IN THE
UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF HOMELAND SECURITY

Procedures for Handling Critical Infrastructure Information
6 C.F.R. Part 29
RIN 1601—AA14

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL ON INTERIM RULE

The North American Electric Reliability Council ("NERC")[1] strongly supports the Interim Rule on the handling of critical infrastructure information ("CII") issued by the Department of Homeland Security ("DHS") on February 20, 2004,[2] and appreciates this opportunity to provide further comment. NERC actively supports the activities of DHS and has been designated by DHS as both the operator of the Electricity Sector Information Sharing and Analysis Center ("ESISAC") [3] and the Sector Coordinator to set the policies for the operation of the ESISAC. In this effort, NERC is guided through our liaison relationship with the Department of Energy. Further, NERC and the ESISAC have a working relationship with all electric industry stakeholders through NERC's Critical Infrastructure Protection Committee ("CIPC"). [4] Industry stakeholders reviewed the Interim Rule and discussed it at several industry CIPC forums; these comments are the results of those discussions. NERC endorses these comments, and any subsequent discussions regarding them should be directed to NERC.

---

[1] NERC is a not-for-profit corporation formed in response to the Northeast blackout in 1965 to promote the reliability of the bulk electric system that serves North America. NERC's mission is to ensure that the bulk electric system in North America is reliable, adequate, and secure. 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 for the reliable operation and adequacy of supply of these systems, as well as to protect the security of the interconnected systems. NERC comprises ten Regional Reliability Councils that account for virtually all he electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

[2] 69 Fed. Reg. 8074 (February 20, 2004); 6 C.F.R. Part 29.

[3] A review of the functions and services provided by the ESISAC can be found at: http://www.esisac.com.

[4] A description of the membership and function of the CIPC can be found at: http://www.nerc.com/~filez/cip.html .

NERC believes the Interim Rule matches closely the intent, spirit, and letter of the Critical Infrastructure Information Act of 2002. NERC supports the goal of the Interim Rule — to increase the level of information sharing between the public and private sectors — and believes the Act and the Interim Rule are a necessary first step in meeting this goal. This is an important first step and DHS is applauded for its initiative. It is hoped that any efforts to expand this Interim Rule will be done in a truly cooperative public-private effort. Participation in the use and application of these regulations will benefit from a cooperative effort as DHS and the private sector work together to balance the need to share critical infrastructure information and the need to protect it.

In the following section, NERC describes four areas that the electric sector is encouraged to see in the CII Interim Rule. Later sections raise two areas that are of significant concern, several areas that DHS should review regarding how the CII Program will be administered, and areas where clarification is needed.

Areas of Support for Interim Rule

A. *Section 29.2 Critical Infrastructure Information Progra.* NERC welcomes the creation of a single office within DHS that will coordinate the designation of CII. The creation of this office will allow DHS to focus the responsibilities for coordinating a program that has the potential to affect multiple federal agencies, state and local government organizations, and foreign governments. It will allow for a single public-private relationship that will assure the uniform application and interpretation of the CII Interim Rule. NERC does caution that the channeling of the CII submittals through a single office has the potential to delay the information going to the appropriate offices in DHS and elsewhere. NERC recommends that DHS monitor the operation of the CII Program and take actions to eliminate any delays.

B. *Section 29.6(b) Presumption of Protection.* NERC supports the language that presumes that submitted information is protected. Having this presumption is necessary to encourage companies to share information.

C. *Section 29.8 Disclosure of Protected Critical Infrastructure Information.* NERC supports the language that sets conditions on when protected information is shared with state and local

governments, as well as federal contractors, and that limits the use of the information. In addition, NERC supports the protections of subsection (g) (1), which states that protected information shared by the Program Manager or designee with state and local governments must be protected from disclosure under state FOIA laws. NERC recommends that DHS quickly initiate the creation of the legal mechanisms to allow it to share CII submittals with other federal agencies and state and local organizations in a manner, or with such protections, so as to ensure that CII will remain confidential.

D. *Section 29.8(i) Restrictions on Use of Protected CII in Civil Actions.* NERC supports the protections granted in this section. Companies that voluntarily share their critical, sensitive data to enhance homeland security should be free to do so without fear that the information they share will be used against them in civil actions. Without this protection, companies will not participate.

While recognizing the positive aspects of the Interim Rule, NERC must also raise several areas that are of significant concern, require administrative review, or need clarification.

Areas of Significant Concern

(1) One significant concern can affect the operational value of the public-private relationship as defined in Homeland Security Presidential Directive/HSPD 7, its predecessor Presidential Decision Directive 63, as well as the benefits intended by the creation of the ISACs. That concern is the limitation on transfers of infrastructure information regarding security incidents occurring at the 85% of the critical infrastructures operated by the private sector. NERC's significant concern is that the CII Interim Rule and the operation of the CII Program will discourage the private sector from continuing to provide DHS with CII directly and rapidly through such time-sensitive programs and offices as the Indications, Analysis, and Warnings ("IAW") program and the National Infrastructure Coordination Center ("NICC"). As the rule is currently written, CII can only acquire protected status when it is submitted to the Protected CII Program Office. Programs and offices such as IAW and NICC can effectively function only when they are provided information on a rapid, "as-occurring" basis. They cannot afford to wait for the CII Program Office to receive information, make CII determinations, etc., and then transmit the information to them. This concern extends to both written documents and oral

communications to facilitate rapid transfer of information to DHS during an incident (see NERC's comment to Section 29.5 (a) (3)(ii) below). Thus, the regulations should specify that CII material will be afforded protected status when provided to DHS through any such time-sensitive program or office. The regulations could be written to specify by name each such eligible program or office, especially the programs or offices to which the ESISAC can directly submit CII for the electricity sector. In addition, the regulations should specify a mechanism for said programs and offices to convey that CII material to the CII Program for further appropriate handling.

(2) In addition, the Interim Rule as worded gives the impression that all the previously submitted CII, using IAW (or similar programs), will not be given Protected CII status, even though at least some was submitted specifically pursuant to assurances that it would be so protected. In order to further assure the private sector that CII will be completely afforded all available protections, and thus encourage the private sector to continue providing CII to DHS, the regulations must clarify that information already provided to DHS pursuant to a written or verbal assurance of confidentiality under the CII Act and other applicable provisions, even though submitted prior to the inception of the CII Program established in the interim regulations, will be fully afforded status as Protected CII, as provided by the Critical Infrastructure Information Act of 2002.

Areas of Administrative Concern

(3) *Section 29.4(e) Protected Critical Infrastructure Information Management System ("PCIIMS").* This section states that an electronic tracking system will be developed to track submitted information. NERC recommends that this section be clarified to state that the actual protected information itself will not be part of this system or electronically retrievable by PCIIMS. Associated with PCIIMS should be a mechanism where a submitter may track the subsequent distribution of each of the Protected CII it submitted to DHS, including the ability to receive automatic email notifications when its documents are released from one office, agency, or contractor to another. Such a system would allow a submitter to be aware of the current distribution of any Protected CII documents it submitted. At the very least, this tracking system should record the distribution and return of Protected CII documents to offices within DHS, as

well as to outside agencies and contractors. It would also be reasonable for such a system to include a brief statement as to the purpose, or justification, for distributing the documents.

(4) *Section 29.5 (a)(3)(ii) Requirements for Protection.* This section states that in cases of oral submissions, a submitter has 15 days to request CII classification. It is impossible for DHS to know, during those 15 days, whether the submitter is going to request that the data be CII classified. Therefore, NERC recommends that this section be changed to require the request for CII protection to be made at the time of submittal and followed-up by the submitter in 15 days with written confirmation. Additionally, during ongoing incidents, it can be expected that the federal government and the private sector will be in near-constant communication. As such, it is unrealistic for either to keep appropriate records regarding request/approval of a CII classification. During an ongoing, or active, incident, NERC recommends that Protected CII status be assigned once and maintained throughout the incident. The closure of the Protected CII incident should be mutually agreed upon by the reporting entity and DHS. After the conclusion of the incident, any CII-related documents concerning the incident's investigation or restoration periods would be submitted to DHS and independently subject to CII classification review and approval.

(5) *Section 29.6(d)(1) Acknowledgement of Receipt of Information.* This section of the Interim Rule states that the CII Program has 30 days in which to classify the CII submittal and to notify the submitter of any decision. Given the importance of the timely classification and possible need for further distribution of the submittal, consideration should be given to reducing the length of this time period to 10-15 days.

(6) *Section 29.6 (d)(3) Acknowledgement of Receipt of Information.* This section states that submitters will be given a tracking number so they can review the status of their CII request. This raises two questions: 1) will the PCIIMS be a public database; and 2) can a reviewer check the status of another submitter? NERC recommends that this section make clear that PCIIMS is not a public database and that a reviewer cannot check the status of another submitter.

(7) *Section 29.6(e)(2)(E)(ii) Acknowledgement of Receipt, Validation, and Marking.* This section concerns the use of submitted information that is determined to not meet the protected requirements. NERC supports the language that provides the submitter with the option of having the information destroyed or held by DHS without protection. However, NERC is concerned with the language that enables the Program Manager to override the choice of the submitter. Under this section, the Program Manager can independently determine that the information is of law enforcement importance, not destroy it, and share it with law enforcement, without informing the submitter. NERC requests that the discretion granted to the Program Manager under this provision be deleted. At the very least, NERC requests clarification as to how the Program Manager is to determine how such information might have law enforcement value and require the Program Manager to immediately notify the submitter that the information was shared with law enforcement and not destroyed.

(8) *Section 29.7(b) Use and Storage.* This section of the CII Interim Rule states that "reasonable steps" shall be taken to secure protected information and that it shall be stored "in a secure environment that affords it the protection commensurate with its vulnerability and sensitivity." This appears to permit the Program Manager to provide tiered levels of security measures and permits the Program Manager to decide which data is the most sensitive data. NERC's view is that all Protected CII should be stored in the same secure manner and that the rule should provide further guidance to the Program Manager as to what methods are appropriate for securing the information.

(9) *Section 29.7(d) Disposal of Information.* This section should clarify that the information will be disposed of in accordance with the Federal Records Act. This will ensure consistency with Section 29.6 (e)(2)(E), which states that information must be disposed of in accordance with the Federal Records Act.

(10) *Section 29.7(e) Transmission of Information.* We recommend that this section be changed to state that the Program Manager or designee will use only secret or encrypted communication protocols to transmit Protected CII documents.

(11) *Section 29.8(d) Further Use or Disclosure of Information by State and Local Governments.* An additional concern not specifically addressed in the Interim Rule is the process that DHS will utilize to assure that Protected CII documents released to state agencies during an incident are controlled. Descriptions of the measures that must be taken have only been addressed at the highest-level in the Interim Rule. Further explanations of the mechanisms DHS expects to put into place need to be provided.

(12) *Section 29.8(j) Disclosure to Foreign Governments.* This section states that Protected CII documents can be disclosed to foreign governments without the written consent of the submitter. Nothing in the Homeland Security Act or the Critical Infrastructure Information Act authorizes releases of CII to foreign governments, and there are obvious problems with such releases created by the differences among the world's legal systems. Therefore, NERC requests that this section be deleted in its entirety, or at least reworded to clarify that only "warnings" based on CII, but not actually including any CII itself, are covered, as contemplated under Sections 214(g) and 214(e)(2)(D) of the Homeland Security Act.

(13) *Section 29.9 (c) Notification to Originator of Protected CII.* This section states that the Program Manager will notify the submitter if information is lost or an unauthorized access has occurred. NERC recommends that this section be changed so that the submitter is notified every time there is a disclosure of Protected CII documents, including to law enforcement.

Areas Where Clarification Is Needed

(14) *Section 29.2 Definitions.* The last sentence of the PCII definition states that the PCII Program Manager can "render a final decision that the information is not Protected CII." A clarification should be added that the information would remain protected until the submitter responds to the designation, assigned by DHS, of the information's status as described in Part 29.6 (e).

(15) *Section 29.2 Definitions.* The CII Interim Rule should be clarified regarding the capabilities of the various ISACs to make CII submittals on behalf of their sector participants.

(16) *Section 29.4 (b)(4) CII Program Administration.* The CII Interim Rule notes that for the CII Program staff training materials will be developed to assure a uniform interpretation and application of the regulations. To the extent appropriate, similar training materials should be made available to the private sector participants to assure that they understand both the nature of information that should be protected and the process for submitting such to DHS.

(17) *Section 29.4(d)(3) – PCIIMS.* This section notes that periodically the operation and performance of the CII Program will be reviewed and an assessment made. Who will be responsible for this review and will the assessments be public? Given the importance of the relationships to be developed through the CII Program, NERC recommends that any assessment team include private sector representation and that a summary of any assessments be publicly available. Additionally, such assessments should include easily understandable metrics to measure the performance of the CII Program that include the number of CII submittals requested and an overview of how they were administered.

Finally, NERC would encourage further efforts on two matters mentioned in the preamble to the Interim Rule but not specifically addressed in the Interim Rule, (i) the additional exploration of how to facilitate protection of indirect submittals through other federal agencies (e.g., the Federal Communications Commission), and (ii) how to address potential overlap with rules of other federal agencies (e.g., the Federal Energy Regulatory Commission ("FERC")), or offices within DHS (e.g., the Transportation Security Administration ("TSA") or the United States Coast Guard ("USCG")), that also protect sensitive infrastructure-related information.

As to the first matter, Section 29.5 of the Interim Rule acknowledges, but does not define, a future mechanism for "indirect" submittals of CII to DHS "through" other federal agencies, while the designation of Protected CII status would remain the responsibility of the DHS. NERC believes the future ability to submit critical infrastructure information directly to other agencies, to be beneficial and supportive of the intentions of the Homeland Security Act, Section 214(e)(2)(A), requiring that mechanisms be established to allow indirect submittal of critical infrastructure information. This mechanism also conforms to, and thoughtfully clarifies, the Act's

somewhat oblique reference at Section 212(4) to "any" agency head designating the critical infrastructure protection program of "a," rather than "the," covered agency to receive critical infrastructure information (once that program has itself been designated "as" such a program pursuant to Section 213). NERC encourages the development of these mechanisms and looks forward to their adoption.

Regarding the second matter, DHS could clarify that otherwise protected information (such as Security Sensitive Information ("SSI") designated by TSA or USCG, or Critical Energy Infrastructure Information ("CEII") designated by FERC) will remain subject to those protections when obtained and used by DHS for critical infrastructure protection purposes, see 44 U.S. Code Section 3510(b).

NERC appreciates the opportunity to comment on this important subject. NERC would be pleased to provide you further comments or clarifications upon request.

NORTH AMERICAN ELECTRIC
RELIABILITY COUNCIL

David N. Cook
Vice President and General Counsel
116-390 Village Boulevard
Princeton, New Jersey 08540-5731
(609) 452-8060
david.cook@nerc.net