

Duke Energy Corporation.txt

Subject: Duke Energy Corporation Comments on DHS NOPR RIN 1601-AA14
Date: Mon, 16 Jun 2003 13:16:07 -0400
From: "C Norwood Davis III" <cndavis@duke-energy.com>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Associate General Counsel
Department of Homeland Security
Washington, DC 20528

Dear Sir or Madam:

On behalf of Duke Energy Corporation, I submit the attached comments on the Department of Homeland Security's Notice of Proposed Rulemaking regarding Procedures for Handling Critical Infrastructure Information (RIN 1601-AA14). Should there be any difficulties in this transmittal, please contact me at 704-382-2498 or cndavis@duke-energy.com.

Sincerely,

C. Norwood Davis
Managing Director
Public Policy Analysis
Duke Energy Corporation

(See attached file: DUK Comments on DHS CII NOPR - June 2003 - FINAL.doc)

DHS	Name: DUK Comments on
2003	CII NOPR - June
	- FINAL.doc
	Type: WINWORD File
	Encoding: base64
	Description: DUK Comments on
DHS	CII NOPR - June
2003	- FINAL.doc

UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF HOMELAND SECURITY

Procedures for Handling Critical § RIN 1601-AA14
Infrastructure Information §

COMMENTS OF DUKE ENERGY CORPORATION

Pursuant to the April 15, 2003 Notice of Proposed Rulemaking (“NOPR”) regarding Procedures for Handling Critical Infrastructure Information (“CII”) of the Department of Homeland Security (“Department” or “DHS”),¹ Duke Energy Corporation (“Duke”) submits the following comments.

I.

COMMUNICATIONS

The name, title, and mailing addresses of the persons at Duke to whom correspondence and communications concerning these comments should be addressed are:

Terrence P. Luddy
Director
Enterprise Security
Duke Energy Corporation
526 South Church Street
Charlotte, NC 28202
(704) 382-6462
tpluddy@duke-energy.com

C. Norwood Davis
Managing Director
Public Policy Analysis
Duke Energy Corporation
526 South Church Street
Charlotte, NC 28202
(704) 382-2498
cndavis@duke-energy.com

¹ *Procedures for Handling Critical Infrastructure Information*, “Notice of Proposed Rulemaking,” 6 CFR Part 29 (2003).

II. BACKGROUND

A. Description of the CII NOPR

The Department has issued this CII NOPR for the purposes of establishing uniform rules and procedures to govern the receipt, care and storage by federal agencies of critical infrastructure information voluntarily provided to the Federal Government in the aftermath of the September 11, 2001 terrorist attacks on the United States, and of fulfilling the Department's responsibilities under the Homeland Security Act (Pub. L. 107-296). In the CII NOPR, the Department seeks to protect the public safety from terrorist attacks on the nation's infrastructure by ensuring that information provided to the federal government that contains sensitive and potentially-debilitating information on critical infrastructure is protected from general disclosure by federal agencies to the public, including disclosure to those persons who may have a desire to perpetrate terrorist acts against such vital assets.

B. Description of Duke Energy Corporation

Duke Energy Corporation is a diversified energy company which owns and operates vital energy infrastructure throughout the world, including pipelines and other facilities for the collection, processing and transportation of natural gas, an extensive network of electric generation (nuclear, coal, hydro-electric and natural gas), transmission and distribution facilities located in its service territory in North Carolina and South Carolina, and a fleet of gas-fired merchant generation facilities. Duke is a company entrusted with the obligation to ensure the safety and reliability of its interstate natural gas pipeline system, generation facilities and its electric transmission and distribution grid, and therefore, Duke has a keen interest in this NOPR and the development of processes and procedures that will enhance protection of the nation's critical assets.

III. EXECUTIVE SUMMARY

Terrorist threats to the United States energy infrastructure have a new relevance since “9-11,” and anticipating and responding to these threats will continue to be of critical national interest for the indefinite future. Within the context of this new reality, Duke appreciates and supports the Department’s efforts to determine how best to safeguard CII. Further, we support the Department’s proposal of a consistent definition of CII between the Department and the Federal Energy Regulatory Commission (the “FERC”) and encourage the Department to continue to seek ways to coordinate its efforts with those of the FERC and to align its policies and procedures with those rules adopted by the FERC (e.g., FERC Order 630) and other federal, state and local agencies.

Duke believes that the final rule adopted in this proceeding should complement and support the ongoing efforts of federal, state and local governmental agencies and private industry that are working to protect the critical infrastructure of this nation. Duke therefore supports the objectives outlined in the CII NOPR to limit public access to CII and place it only in the hands of those parties who have justified their need for such access. Failure to protect CII could, as the Department has properly recognized, jeopardize the general health, welfare, and safety of our nation. However, we caution that any time CII is shared with another entity, some level of security is compromised. Therefore, we urge the Department to consider ways to enhance its procedures to protect CII. Specifically, Duke offers the following ways to improve upon the final rule and its implementation:

- The Department should expand the type of information to be encompassed by the rule to include more than ‘voluntarily-provided’ information;
- The Department should enhance its internal administration and protection procedures; and

- The Department should place additional limitations on the release of CII to third parties, including state and local agencies, without a clear showing of need.

IV.

DETAILED COMMENTS

A. Clarify the Definition of Protected Critical Infrastructure Information

The proposed rulemaking protects only CII that is “voluntarily submitted”. Given the previously stated nature of CII, Duke suggests that the scope of the rulemaking be expanded to include all CII that is possessed or received by the federal government regardless as to whether submission was voluntary, compulsory, or inadvertent. Duke does not believe that information is any less deserving of CII designation due to the fact that such information is disclosed pursuant to a mandatory application, order, subpoena or other non-voluntary process. As noted by the Department, the proposed CII rule does not contemplate a complete bar on public disclosure, but instead, establishes a much-needed screening mechanism to ensure that all disclosures are carefully weighed. Therefore, Duke believes a broadening of the scope of the rule to include non-voluntary information is appropriate and would not significantly impinge upon the rights of any third party to obtain such information if so needed.

B. Strengthen Program Administration

Additionally, Duke believes that there are several internal administrative and procedural steps that the Department can take to enhance its receipt, care and storage process. These steps include:

- enhancing §29.4 of the rule to include internal audit programs and independent oversight authority to assure compliance with the intent of the rulemaking as well as to identify and correct deficiencies in a timely manner;

- clarifying in §29.6(f) what constitutes a breach of good faith;
- specifying in §29.6(g) what criteria must be met in order for the CII Program Manager to change the status of CII, and outlining what happens to the re-designated information (i.e., whether it is maintained, destroyed or whether notification of the submitter is required); and
- identifying in §29.4(e) the necessary security provisions, data quality management, or records retention processes essential to maintain the Critical Infrastructure Information Management System (CIIMS) and undertaking adequate steps to ensure the quality, accuracy, and security of Protected CII within the CIIMS.

C. Limit Release of Critical Infrastructure Information to Third Parties

Duke believes the Department should consider further limitations on the disclosure of CII to certain third parties. For example, §29.8(a) of the proposed rule would give the Department excessively broad discretion to authorize access to or the disclosure of Protected CII without a clear showing of need by the requesting party. Duke recommends that the Department implement clearly defined internal procedures which must be followed prior to disclosure, including prior notification to the submitter.

Another area of the proposed rule where the disclosure procedures for the Department appear to be excessively broad is in §29.8(b). That section would allow for the disclosure of CII to state and local governments who express a need in order to protect critical infrastructure and without any showing of adequate protections in place by such agencies or any notice to or the written consent of the submitter. Duke Energy recommends that the rulemaking be narrowed to allow disclosure to state and local agencies only after consultation with the submitter and upon a

showing by such state and local agencies that they have in place appropriate processes and procedures to adequately protect the CII. Otherwise, the Department will create a potentially large loophole in its attempt to protect CII when it discloses such information to a local agency without any protections in place for CII. Duke believes that the proposal to disclose to state and local agencies is far too ambiguous in this regard and could compromise the very security the Department is seeking to preserve. Instead, the Department should adopt reasonable criteria for disclosure to state and local agencies and limit such dissemination to the extent practicable.

Similarly, §29.8(c) of the proposed rulemaking allows for the disclosure of CII to federal contractors that are “performing services in support of the purposes of DHS”. Duke recognizes the need for the Department to rely upon the expertise of federal contractors, but recommends that the provision be enhanced to ensure appropriate security clearances, authorization processes, and review processes are established prior to release of information to federal contractors.

V. Conclusion

Wherefore, for the reasons set forth above, Duke respectfully requests that the Department consider these comments and clarify or modify its Procedures for Handling Critical Infrastructure Information accordingly.

Respectfully submitted,

DUKE ENERGY CORPORATION

Terrence P. Luddy
Director
Enterprise Security
Duke Energy Corporation
526 South Church Street
Charlotte, NC 28202
(704) 382-6462
tpluddy@duke-energy.com

C. Norwood Davis
Managing Director
Public Policy Analysis
Duke Energy Corporation
526 South Church Street
Charlotte, NC 28202
(704) 382-2498
cndavis@duke-energy.com

Comments of Duke Energy Corporation

Dated: June 16, 2003