

National Association of Regulatory Utility Commissioners.txt

Subject: RIN1601-AA14: NOPR on Procedures for Handling Critical Infrastructure Information -- Comments of NARUC

Date: Mon, 16 Jun 2003 16:08:00 -0400

From: "Sharla Barklind" <SBarklind@naruc.org>

To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Attached, please find the Comments of the National Association of Regulatory Utility Commissioners (NARUC) on the Public Notice of Proposed Rulemaking on Procedures for Handling Critical Infrastructure Information. Copies of these comments have also been sent by regular mail.

Should you have any questions or need additional information, please do not hesitate to contact me at 202-898-1350 or sbarklind@naruc.org .

<<03 06 16 NARUC DHS.FIN1.doc>>

<<061603 Critical Infra. filing -DHS-.pdf>>

Sharla M. Barklind
Assistant General Counsel
National Association of Regulatory Utility Commissioners
1101 Vermont Ave., NW, Suite 200
Washington, DC 20005
202-898-1350
sbarklind@naruc.org

PLEASE NOTE: This message and any attachments may be protected by the attorney-client privilege, work product doctrine or other legal privilege. If you are not the intended recipient or have received this message in error, please notify the sender and promptly delete the message. Thanks for your assistance.

03 06 16 NARUC DHS.FIN1.doc
Name: 03 06 16 NARUC DHS.FIN1.doc
Type: WINWORD File
(application/msword)
Encoding: base64
Description: 03 06 16 NARUC DHS.FIN1.doc

061603 Critical Infra. filing -DHS-.pdf
Name: 061603 Critical
Infra. filing
-DHS-.pdf
Type: Acrobat
(application/pdf)
Encoding: base64
Description: 061603 Critical
Infra. filing
-DHS-.pdf

**UNITED STATES OF AMERICA
DEPARTMENT OF HOMELAND SECURITY
WASHINGTON, D.C.**

<i>Proposed Rule on</i>)	
<i>Procedures for Handling</i>)	
<i>Critical Infrastructure Information</i>)	
)	
6 CFR Part 29)	
		RIN 1601-AA14 (April 15, 2003)

**INITIAL COMMENTS OF THE
NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS**

The National Association of Regulatory Utility Commissioners (“NARUC”) respectfully files these comments in response to the “Public Notice of Proposed Rulemaking” (“Notice” or “NOPR”) published by the Department of Homeland Security (“DHS”) at 68 Federal Register 18524 (published on April 15, 2003) to examine “Procedures for Handling Critical Infrastructure Information” (“CII”). NARUC commends DHS for acting swiftly after DHS’ creation to enact a rule to address issues that touch on the proper balances between secrecy and openness in government and between State and Federal authority and responsibility in utility regulation. As described in more detail below, NARUC believes DHS should provide some additional clarifications of its rules to limit the prospect for duplicative reviews before information is released and to assure State and Federal agencies retain the access they need to continue to fulfill their statutory mandates efficiently.

In support of its positions, NARUC respectfully submits the following:

I. INTRODUCTION

NARUC represents the governmental agencies of the fifty States, the District of Columbia, Puerto Rico and the Virgin Islands engaged in the regulation of public utilities and common carriers. NARUC's mission is to serve the public interest by improving the quality and

effectiveness of public utility regulation. NARUC's member commissions have the obligation under State law to ensure the establishment and maintenance of such utility services as may be required by the public convenience and necessity, and to ensure that such services are provided at rates and conditions that are just, reasonable and nondiscriminatory for all consumers.

NARUC, which Congress calls "the national organization of the State commissions", 47 U.S.C.A. § 410(c) (1971), presents the collective interest of State commissions charged with regulating conditions of service of the intrastate operations of electric, natural gas and telephone utilities. Both Congress and the Federal courts have long recognized that NARUC is a proper party to represent the collective interest of State regulatory commissions. *See, e.g., United States of America v. Southern Motor Carrier Rate Conference, et al.*, 467 F.Supp. 471 (N.D. Ga. 1979), *aff.* 672 F.2d 469 (5th Cir. Unit "B" 1982); *aff. en banc*, 702 F.2d 532 (5th Cir. Unit "B" 1983, *rev'd*, 471 U.S. 48 (1985). *See also, Indianapolis Power and Light Co. v. Interstate Commerce Commission*, 587 F.2d 1098 (7th Cir. 1982); *Washington Utilities and Transportation Commission v. FCC*, 513 F.2d 1142 (9th Cir. 1976).

During the last two years, many of NARUC's member commissions have been reviewing State policies and procedures regarding the public availability of CII within their own commissions and States, and developing policies to ensure protection of CII. The successful completion of these protective policies, NARUC respectfully suggests, is itself an essential building block of Homeland Security. Accordingly, NARUC's member commissions have a profound and direct interest in the terms and conditions of the availability of CII to public agencies such as State Commissions.

The entities regulated by State Commissions -- including the nation's gas, electric, water, wastewater and telecommunications utilities -- own and operate a central and substantial portion of the nation's Critical Infrastructure (CI). To fulfill their obligations, State Commissions have

historically relied on facility owners and operators to provide them with high quality and highly detailed information on the nation's utility infrastructure. The complete and timely provision of this information is essential. Pursuant to the Nation's tradition of public utility regulation, much of the work done by Commissions is in the public view. State Commissions are keenly aware that recent events compel immediate reflection on, and appropriate revision of, longstanding rules governing access to information regarding utility industry infrastructure. We have an obvious interest in working with DHS to assure that needed restrictions:

1. Protect, to the extent feasible, the ability of State Commissions to obtain information needed to fulfill their regulatory mandate;

2. Recognize that State Commissions are agencies with a "need to know" in regard to CII related to State Commission obligations;

3. Recognize that State Commissions' fulfillment of their longstanding obligations to ensure the safe, reliable, and efficient provision of utility services is itself an important element of Homeland Security protection;

4. Are crafted in a manner that minimizes unneeded red tape and delay.

NARUC commends DHS for acting swiftly after DHS' creation to enact a rule to address issues that touch on the proper balances between secrecy and openness in government and between State and Federal authority and responsibility in utility regulation. In the spirit of shared national effort to address and resolve these issues, we offer these comments from their perspectives as lawfully constituted regulators of a substantial portion of the nation's critical infrastructure.

II. DISCUSSION

In summary, State Commissions have the following comments:

1. *DHS seeks uniformity among agencies but does not address the potential conflicts between its rule and the rule(s) issued by other agencies.*

The DHS rule proposes to establish a “uniform” rule to govern Federal agencies who receive CII. DHS does not, however, consider the relation between its terms and those already imposed on CII by rule(s) promulgated by other Federal agencies. For example, the Federal Energy Regulatory Commission (“FERC”) has recently enacted a rule to protect Critical Energy Infrastructure Information (“CEII”).¹ Also, the *Bioterrorism Preparedness Act of 2001* requires vulnerability assessments to be submitted to the U.S. EPA.²

On its face, the definition of CII provided in DHS’s rule appears to be in substantial conflict with the definition provided in the FERC CEII rule. CII, as defined by DHS, is limited to information “not customarily in the public domain.” However, the FERC, as the expert regulator of the energy utility industry, recognized that much utility infrastructure information *has* customarily been in the public domain. The FERC rule appears, therefore, to protect energy information even where it *has* customarily been in the public domain. State Commissions appreciate that the “not customarily” test contained in the DHS rule is that established in the Homeland Security Act itself, at Section 212 (3). Nonetheless, DHS should, with particular regard to regulated utility infrastructure clarify the impact of its regulations on other agencies’

¹ Order No. 630, Critical Energy Infrastructure Information, 102 FERC para. 61, 190 (Feb. 21, 2003)(codified at 18 C.F.R. secs 373.312, 388.112, 388.113).

² 107 P.L. 188; 116 Stat. 594; 2002 Enacted H.R. 3448; 107 Enacted H.R. 3448, PUBLIC LAW 107-188 [H.R. 3448], JUN. 12, 2002, PUBLIC HEALTH SECURITY AND BIOTERRORISM PREPAREDNESS AND RESPONSE ACT OF 2002, UNITED STATES PUBLIC LAWS 107th Congress -- 2nd Session.

rules and any resulting need for consistent treatment.³ DHS should also address any other relevant distinctions between the DHS and the FERC/other federal agency rules, including (1) how DHS's finding on information protection should be coordinated with an expert regulatory agency's treatment of the relevant information, e.g., if an expert agency (FERC, FCC, EPA, etc) makes findings, whether DHS officials are required to make related determinations of the customary treatment of information, and, if so, how; and (2) whether utility infrastructure information that, as an expert regulatory agency has found, has historically been in the public domain, may somehow nonetheless qualify as CII.

As suggested by these requested clarifications, the DHS proposal does not clearly address how the CII review mechanisms it provides will relate to similar mechanisms created by other agencies. For example, the review mechanisms contained in DHS' rule appear to parallel procedures contained in the FERC CEII rule, although they appear to protect distinguishable data sets. NARUC believes it would be wasteful and counterproductive for the DHS rules to result in multiple reviews by more than one federal agency that would delay access to CII data by State Commissions, and other government bodies with a bona fide need for timely access. NARUC therefore requests that DHS review and clarify the relation of the DHS procedures with similar procedures created by other agencies for the same data, and determine whether multiple reviews are needed to validate the CII status of, and provide for restricted release of, the same information.⁴ Also, access to water company vulnerability assessment is strictly limited; this should be taken into account.

³ For example, FERC's rules appear to address only information submitted in compliance with regulatory mandates. That would appear in most, if not all, instances to insulate that data from the application of DHS's proposed rules. The DHS should clarify if that is the case and, correspondingly, if that eliminates the need for consistency between the DHS and FERC rule approaches.

⁴ Indeed, some distinctions are *implied* by the definition of voluntary in § 29.2 (j) of the proposed rule require additional clarification. For example, this section says information that is supplied voluntarily "...does not include information submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings." This definition can be read to effectively prevent the application of the DHS rules to the majority of CI information provided to the FERC, the FCC, EPA, or other federal agencies during the regular course of their proceedings. If that is the intended reading, some additional clarifications either in the text of the rule or in the order approving the rule would be helpful.

2. The definition of “voluntarily” provided information requires clarification in relation to information provided to agencies other than DHS.

As required by the Homeland Security Act, DHS’ proposed rule recognizes that CII is limited to “voluntarily” provided information. The test for “voluntariness” is whether the data was provided voluntarily to DHS itself. However, the method for determining whether information is provided voluntarily is not clear where information is first provided to an agency other than DHS. The proposed rules suggest agencies cannot “voluntarily” forward this information unless the company providing the information grants written permission.

3. The terms of the proposed rule may be read in a manner that impairs the ability of State Commissions to perform their statutory functions, and the rule should be clarified to prevent such misreading

The DHS rule provides, as required by the Homeland Security Act, that State agencies’ existing rights to collect data directly from regulated entities will remain unimpaired. However, in today’s world of networked and interconnected utility services, State Commissions routinely rely on Federal agencies to provide data -- such as that related to the operation of regional transmission networks -- emanating from utilities beyond individual State jurisdictions.

In this setting, the proposed rule:

(1) provides that DHS “may” withhold CII from State agencies, without any further guidelines that limit discretion to withhold needed data from State Commissions. State Commissions respectfully request that the rule should make clear that State Commissions have a presumptive need to know to obtain data relevant to their missions.

In short, the rule should be clarified to provide that CII “should” (and not “may”) be made available as long as non-disclosure requirements can be assured;

(2) may be read to limit State Commissions’ use of CII data to purposes related to the prevention of terrorist attacks on facilities. The rule should make clear that the protection of Homeland Security requires that State Commissions not be barred (subject to non-disclosure requirements) from using data to fulfill the breadth of their mission.

III. On Behalf of the Requirement for Uniformity, DHS Should Address the Relation of Its Definition of CII and its Review Mechanisms for CII to Those Provided by Other Agencies

The DHS proposed rule:

establishes uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Federal Government by the public. These procedures apply to all Federal agencies that receive, care for, or store CII that is voluntarily submitted to the Federal Government pursuant to the CII Act of 2002. 6 U.S.C. 130, *et seq.*

However, in seeking to establish uniform rules for all Federal agency CII, DHS does not acknowledge the existence of preexisting rules governing the same or similar data. It therefore, does not consider the relation of the proposed rule to those that already exist. Indeed, as referenced earlier, § 29.2 (j) of the proposed rule can be read to effectively prevent the application of the DHS rules to the majority of CII provided to the FERC, the FCC, EPA, or other federal agencies during the regular course of their proceedings. If this is DHS’ intention, then it would be helpful to state that more clearly in the rule text.

A. DHS Must Consider and Clarify the Relation Between the “Not Customarily in the Public Domain” Requirement for CII and the Findings of FERC’s CEII Rule in Regard to Electric and Natural Gas Utility Infrastructure Data.

With regard to the scope of the information that is to be protected as CII, DHS states, at 29.2(b):

Critical Infrastructure Information or CII means *information not customarily in the public domain* and related to the security of critical infrastructure or protected systems... (emphasis added).

Because of the historic nature of public utility regulation, a great amount, perhaps the preponderance, of information related to regulated electric, gas, water, wastewater and telecommunications utilities (and further “regulated” utilities) has “customarily” been “in the public domain.” In issuing its (“CEII”) rule, the FERC explained that because this is the case, the test of whether information has customarily been in the public domain is one that *it will not* apply to CEII. In its examination of the reach of Freedom of Information Act (FOIA) exemption for “commercial information”, FERC explained that if the test were solely whether CEII data has been previously available, FERC could not now withhold it. FERC explained that changed circumstances regarding customarily available CEII data (including those related to the deregulation of the utility industry as well as recent Homeland Security concerns) can be a basis for FERC’s determination that information should be protected even where, if the test were its customary status, protection would not be in order. DHS’s independent statutory provision for protecting CII information and the express exemption from FOIA provisions for “protected information” seem to raise additional questions about the same information provided to both DHS and other agencies.

The proposed DHS rule, at Section 29.6 (e) provides that the DHS CII Program Manager shall be responsible for reviewing all submissions to “validate the satisfaction of the definition of CII as established by the law.” Section 29.6 (e) further provides that in making the “initial validation determination, the Program Manager shall give deference to the submitter’s expectation that the information qualifies for protection.”

With great respect, given the great potential amount of claimed CII, it is not clear that the Program Manager will, at least at the onset, have sufficient expertise and experience to make the determination in his/her own right. In these circumstances deference to the submitter without required check from independent sources may not serve the public interest. While a public utility submitter may state that information has not customarily been in the public domain, the relevant agencies, the FCC, FERC, EPA, and State Commissions should nonetheless also be consulted.

In short, with regard to CII relating to infrastructure owned or operated by regulated utilities, it is requested that DHS clarify:

(1) whether DHS will defer to determinations as to whether information has customarily been in the public domain made by the expert regulatory agencies vested with jurisdiction over these utilities;

(2) how DHS rules interact with FERC's finding regarding the "customary" availability of utility data within its jurisdiction?

B. *The Rule's Potential for Reviews of the Same Data By Multiple Federal Agencies Before State Agencies Can Gain Access Should Be Reconsidered.*

The proposed rule provides for review of data submitted as CII by a DHS CII Program Manager to determine whether, in fact, the characterization is correct. *See*, Section 29.4. The rule further provides, at Section 29.5 (d) (2):

The Federal agency or DHS component forwarding the information to the CII Program Manager may not disseminate, distribute, or make public the information until the CII Program Manager has notified the agency or component that the Program Manager has validated the information.

The rule text suggests that much of the information NARUC's member commissions require will be submitted via regulatory proceedings at other agencies, and thus may not be subject to the DHS's rules. As discussed, *infra*, we respectfully request clarifications on the application of DHS's rules to other agency proceedings. However, in the event we have misconstrued the generic impact of the rule to information "involuntarily" submitted to other federal agencies and/or in the event that some information submitted to other agencies does fall within the meaning of "voluntary" and thus subject to the DHS's rules, we are concerned that the possible need for CII review both under the submitting agency and the DHS process could require not one but two agency reviews before the data can be released to the requesting state. Therefore, we request that the DHS develop a procedure that assures that it can cooperate with other agencies to assure expeditious, non-duplicative review of CII release, so that information review delays don't compromise State protection of critical infrastructure.

For example, FERC's CEII rule also creates a new office to vet and approve (or disapprove) requests for CEII status and for access to information designated as CEII. Under the proposed DHS rule, State agencies with a need to use CII that also has been submitted as CEII to the FERC or other federal regulatory agencies might have to wait the completion of two (or perhaps more, if other agencies are involved) review processes. In some cases, for example, electric utility transmission network information, time may be of the essence in the availability of the data to State Commissions. Unneeded delay in access to the data could itself negatively impact Homeland Security. There is no evident basis for assuming that the reviews will be sufficiently different so that multiple reviews are needed. Similarly, the U.S. EPA has been established as the Federal agency to review vulnerability assessments regarding the water and wastewater systems.

Accordingly, NARUC respectfully requests DHS clarify that the bulk of data also submitted to other federal agencies are not subject to the DHS rule and will be accessible to the States from those agencies via those agencies' CI procedures without a duplicative DHS review or revise the DHS rule to provide that protected infrastructure information may be made available to State Commissions upon review by an agency operating under an (at least) equivalent set of rules to those governing DHS review.

IV. *DHS Should Clarify the Measure and Means by which the “Voluntariness” Test is Applied.*

As required by the Homeland Security Act, the proposed rule provides that CII is limited to information that is provided “voluntarily.” However, the means for testing “voluntariness” in the proposed rule raises questions as to: (1) the treatment of information provided initially to another agency, and then “voluntarily” provided by that agency to DHS; and (2) who makes the determination of “voluntariness” in regard to the provision of information to other agencies -- DHS or that agency.

Section 29.2 (b) provides:

Voluntary or voluntarily, when used in reference to any submission of VII to DHS means submitted in the absence of legal authority to compel access to or submission of such information; ...The term does not include information or statements submitted or relied upon as a basis for making licensing decisions, or during regulatory proceedings...the term ‘voluntary’ does not include information or statements contained in any documents or materials filed pursuant to section 12(i) of the Securities Exchange Act of 1934.

Thus, as just quoted, CII does not include information or statements submitted or relied on in regulatory proceedings. However, this proviso appears not to cover all information

routinely relied on in regulatory decision making. For example, it does not appear to cover data included in required reports, which are not necessarily submitted in conjunction with a proceeding, and which may or may not be relied on as a basis for licensing decisions.

The rule further provides, at Section 29.2(i):

Submittal to DHS as referenced in these procedures means any transmittal of CII from an entity to DHS. The CII may be provided to DHS either directly or indirectly via another Federal agency, which upon receipt of the CII, will forward it to DHS.

Thus, as quoted, information that has been involuntarily submitted to an agency other than DHS may qualify as CII if it is retransmitted by the agency to DHS, and does not meet the “voluntariness” test in regard to DHS’s authority to compel data.

However, Section 29.3(a) of the rule recognizes that:

The CII Act of 2002 and these procedures do not apply to any information that is submitted to a Federal agency pursuant to any legal requirement....when information is required to be submitted to a Federal agency to satisfy a provision of any law, it is not to be marked by the submitter, DHS, or by any other party, as submitted or protected under the CII Act of 2002 or to be otherwise afforded the protections of the CII Act of 2002.

This section provides that information submitted involuntarily to an agency does not become voluntarily transmitted through retransmission to DHS. At first blush, therefore, Section 29.3(a) would appear to confirm: (1) that the test for voluntariness is met by looking at the initial submission to an agency, not the agency forwarding to DHS; and (2) information involuntarily submitted to an agency other than DHS does not become voluntarily transmitted by its forwarding to DHS.

FERC has explained that most submissions it receives appear to be involuntary. However, the question is not so simple. The Department of Justice, in issuing its CII guidance, recognized that the “existence of agency authority to require submission of information does not automatically mean such a submission is ‘required.’” Department of Justice Freedom of Information Act Guide and Privacy Act Overview, May 2002 ed., at 202.

In light of the differing provisions governing “voluntariness,” DHS should clarify: (1) under what circumstances, if any, information can be classified as CII if it is involuntarily provided to another agency and then transmitted to DHS; (2) who shall make the determination as to whether information has been involuntarily provided to another agency— the further agency or DHS (or someone else); and (3) the extent to which the DHS definition of “voluntary” effectively prevents the application of the DHS rules to the majority of CII provided to the FERC, the FCC, EPA, or other federal agencies during the regular course of their proceedings.

V. *DHS Should Ensure that Homeland Security Is Not Compromised By Restriction of State Commission Access to Data Needed to Fulfill Their Public Missions*

Consistent with the Homeland Security Act, the proposed rule generally recognizes that State Commissions must be afforded access to CII needed to fulfill their missions, with appropriate restrictions on further disclosure. However, elements of the proposed rules may: (1) limit State Commission ability to use CII as needed to fulfill their missions; (2) limit State Commission ability to gain access to CII on the timely basis they need to fulfill their missions. As we discuss here, these elements of the rule may be inadvertent.

A. *State Commissions Applaud DHS’ Recognition of the Continued Direct Information Gathering Authority of State Agencies and The Openness*

of Regulatory Proceedings.

At the outset, State Commissions laud those aspects of DHS' proposed rule that assure that the authority of State Commissions to obtain CII directly will not be impaired, and that recognize the continued importance of public access to proceedings that have historically been public. Thus:

(1) The rule, in accord with the Homeland Security Act, makes plain that there is no intent to impair the ability or authority of State Commissions to continue to obtain information directly from entities they regulate to the extent that they have authority to do so.

Thus, Section 29.3(d) provides:

Independently obtained information. These procedures shall not be construed to limit or in any way affect the ability of a federal, State, or local Government entity, agency, or authority, or any third party, under applicable law, to obtain information by means of a different law, regulation, rule, or other authority.

Similarly, section 29.8 (g) (2) provides:

These procedures do not limit or otherwise effect the ability of a State or local government entity, agency, or authority to obtain information directly from the same person or entity voluntarily submitting information to DHS. Information independently obtained by a State or local government, entity, agency, or authority is not subject to the CII Act of 2002's prohibition on making such information available pursuant to any State or local law requiring disclosure of records or information.

(2) The rule's definition of "voluntary" as quoted above, excludes "information or

statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.” This provides that much, though not all, of the information traditionally available to the public as part of the regulatory process will not be kept from the public as CII.⁵

B. *DHS Should Make Plain That its Rule Presumes that State Commissions Have a Need to Know CII Relevant to Their Mandates, Subject to Appropriate Disclosure Provisions, to Fulfill Their Statutory Obligations*

The proposed DHS rule provides that CII “may” be made available to State Commissions. Section 29.8 (b) provides:

Federal, State and Local Government access. The CII Program Manager may provide Protected CII to an employee of the Federal Government, or of a State or local government, provided that such information is shared for purposes of securing the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another informational purpose relating to homeland security. Protected CII may be made available to a State or local government entity only pursuant to its express agreement with the Program Manager that acknowledges the understanding and responsibilities of the recipient.

Section 29.8 (d) (3) provides:

⁵ We note that this provision is particularly important because, as provided for by Section 214 of the Homeland Security Act, and included in the proposed rule, prohibitions on *ex parte* communication do not apply to the communication of CII. Thus, the application of CII status to materials that serve as the basis for decisions in regulatory proceedings could compromise the due process rights of hearing participants who may not know about CII communications. The FERC CEII rule, by contrast to the DHS rule, provide for protected CEII status for material provided in regulatory proceedings as CEII. However, the FERC rule provides for notice in the public file that material has been provided on a CEII protected basis.

State and local governments may use Protected CII only for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act.

As crafted, these provisions raise two potential problems for State Commissions that may limit their ability to do their job.

First, the rule appears to give the DHS Program Manager unbridled discretion to withhold CII from State Commissions, without regard to their need to know or the criticality of the data to the performance of their missions.

Second, in limiting the use of data to “Homeland Security” purposes, the proposal might be read to preclude State Commissions from using data as is necessary (subject to appropriate restrictions on disclosure) to fulfill their mandates.

These potential problems raise significant concerns for State Commissions as some information critical to the missions of State Commissions may be available to them *only* because the information is provided to Federal regulators. The proposed DHS rule, as cited above, does recognize that State Commissions have, and will retain, ability to directly compel production of information. However, this authority typically extends only to utilities within the jurisdiction of each State Commission.

In today’s networked world, effective regulation requires access to information regarding the operation of non-jurisdictional utilities that are connected to those within State jurisdiction. In the absence of access to such information through the Federal regulatory process, State Commissions may not have access to the data they need to do their jobs.

In the case of electricity, for example, high voltage transmission networks are now operated by utilities on a regional basis. For example, as the California experience illustrates, it is essential for State regulators to have data on the ability of their jurisdictional utilities to gain reliable and efficient access to regional transmission networks to import power. State Commissions can compel access to data on transmission from utilities within their jurisdiction, but cannot compel access to data from non-jurisdictional utilities who own or operate portions of the regional transmission network.

1. ***DHS Should State a Presumption that State Commissions Are Entitled To Access to CII Needed to Fulfill Their Mandates, Conditioned Only On Assurance that Appropriate Non Disclosure Requirements Will be Honored.***

The proposed DHS rule merely states that the data “may” be provided to State Commissions by the DHS CII Program Manager. It does not provide guidance that limits the DHS Program Manager in the exercise of his or her discretion. Nor does the rule provide a rationale for the delegation of such broad discretion to the Program Manager.

The FERC CEII rule, by contrast, states a presumption that, upon appropriate showing, State Commissions have a “need to know” data that is relevant to their regulatory obligations.⁶ The DHS rule should be revised to state a governing presumption that State Commissions are presumptively entitled to data required for the performance of their statutory mandate.

In sum, the rule should be revised to provide that CII “shall” be made available to State

⁶ The FERC final rule, at para. 53, explains that State Commissions “will be presumed to have a need to know information within their state involving issues within their responsibilities.” State Commissions must provide an explanation of their need to know data about nonjurisdictional entities. *Id.*

Commissions (or other State agencies) on showing of need to know; but the availability may be conditioned on the assurance of adequate security for the information. If the concern is that data will fall into wrong hands, then the rule should provide appropriate limits in that regard.

2. *DHS Should Make Clear that CII May Be Used By State Commissions to Fulfill Their Statutory Mandates Because the Fulfillment of these Mandates is a Building Block of Homeland Security.*

Sections 29.8 (b) and 28 (d)(3) restrict the use of CII data by State agencies to Homeland Security purposes. As quoted, the wording of these provisions might be read to mean that data can only be used insofar as is needed to protect the physical integrity (or the integrity of virtual systems) against terrorist attack. As explained above, in addition to using data on, for example, electric transmission networks to secure the networks against terrorist attack, State Commissions use such data to assure the reliable, safe, and efficient supply of electricity.

NARUC respectfully suggests that while Homeland Security is dependent on the security of the transmission network from terrorist attack, such security also depends on the nation's ability to assure that the transmission networks will, whether or not under terrorist attack, continue to be available on a safe, reliable, and efficient basis. The present wording of the rule, however, might be read to limit the use of CII data solely to efforts to protect transmission networks against terrorist attacks.

CONCLUSION

Wherefore, in view of the foregoing it is respectfully requested that DHS reconsider its proposed rule on CII in consideration of the above, and provide for revisions and modifications where appropriate.

Respectfully submitted,

/S/
James Bradford Ramsay
GENERAL COUNSEL

/S/
Sharla M. Barklind
ASSISTANT GENERAL COUNSEL

National Association of Regulatory Utility Commissioners
1101 Vermont Avenue, Suite 200
Washington, DC 20005
Phone: (202) 898 –2200
Fax: (202) 898-2213

E-mail: jramsay@naruc.org or sbarklind@naruc.org

Webpage: www.naruc.org

DATE: June 16, 2003