilities regulated by the Nuclear Regulatory Commission.
- Provide guideline examples of security measures that Electric Utility entities may consider taking, based on Cyber Alert Levels issued.
- Ensure that the electricity infrastructure Cyber Threat Alert Levels are consistent with the threat information received by the NERC from Government sources and other ISACs.
- Assure that threat information from the Telecom, Oil/Gas, Information Technology, and other Sectors is included as appropriate in the formulation of a Cyber Threat Alert Level.
- Note that Cyber Threat Alert Levels could be issued (for example) for a specific computer platform or a communications protocol or service, such as "Windows 2000" or "SCADA Communications."

Threat Alert Level Definitions

ES-Cyber-GREEN (Low)

ES-Cyber-GREEN condition applies when there is no known threat of cyber attack or only a general concern about hacker activity that warrants only routine security procedures. Any cyber security measures applied should be maintainable indefinitely and without adverse impact to business or expenses. This may be equivalent to normal daily conditions.

ES-Cyber-BLUE (Guarded)

ES-Cyber-BLUE condition applies when there is a general threat of increased cyber (hacker intrusions, viruses, etc.) activity with no specific threat directed toward the electric industry. Additional cyber security measures may be necessary, and if initiated they should be maintainable for an indefinite period of time with minimum impact on normal business or expenses.

ES-Cyber-YELLOW (Elevated)

ES-Cyber-YELLOW condition applies when a general threat exists of disruptive cyber activity is directed against the electric industry. Implementation of additional cyber security measures is expected. Such measures are anticipated to last for an indefinite period of time.

ES-Cyber-ORANGE (High)

ES-Cyber-ORANGE condition applies when a credible threat exists of disruptive cyber activity directed against the electric industry. Additional cyber security measures have been implemented. Business entities need to be aware that corporate resources will be required above and beyond those required for normal business or expenses.

ES-Cyber-RED (Severe)

ES-Cyber-RED Condition applies when an incident occurs or credible intelligence information is received by the electric industry indicating a disruptive cyber attack

against the electric industry is imminent or has occurred. This condition may apply as a result of an incident in North America outside of the Electricity Sector. Maximum cyber security measures are necessary. Implementation of such measures could cause hardship on personnel and seriously impact facility business and security activities.

Cyber Response Guidelines for the Threat Alert Levels

The following are examples of security measures to be considered at each cyber threat level. This is not an exhaustive or all-inclusive list of possible security measures. The intent is to provide a scope of measures that each organization may implement for their specific threat response plan, based upon their own specific requirements. Not all measures are applicable to all organizations. Some organizations may decide to re-order the sequence of some measures, as they perceive appropriate to their environment and responsibilities. It is also expected that most organizations may perceive the need to develop additional, specific security measures to meet their requirements.

It is also recognized that some measures might not always be necessary or applicable against a particular threat. Therefore, when developing your specific response plan, it is recommended you do so with consideration as a checklist of all the possible security measures you might choose to initiate, based on the specific threat information available.

ES-Cyber-Green (Low)

1. Have an emergency plan for IT operations:
   A. Ensure all business critical information and information systems (including applications and databases) and their operational importance are identified.
   B. Ensure all points of access and their operational necessity are identified.
2. On a continuing basis, conduct normal security practices. For example:
   A. Conduct education and training for users, administrators, and management.
   B. Ensure an effective password management program is in place.
   C. Conduct periodic internal security reviews and external vulnerability assessments.
   D. Conduct normal auditing, review, and file back-up procedures.
   E. Ensure effective virus protection scanning processes are in place.
   F. Confirm the existence of newly identified vulnerabilities and test and install patches as available.
   G. Periodically review and test higher Threat Alert Level actions and IT recovery plans.
3. Maintain law enforcement liaison-e.g. local FBI, InfraGard, RCMP

ES-Cyber-Blue (Guarded)

4. Implement measures 1-3 if not already implemented.
5. Communicate work force awareness messages to be alert and who to report unusual cyber activities to.
6. Review security and operational plans and procedures and ensure they are up-to-date.

ES-Cyber-Yellow (Elevated)

7. Implement measures 1-6 if not already implemented.
8. Increase level of auditing, review, and critical file back-up procedures.
9. Conduct internal security review on all critical systems.
10. Increase review of intrusion detection and firewall logs.

11. More frequent checks of cyber security communications for software vulnerability.
12. Identify additional business/site specific measures as appropriate.
13. Increase frequency of measure 3 – include additional instructions as appropriate to your Cyber Alert Level Response Plan.

ES-Cyber-Orange (High)

14. Implement measures 1-13, if not already implemented.
15. Conduct immediate internal security review on all critical systems.
16. Determine staffing availability for backup operations and provide notice.
17. Consider increasing physical access restrictions to computer rooms, communications closets, and critical operations areas.
18. Consider account access restrictions-temporarily disable non-critical accounts.
19. Consider delaying scheduled, routine maintenance or non-security sensitive upgrades.
20. Media releases should be reviewed with Cyber Alert Level Coordinator prior to release.
21. Review plan for returning to Alert Advisory Level-Yellow, Blue or Green.
22. Additional business/site specific measures as appropriate.

ES-Cyber-Red (Severe)

23. Implement measures 1-22, if not already implemented.
24. Consider 7/24 emergency tech support staffing.
25. Consider continuous 7/24 monitoring of intrusion detection and firewall logs.
26. Consider continuous 7/24 monitoring of cyber security communications for latest vulnerability information. Contact software vendors for status of software patches and updates.
27. Consider reconfiguring information systems to minimize access points and increase security.
28. Consider rerouting mission-critical communications through unaffected system.
29. Consider disconnecting non-essential network access.
30. Consider alternative modes of communication and disseminate new contact information, as appropriate.
31. Consider activation of the company emergency management team/procedures.
32. Actively monitor communications with all appropriate law enforcement and cyber security agencies for two-way updates on threat status.
33. Review plan for returning to Advisory Alert Level- Orange, Yellow, Blue and Green.
34. Additional business/site specific measures as appropriate.