

2005



NARUC

The National
Association
of Regulatory
Utility
Commissioners

Technical Assistance Briefs:
Critical Infrastructure
Information Sharing Rules:
Model Protocols for States

VERSION 1

Prepared by
The Institute of Public Utilities

April 2005

Funded by the U.S. Department of
Energy's Office of Electricity and
Energy Assurance

**TECHNICAL ASSISTANCE BRIEF ON
CRITICAL INFRASTRUCTURE PROTECTION**

**CRITICAL INFRASTRUCTURE INFORMATION
SHARING RULES: MODEL PROTOCOLS FOR STATES**

NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS
AD HOC COMMITTEE ON CRITICAL INFRASTRUCTURE

APRIL 2005

VERSION 1

NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS

1101 Vermont, N.W., Suite 200

Washington, DC 20005, USA

Phone: (202) 898-2200

Fax: (202) 898-2213

admin@naruc.org

**NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS
AD HOC COMMITTEE ON CRITICAL INFRASTRUCTURE**

Letter from the Chair

Commissioner Connie O. Hughes, New Jersey Board of Public Utilities
March 2005

As Chair of the NARUC Ad Hoc Committee on Critical Infrastructure, I am proud to present landmark series of reports to public utility regulators, policymakers, utility industry leaders, as well as consumers on issues surrounding complex issues pertaining to our Nation's utility critical infrastructures. These documents set strategies for consideration for future potential challenges within the utility sectors.

I trust that these documents will assist and provide better understanding and greater knowledge on the complex issues and components related to critical infrastructure protection.

The Committee appreciates and is grateful for the assistance in preparing these reports by Dr. Janice A. Beecher, Institute of Public Utilities at Michigan State University and Dr. James B. Atkins, Regulatory Heuristics. I also acknowledge the support and funding provided by the U.S. Department of Energy's Office of Electricity and Energy Assurance under the leadership of Alex de Alvarez and assistance of Alice Lippert. I also thank the National Association of Regulatory Commissioners, the NARUC Staff Subcommittee on Critical Infrastructure and other state partners including the National Association of State Energy Officials, the National Conference of State Legislatures and the National Governors Association.

Commissioner Connie O. Hughes
Chair, Ad Hoc Committee on Critical Infrastructure

This Technical Brief (Paper No. 6) is part of a series of reports prepared under the direction of the NARUC Ad Hoc Committee on Critical Infrastructure. Funding for this project was provided to NARUC by the U.S. Department of Energy in cooperation with the National Association of State Energy Officials.

The purpose of these complementary and reinforcing papers is to provide public utility commissioners and other participants in the regulatory policy community with introductory overviews, suggested protocols, and additional resources on critical infrastructure protection issues.

Paper 1. *Issue Paper on Critical Infrastructure Protection.* The federal and state roles in critical infrastructure protection are introduced and explored, with a special focus on the role of the state agencies and public utility commissions.

Paper 2. *Utility and Network Interdependencies: What State Regulators Need to Know.* As explored here, almost all utilities operate networks, and these sector networks are highly interdependent, which in turn relates to consideration of vulnerability and planning which takes on an added dimension of complexity needs, as well as regulatory considerations.

Paper 3. *A Primer on Energy Assurance for Public Utility Commissions.* The primer provides an introduction to energy assurance planning, which broadens traditional energy emergency response and planning to include critical infrastructure protection and energy and fuel shortage mitigation.

Paper 4. *State Government Organizational Issues, Roles, and Policy.* This discussion paper explores state governmental roles with respect to critical infrastructure protection, with a focus on the state public utility commissions and regulatory policy considerations.

Paper 5. *Regional Coordination and Intergovernmental Communication in the Energy Sector.* This paper highlights the importance of regional coordination and communication, focusing in particular on the protocols developed for the Energy Emergency Assurance Coordinators (EEAC) system that has identified state level energy experts for petroleum, gas and electricity.

Paper 6. *Critical Infrastructure Information Sharing Rules: Model Protocols for States.* The paper discusses both federal and state actions to date regarding the sharing of critical infrastructure information and provides a framework for future cooperation and efforts to harmonize information sharing among state commissions, the FERC and the Department of Homeland Security.

Paper 7. *NARUC Inventory on State Energy Assurance Planning.* The paper reports in detail the findings of a 2004 assessment of state commissions regarding energy assurance planning and related policy issues.

Paper 8. *NARUC Inventory on Gas Curtailment Planning.* The paper reports in detail the findings of a 2004 assessment of state commissions regarding gas curtailment planning and related policy issues.

TABLE OF CONTENTS

Executive Summaryiv

Introduction 1

Federal Infrastructure Information Disclosure Rules.....3

 Federal Energy Regulatory Commission.....3

 FERC Order No. 630.....3

 FERC Order No. 630-A.....4

 FERC Order No. 6494

 Department of Homeland Security.....5

 Critical Infrastructure Information Act of 20025

 DHS Proposed Rule for Handling Critical Infrastructure Information7

 NARUC Response to the DHS Proposed Rule.....9

 DHS Interim Rule for Handling Critical Infrastructure Information10

State Efforts on Infrastructure Information Disclosure Rules15

 Drinking Water Sector15

 NARUC Energy Assurance Planning Inventory16

 State Information Disclosure Best Practices17

CI Information Sharing Protocols.....23

 State FOIA Exemption Rules.....23

 Designation of a Security Information Coordinator.....25

 Cooperative Efforts with FERC and DHS26

 Federal Energy Regulatory Commission.....26

 Department of Homeland Security.....27

 Coordination with Non-Governmental Organizations28

Commission Procedures for Protecting Sensitive Information29

Appendix A: FERC CEII Request Form32

Appendix B: Selected State FOIA Exemptions33

EXECUTIVE SUMMARY

The September 11, 2001 terrorist attacks on the United States forever changed the planning, operation and management of the Nation's telecommunications energy, water and wastewater critical infrastructures (CI). The protection of these interdependent infrastructure sectors presents a challenge to federal, state and local governments, as well as the private interests that own and operate much of these networks. Access and utilization of CI information, ranging from maps to complex network and system models, is vital in protecting and reducing the vulnerability to terrorism and other threat events, and also in improving system recovery following an event.

Since 2001, the Federal Energy Regulatory Commission (FERC) and the Department of Homeland Security (DHS) have issued rules governing the disclosure of critical infrastructure (CI) information. While promoting and encouraging information sharing, the rules have been highly contentious regarding access of state regulators to CI information.

State public utility commissions both individually and collectively through the National Association of Regulatory Utility Commissioners (NARUC), have a long history of policy formulation and progressive regulatory oversight of the much of the Nation's energy, telecommunications, water and wastewater infrastructure. State commissions have been at the forefront of CI protection because of their jurisdiction over, including but not limited to, certification, ratemaking, quality-of-service, integrated resource planning, cost-recovery and facility siting. In order for them to make sound and fact-based decisions, state commissions must have open and unconstrained access to CI information.

This paper discusses both federal and state actions to date regarding the sharing of CI information, and to provide suggestions for future cooperation and efforts to harmonize CI information sharing among state commissions, the FERC and the DHS. Specifically, this paper discusses and responds to the following questions:

- What protocols are needed for state commissions to effectively operate within the DHS and FERC rules on disclosure of critical infrastructure information?
 - Are there state policies and procedures on disclosure of critical infrastructure information that represent best practices?
 - How can the sharing of sensitive critical infrastructure information be improved among federal and state entities?

Since September 11, 2001, substantial resources and efforts have been expended by federal, state and local governments, as well as the private sector, developing processes and rules to reduce the vulnerability of Nation's CI. Protection of CI Information from unjustified public disclosure represents one the most important and challenging regulatory issues facing state commissions. The review of the federal and state efforts presented in this paper suggests that programmatic inefficiencies and inconsistencies in developing CI information disclosure rules and procedures.

Therefore, given the inconsistencies between the DHS Interim Rule and FERC Order No.630, and subsequent amendments, what administrative or legal procedures should state commissions consider to efficiently share and utilize CI information with these agencies and other state commissions? Additionally, what protocols should state commissions consider to efficiently and effectively harmonize public utility regulation given the diversity of State rules on disclosure of critical infrastructure information?

The suggested information management protocols for state commissions address:

Implementation of State FOIA Exemption Rules. State commissions should seek to implement forward-looking FOIA Exemption Rules which properly address broad utility sectors and associated processes

Designation of a Security Information Coordinator. State commissions and/or regional state committees should appoint a security information coordinator to manage CI information.

Cooperative Efforts with FERC and DHS. State commissions, regional state committees, NARUC, or NARUC-affiliated regional associations should initiate the development of memorandum of understanding, or other appropriate instrument, with the FERC and DHS regarding CI information sharing.

Coordination with Non-Governmental Organizations. State commissions, regional state committees, NARUC, or NARUC-affiliated regional associations should initiate the development of a memorandum of understanding, or other appropriate instrument, with NERC regarding CI information sharing.

In addition to protocols regarding sharing of CI information and strong FOIA exemptions to protect it, the state public utility commissions can implement a number of additional procedures to ensure that sensitive information legally and physically protected and properly handled.

INTRODUCTION

The September 11, 2001 terrorist attacks on the United States forever changed the planning, operation and management of the Nation's telecommunications energy, water and wastewater critical infrastructures (CI). The protection of these interdependent infrastructure sectors presents a challenge to federal, state and local governments, as well as the private interests that own and operate much of these networks. Access and utilization of CI information, ranging from maps to complex network and system models, is vital in protecting and reducing the vulnerability to terrorism and other threat events, and also in improving system recovery following an event.

The National Strategy for Homeland Security set forth a number of principles to guide the Nation's development of information systems for homeland and energy security.¹ These principles included

- Unifying the “homeland security community such that federal, state, and local governments are viewed as one entity”
- That “information will be captured once at the source and used many times to support multiple requirements” and
- To “protect the public's right to access information, but to do so in balance with security concerns.”

Regarding the last point, the Nation has been built on the principle of open government and access to various types of public information under both federal and state Freedom of Information Act (FOIA) policies. However, government must now balance the public's right to know specific and detailed energy infrastructure information versus the potential risks of public disclosure.

A 2003 report from the National Conference of Legislatures (NCSL) provided an overview of energy security issues and the role of state governments “in effectively preventing and responding to energy security threats.”² One of the policy options proposed was that State Legislatures should “provide for sharing of information and coordinating responses between federal, state and local government agencies as well as the energy industry.” Since 2001, the Federal Energy Regulatory Commission (FERC) and the Department of Homeland Security (DHS) have issued rules governing the disclosure of critical infrastructure (CI) information. While promoting and encouraging information sharing, the rules have been highly contentious regarding access of state regulators to CI information.

¹ Office of Homeland Security, *National Strategy for Homeland Security* (Washington, DC, July 2002).

² National Conference of State Legislatures, *Energy Security* (Washington, DC, April 2003).

State public utility commissions, both individually and collectively through the National Association of Regulatory Utility Commissioners (NARUC), have a long history of policy formulation and progressive regulatory oversight of the much of the Nation's energy, telecommunications, water and wastewater infrastructure. State commissions have been at the forefront of CI protection because of their jurisdiction over, including but not limited to, certification, ratemaking, quality-of-service, integrated resource planning, cost-recovery and facility siting. In order for them to make sound and fact-based decisions, state commissions must have open and unconstrained access to CI information.

NARUC has been actively involved in improving and promoting policies to improve the sharing of utility-related CI information between state and federal agencies. In particular, the NARUC Ad Hoc Committee on Critical Infrastructure authored a Resolution Regarding the FERC's Critical Energy Infrastructure Information (CEII) Policy, and Statement on the Treatment of Previously Public Documents. The resolution was approved by the NARUC Board on November 11, 2002 and recognized the importance of rules on disclosure of CI information and resolved that the NARUC Ad Hoc Committee on Critical Infrastructure would continue to work with FERC on rules governing access to, and disclosure of CI information.

This paper discusses both federal and state actions to date regarding the sharing of CI information, and to provide suggestions for future cooperation and efforts to harmonize CI information sharing among state commissions, the FERC and the DHS. Specifically, this paper discusses and responds to the following questions:

- What protocols are needed for state commissions to effectively operate within the DHS and FERC rules on disclosure of critical infrastructure information?
 - Are there state policies and procedures on disclosure of critical infrastructure information that represent best practices?
 - How can the sharing of sensitive critical infrastructure information be improved among federal and state entities?

FEDERAL CRITICAL INFRASTRUCTURE DISCLOSURE RULES

FEDERAL ENERGY REGULATORY COMMISSION

FERC Order No. 630

In direct response to the terrorist attacks on the United States on September 11, 2001, the Federal Energy Regulatory Commission (FERC) issued a Policy Statement in Docket No. PL02-1-000 (October 11, 2001) that removed from easy public access certain documents that previously had been public. On February 21, 2003, FERC issued Order No.630 which established a procedure for gaining access to critical energy infrastructure information (CEII) that would otherwise not be available under the Freedom of Information Act (FOIA).³ In general, the rule establishes procedures to limit the public disclosure of sensitive infra-structure information, thereby decreasing the use of such information to plan or execute terrorist attacks.

In Order No.630, CEII is defined as information about proposed or existing critical infrastructure that:

- (i) Relates to the production, generation, transportation, transmission, or distribution of energy;
- (ii) Could be useful to a person in planning an attack on critical infrastructure;
- (iii) Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and
- (iv) does not simply give the location of the critical infrastructure.⁴

FERC created a CEII Coordinator to process non-FOIA requests for CEII and make various determinations regarding such requests. If the CEII Coordinator determines that the requested information is indeed CEII, the CEII Coordinator determines the eligibility of the requestor to receive the CEII and if any conditions are required concerning release of the information. Ultimately, the CEII Coordinator must balance the requester's need for the information against the sensitivity of the information.⁵

³ U.S. Federal Energy Regulatory Commission, *Order No. 630, Critical Energy Infrastructure Information*, 102 FERC ¶ 61, 190, 18 CFR Parts 375 and 388 (Docket Nos. RM02-4-000, PL02-1000), February 21, 2003.

⁴ *Ibid.* at 19 and 69. See 18 CFR 388.113 (c) (1).

⁵ *Ibid.* at 70. See 18 CFR 388.113 (d) (3).

FERC Order 630-A

On July 23, 2003, FERC issued Order 630-A revising Order No. 630. The Order revised the CEII filing instructions, the CEII request procedures, and the instructions for requesting rehearing of the CEII Coordinator's decision.⁶ Specifically, Order No. 630-A revised 18 CFR Section 388.113 paragraphs (d)(3)(i) to read:

File a signed, written request with the commission's CEII Coordinator. The request must contain the following: requester's name (including any other name(s) which the requester has used and the dates the requester used such name(s)), date and place of birth, title, address, and telephone number; the name, address, and telephone number of the person or entity on whose behalf the information is requested; a detailed statement explaining the particular need for and intended use of the information; and a statement as to the requester's willingness to adhere to limitations on the use and disclosure of the information requested. Requesters are also requested to include their social security number for identification purposes. Federal agency employees making requests on behalf of Federal agencies may omit their social security number, and date and place of birth.

FERC Order No. 649

Most recently on August 3, 2004, the FERC again amended its regulations for gaining access to CEII. Among other items, Order No.649 modified the procedure simplifying federal agency access to CEII.⁷ Once a federal agency has been granted access to CEII in a docket, it is entitled to receive subsequent CEII in that same docket. However, the federal agency must file a request for the additional information. The subsequent request may be as simple as a phone call or e-mail to a staff contact requesting additional CEII in the docket.

Order No.649 also examined the advantages and disadvantages of placing time limits (such as two years) on a recipient's use of CEII. The FERC concluded that the sensitivity of much of the CEII will diminish over time and declined to place time limits on a recipient's access to CEII, but would consider doing so in a unique case where a compelling need could be shown.⁸

⁶ U.S. Federal Energy Regulatory Commission, *Order No. 630-A, Critical Energy Infrastructure Information*, 104 FERC ¶ 61,106, 18 CFR Part 388 (Docket Nos. RM02-4-001 and PL02-1-001), Issued July 23, 2003.

⁷ U.S. Federal Energy Regulatory Commission, *Order No. 649, Critical Energy Infrastructure Information*, 108 FERC ¶ 61,121, 18 CFR Part 388, (Docket Nos. RM02-4-002, PL02-1-002, RM03-6-001), Issued August 3, 2004).

⁸ *Ibid.* at 15.

Regarding the filing and processing of CEII requests, one comment stated that it was unnecessarily burdensome to require individual members of an organization to file separate requests and non-disclosure agreements (NDAs). The FERC failed to agree stating that it chose not to clear entire entities to receive CEII, deciding instead to clear each individual requesting CEII. The FERC also concluded in Order No. 649 that the current approach of not allowing blanket approval is necessary to effectively limit the number of people getting access to CEII. Moreover, the burden associated with filing a CEII request is minimal.⁹

Specific information regarding the FERC CEII Program, including guidance on how to file a CEII request can be found on the [FERC website](#).¹⁰ A copy of the CEII Request Form can be found in Appendix A of this report and is [available for download](#).¹¹

DEPARTMENT OF HOMELAND SECURITY

Critical Infrastructure Information Act of 2002

The Critical Infrastructure Information Act of 2002 (“CIIA”), to be codified at 6 U.S.C. Sections 131 - 134, was passed on November 25, 2002 as subtitle B of Title II of the Homeland Security Act (P.L. 107-296, 116 Stat. 2135, sections 211 - 215), and regulates the use and disclosure of information submitted to the Department of Homeland Security (DHS) about vulnerabilities and threats to critical infrastructure.¹²

The CIIA serves to promote information sharing between the private and public sectors on vulnerabilities and threats of the nation's critical infrastructures in order to protect these critical assets. The CIIA establishes several limitations on the disclosure of critical infrastructure information voluntarily submitted to DHS.

The CIIA sets forth a number of important definitions including “critical infrastructure information” and “voluntary”. Critical infrastructure information (CII) is defined as “information not customarily in the public domain and related to the security of critical infrastructure or protected systems

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including misuse of or unauthorized access

⁹ Ibid. at 8.

¹⁰ U.S. Federal Energy Regulatory Commission, <http://www.ferc.gov/>.

¹¹ U.S. Federal Energy Regulatory Commission, <http://www.ferc.gov/help/how-to/file-ceii.asp>.

¹² *The Critical Infrastructure Information Act of 2002* (“CIIA”), P.L. 107-296, November 25, 2002, 6 U.S.C. Sections 131 - 134, Subtitle B of Title II of the Homeland Security Act.

to all types of communications and data transmission systems) that violates federal, state, or local law, harms interstate commerce of the United States, or threatens public health and safety;

(B) the ability of critical infrastructure or protected systems to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or,

(C) any planned or past operational problem or solution regarding critical infrastructure...including repair, recovery, reconstruction, insurance, or continuity to the extent it relates to such interference, compromise, or incapacitation.”¹³

Voluntary, “in the case of any submittal of critical infrastructure information to a covered Federal agency, means the submittal in the absence of such agency’s exercise of legal authority to compel access to or submission of such information...”¹⁴ DHS is the “covered federal agency” in the CIIA.¹⁵ The information must also be accompanied by an “express statement” that “the information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002.”¹⁶ However, the term voluntary “does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.”¹⁷

“Any CII voluntarily submitted to the DHS for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, is exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act).”¹⁸ Further, the “CII shall not, if provided to a State or local government or government agency

(i) be made available pursuant to any State or local law requiring disclosure of information or records;

(ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the

¹³ P.L. 107-296, § 212 (3).

¹⁴ P.L. 107-296, § 212 (7).

¹⁵ P.L. 107-296, § 212 (2).

¹⁶ P.L. 107-296, § 214 (a) (2) (A).

¹⁷ P.L. 107-296, § 212 (7) (B).

¹⁸ P.L. 107-296, § 214 (a) (1) (A).

written consent of the person or entity submitting such information; or

(iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act.”¹⁹

Despite these limitations on disclosure, the CIIA is not intended to prohibit the ability of other entities from obtaining information on CII. Section 214 (c) states that “nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law.”²⁰ Additionally, “Protected CII shall not be construed to constitute compliance with any requirement to submit such information to a Federal agency under any other provision of law.”²¹

DHS Proposed Rule for Handling Critical Infrastructure Information

The DHS Proposed Rule to address the “Procedures for Handling Critical Infrastructure Information” was published at 68 Federal Register 18524 on April 15, 2003. The Proposed Rule established uniform procedures for the receipt, care, and storage of CII voluntarily provided to the Federal Government by the public. The procedures apply to all Federal agencies that receive, care for, or store CII that is voluntarily submitted to the Federal Government pursuant to the CIIA.

The Proposed Rule also establishes a CII Program Manager within the DHS to direct and administer the program. The CII Program Manager is also charged with “establishing procedures to ensure that any DHS component or other entity that works with CII appoints one or more employees to serve as a CII Officer to provide proper management and oversight.” Refer to Section 29.4 (c). Section 29.4 (d) states that “the CII Officer shall:

- (1) Oversee the storage and handling of Protected CII;
- (2) Establish and maintain an ongoing self-inspection program, to include periodic review and assessment of the entity’s storage, handling, and use of Protected CII;

¹⁹ P.L. 107-296, § 214 (a) (1) (E).

²⁰ P.L. 107-296, § 214 (c).

²¹ P.L. 107-296, § 214 (d).

- (3) Establish additional procedures as necessary to prevent unauthorized access to Protected CII; and
- (4) Ensure prompt and appropriate coordination with the CII Program Manager regarding any request, appeal, challenge, complaint, or suggestion arising out of the implementation of these procedures.”

The Proposed Rule provides in Section 29.8 (b) that “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.”

Consistent with the CIIA, Section 29.3 (d) of the Proposed Rule provides that “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.”

Access to Protected CII by Federal, State and local governments is set forth in Section 29.8 (b). The section states that “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.”

This Section also provides further guidance and restrictions on the use of such information. Specifically, “State and local governments receiving information marked “Protected Critical Infrastructure Information” shall not disclose that information to any other party...”, “without first obtaining authorization from the CII Program Manager, who shall be responsible for requesting and obtaining written consent for any such State or local government disclosure from the person or entity that submitted the information.” Refer to Section 29.8 (b). State and local governments are further prohibited from disclosing or distributing Protected CII to another party “unless the Program Manager first obtains the written consent of the person or entity submitting the information.” Lastly, “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.”

NARUC Response to the DHS Proposed Rule

NARUC filed comments June 16, 2003, on the Proposed Rule to address the “Procedures for Handling Critical Infrastructure Information” and sought to work with DHS to:²²

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.

More specifically, NARUC voiced a number of concerns regarding (1) inconsistencies with other critical infrastructure protection programs, in particular those of the FERC, (2) the definition of “voluntary”, and (3) the potential for the Proposed Rule to impair the ability of state commissions to perform their statutory functions. NARUC requested DHS to clarify and consider the following:

1. In regard to infrastructure owned and operated by regulated utilities, the relation between the “Not Customarily in the Public Domain” requirement for CII and FERC’s CEII Rule.²³
2. That “data also submitted to other federal agencies are not subject to the DHS rule and will be accessible to the States from those agencies”... “without a duplicative DHS review...”²⁴
3. Regarding the application of the term “voluntary” to submittal of CII,
 - a. Under what circumstances can information be “classified as CII if it is involuntarily provided to another agency and then transmitted to DHS”;

²² National Association of Regulatory Utility Commissioners, Comments to DHS Regarding the Proposed Rule to address the “Procedures for Handling Critical Infrastructure Information” (June 16, 2003).

²³ NARUC Comments, 7.

²⁴ NARUC Comments, 11.

- b. Who determines whether information has been involuntarily provided to another agency; and
 - c. “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.”²⁵
4. “DHS should modify the rule to presume that State Commissions have a need to know CII relevant to their mandates, subject to appropriate disclosure provisions, to fulfill their statutory obligations.”²⁶
5. DHS should clearly state “that CII may be used by State Commissions to fulfill their mandates” since those mandates are “the building blocks of homeland security.”²⁷

DHS Interim Rule for Handling Critical Infrastructure Information

All total, DHS received 117 different sets of comments on the Proposed Rule including those submitted by NARUC. DHS made a number of changes to the Proposed Rule and published the Interim Rule at 69 Federal Register 8074 on February 20, 2004. A number of the changes and additions made by DHS clarify some of NARUC’s comments, although other comments remain either unaddressed or unclear. These include:

1. DHS received numerous comments regarding the indirect submission of CII to DHS from other Federal government entities. DHS removed references throughout the Interim Rule to indirect submissions, and revised Sections 29.2 and 29.5 to clarify that only the DHS will be the recipient of voluntarily submitted CII. However, this matter will need to be revisited since the Supplementary Section of the Interim Rule states that

After the Protected CII Program has become operational, however, and pending additional legal and related analyses, the Department anticipates the development of appropriate mechanisms to allow for indirect submissions in the final rule and would welcome comments on appropriate procedures for the implementation of indirect submissions.

2. As in the proposed rule, the Interim Rule retains the scope of applicability of the rule to include “ all Federal agencies that receive, care for, or store CII voluntarily submitted to the Federal Government

²⁵ NARUC Comments, 13.

²⁶ NARUC Comments, 15.

²⁷ NARUC Comments, 18.

pursuant to the CIIA” and ... “to State, and local governments, and government authorities, pursuant to their express agreements.” Refer to Section 29.1 (b). The Interim Rule also contains a slight modification to the definition of voluntary. The Proposed Rule stated

The term *does not include* information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

While the Interim Rule was changed to read

The term also *explicitly excludes* information or statements submitted during a regulatory proceeding or relied upon as a basis for making licensing or permitting determinations.

This change addresses in part NARUC’s concerns regarding the application of DHS CII rules to information submitted “involuntarily” to other federal agencies under existing regulatory programs and which is “customarily in the public domain”.

3. The Interim Rule also retains, at Section 29.2 (b), the definition of CII as “information not customarily in the public domain and related to the security of critical infrastructure or protected systems.” As stated in the NARUC comments on the Proposed Rule, this definition is not only contained in the Interim Rule, but also the CIIA. However, language added to Section 29.3 (d) concerning independently obtained information directly addresses the issue. This section now provides

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 otherwise obtain CII by means of a different law, regulation, rule, or other authority, *including such information as is lawfully and customarily disclosed to the public. Independently obtained information does not include any information derived directly or indirectly from Protected CII subsequent to its submission. Nothing in these procedures shall be construed to limit or in any way affect the ability of such entities, agencies, authorities, or third parties to use such information in any manner permitted by law.*

Therefore, there should be no question regarding the ability of States to use CII information obtained from other Federal agencies, FERC in particular, to meet their statutory mandates. NARUC’s comment over the treatment of CII submitted to other federal agencies is also addressed with a modification at Section 29.3 (a) which now states

The CII Act of 2002 and these procedures do not apply to or affect any requirement pertaining to information that must be submitted to DHS pursuant to a Federal legal requirement, *nor do they pertain to any obligation of any Federal agency to disclose mandatorily submitted information (even where it is identical to information voluntarily submitted to DHS pursuant to the CII Act of 2002).*

However, one other modification in the Interim Rule may need future clarification when read with the above paragraph. The last sentence in Section 29.3 (a) was also amended by the addition of a caveat regarding the submittal of information from another federal agency. This section now provides

Information submitted to any other Federal agency pursuant to a Federal legal requirement is not to be marked as submitted or protected under the CII Act of 2002 or otherwise afforded the protection of the CII Act of 2002, *provided, however, that such information, if it is separately submitted to DHS pursuant to these procedures, may upon submission to DHS be marked as Protected CII or otherwise afforded the protections of the CII Act of 2002.*

A reading of these two sentences from Section 29.3 could result in two possible conclusions. First, that other federal agencies may provide data to state commissions (under their own rules of disclosure) even though it is identical to information being protected as CII under the DHS interim rule, or second, that this same information could be protected as CII under the Interim Rule if “separately submitted” to the DHS by the other federal agency. This change would also seem to contradict the provisions in Sections 29.1 and 29.5 that prohibit indirect submissions of CII.

4. The “need or right to know” on the part of state commissions would not appear to have been directly addressed in the Interim Rule. Section 29.8 (a) remains unchanged from the Proposed Rule and that Section provides

The Under Secretary for IAIP, or the Under Secretary’s designee, *may* choose to provide or authorize access to Protected CII when it is determined that this access supports a lawful and authorized Government purpose as enumerated in the CII Act of 2002, other law, regulation, or legal authority.

As in the Proposed Rule, the Interim Rule uses the word “may” regarding access to Protected CII and gives DHS the authority to determine the “lawfulness” of the purpose of the request. Reasonable access by state commissions to Protected CII should be unquestioned

given the long history and established authority of state commissions to regulate security and reliability functions of jurisdictional electric and gas utilities and inter-connected energy systems.

Notwithstanding the lack of an explicit “need or right to know” on the part of state commissions, an oversight mechanism to [implicitly] improve information access by state commissions was added to Section 29.4 (c). The Proposed Rule states:

The CII Program Manager shall establish procedures to ensure that any DHS component or *other entity* that works with Protected CII appoints one or more employees to serve as a CII Officer for the activity in order to provide proper management and oversight. Persons appointed to these positions shall be fully familiar with these procedures.

Whereas the Interim Rule was modified to specifically include State entities and reads

The Protected CII Program Manager shall establish procedures to ensure that any DHS component or *other Federal, State, or local entity* that works with Protected CII appoints one or more employees to serve as a Protected CII Officer for the activity in order to *carry out the responsibilities stated in paragraph (d) of this section*. Persons appointed to these positions shall be fully familiar with these procedures.

Paragraph (d) provides for the duties and responsibilities of Protected CII Officers which includes “Ensure the expeditious and secure sharing of Protected CII with appropriate authorities, as set forth in Section 29.1 (a) and paragraph (b)(3) of this section.” Both of these paragraphs describe sharing of Protected CII with State entities.

5. As discussed in 4 above, Section 29.8 (a) enabled access “to Protected CII when it is determined that this access supports a lawful and authorized Government purpose as enumerated in the CII Act of 2002, other law, regulation, or legal authority.” Paragraph (a) would suggest that state commissions could request access to Protected CII fulfill their statutory obligations and mandates since these comprise “other law, regulation, or legal authority”. For example, state commissions could use Protected CII in the conduct of rate proceedings, siting hearings, fuel adjustment hearings or other docketed or undocketed sessions on electric reliability or gas curtailment plans. However, throughout the Interim Rule, disclosure of Protected CII is to be used [only] for the purpose of protecting critical infrastructure. Section 29.8 (b) (3) states

The Protected CII Program Manager or the Protected CII Program Manager's designees 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 including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland. Protected CII may be provided to a State or local government entity only pursuant to its express written agreement with the Protected CII Program Manager *to comply with the requirements of paragraph (d) of this section* and that acknowledges the understanding and responsibilities of the recipient.

And Section 29.8 (d) (3) provides

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.

Therefore, Section 29.8 would seem to have contradictory rules on the utilization of Protected CII. NARUC's desire to have DHS recognize the statutory obligations and mandates of state commission as the "the building blocks of homeland security" is not directly addressed in the Interim Rule.

6. Lastly, the Interim Rule contains the same language as the Proposed Rule in Section 29.8 (g) (1) concerning Freedom of Information Act or State or local information access laws. The Section states

Protected CII shall be treated as exempt from disclosure under the Freedom of Information Act and, if provided by the Protected CII Program Manager or the Protected CII Program Manager's designees to a State or local government agency, entity, or authority, or an employee or contractor thereof, shall not be made available pursuant to any State or local law requiring disclosure of records or information.

Section 29.8 (g) (2) goes on to state

...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.

Throughout the Interim Rule, such a “dual track” approach to manage access to, and distribution of, CII is provided. This is exemplified by reading paragraph (1) and (2) above.

STATE CRITICAL INFRASTRUCTURE INFORMATION DISCLOSURE RULES

DRINKING WATER SECTOR

Since September 11, 2001, numerous states have enacted changes to their FOIA laws to exempt CI information from public disclosure. The drinking water sector has been at the forefront of these efforts to “reinforce public disclosure laws to protect vulnerability assessments and other sensitive information related to critical infrastructure protection.”²⁸ State amendments or changes to FOIA laws were, in part, a direct result of the Bioterrorism Preparedness Act of 2002 which requires vulnerability assessments to be submitted to the U.S. EPA.²⁹ Title IV at Section 1433 (a) of the Act required that

Each community water system serving a population of greater than 3,300 persons shall conduct an assessment of the vulnerability of its system to a terrorist attack or other intentional acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water.

In addition, none of the “information contained in or derived from an assessment” can be made “available to anyone other than an individual designated by the Administrator.”³⁰ Section 1433 (a) also provided

Except for information contained in a certification under this subsection identifying the system submitting the certification and the date of the certification, all information provided to the Administrator under this subsection and all information derived there from shall be exempt from disclosure under section 552 of title 5 of the United States Code.

In February 2003, the National Conference of State Legislatures (NCSL) published a comprehensive survey of state statutes affording protection to

²⁸ Association of Metropolitan Water Agencies, *State Laws Protecting Water Security Information* (Washington, DC, September 2003).

²⁹ *Public Health Security and Bioterrorism Preparedness And Response Act Of 2002*, 107 P.L. 188; 116 Stat. 594; June 12, 2002, 107th U.S. Congress -- 2nd Session.

³⁰ P.L. 107-188, § 1433 (a) (5) (C).

drinking water systems. The report entitled “Protecting Water System Security Information in Water Security” provides a comprehensive review and analysis of various water security statutes, exemptions, water security bills introduced during 2003, and an appendix of state water security standards.³¹ These exemptions fall into two principle categories. The first is the specific protection and exemption of CI information directly under State FOIA exclusive of federal exemptions. The second is additional State FOIA exemptions for CI information that is exempt under the Federal FOIA, such as in the case of the Bioterrorism Preparedness Act of 2002. The rationale for state-specific exemptions for CI information is that such protections will reduce the success of court challenges to limits on information disclosure, and also provide “a second layer of coverage if the federal law is challenged and found to be void.”³²

ENERGY SECTOR

In an effort to exam the status of similar efforts pertaining specific to the energy sector, the Institute of Public Utilities (IPU) at Michigan State University conducted an inventory for NARUC during 2004 and early 2005 to assess state energy assurance planning programs including state Commission efforts to improve the protection of CI information from disclosure.³³ Two inventory questions were asked to assess the status of state commission or state actions concerning State FOIA modifications and the designation of state commission staff to handle security issues. The questions were:

Has your State implemented any statute, regulation or rule that modifies FOIA procedures in your State to protect sensitive information or provide other legal means of protecting information from disclosure?

Has your Commission designated a member of your staff to act as a security coordinator within your Commission?

Of the thirty-five state commissions (34 states plus the District of Columbia) responding to the inventory, a total of twenty-one states responded that they had taken some action to modify FOIA procedures in their State to protect sensitive information or provide other legal means of protecting information from disclosure. Thirteen states responded as “having taken no action” regarding State FOIA modifications.³⁴ Refer to Exhibit 1. However, these states may have responded incorrectly or misinterpreted the question since most of these states also have exemptions for water-related security. A comparison of the inventory responses from the twenty-one states having modified their State FOIA laws to

³¹ National Conference of State Legislatures, *Protecting Water System Security Information in Water Security: Innovations in State Policy* (Washington, DC, September 2003).

³² *Ibid.* at 3.

³³ NARUC *Inventory on State Energy Assurance Planning* (Technical Brief No. 7 in this series).

³⁴ *Ibid.*

the data found in the NCSL Water Security Report found that with the exception of Arkansas, the same [general] statute, regulation or rule exempting critical energy infrastructure also exempted drinking water infrastructure. These states have either generic or comprehensive FOIA exemptions which approach CI information disclosure across utility sectors. These state statutes, regulations or rules modifying State FOIA procedures can be found in Appendix B.

A total of twenty-five Commissions have designated a staff member to act as a security coordinator.³⁵ The responses to these questions are shown in the Exhibit 1. With the exception of the state commissions in Florida and Indiana, every state that has modified their respective State FOIA laws has also designated a staff member to act as a security coordinator within the commission. Of the thirteen states responded as “having taken no action” regarding State FOIA modifications, five states indicated as having designated a staff member to act as a security coordinator within the commission.

STATE INFORMATION DISCLOSURE BEST PRACTICES

While not intended to be an exhaustive review of all states, examination of efforts to modify information disclosure rules in a select number of states responding to the NARUC Inventory can provide a “set of best practices” for other state commissions without such rules. State FOIA exemptions to protect disclosure of CI information fall into four general categories, although State statutes may include multiple categories of exemptions. These include:

First, the commission has the specific statutory authority to issue protective orders covering confidential or proprietary information which can include CI information. This is a common tool available to state commissions. The drawback of this type of exemption process is that a decision must be made on a case-by-case basis for any potential CI information in question. Examples include:

Arkansas. Under Ark. Code Ann. 23-2-316, the commission has the specific statutory authority to issue protective orders of non-disclosure covering confidential or proprietary information. The section states that any fact and information, including all reports, records, files, books, accounts, papers, and memoranda in the possession of the commission can be protected from disclosure whenever the commission determines it to be necessary in the *interest of the public... in the interest of the utility* to withhold such facts and information from the public.

³⁵ Ibid.

Exhibit 1. FOIA Modification and Security Coordination at the State Commissions

State	State FOIA Modification For Energy CI ?	State Commission Security Coordinator Designated ?
Alabama	No	No
Arizona	Yes	Yes
Arkansas	Yes	Yes
Connecticut	Yes	Yes
Delaware	No	No
District of Columbia	No	Yes
Florida	Yes	No
Georgia	Yes	Yes
Hawaii	No	Yes
Illinois	Yes	Yes
Indiana	Yes	No
Iowa	Yes	Yes
Kansas	No Response	Yes
Louisiana	Yes	Yes
Maine	Yes	Yes
Maryland	Yes	Yes
Michigan	Yes	Yes
Mississippi	No	No
Missouri	No	Yes
Montana	No	No
Nebraska	No	No
Nevada	No	No
New Hampshire	Yes	Yes
New Jersey	Yes	Yes
New Mexico	No	No
New York	Yes	Yes
Ohio	Yes	Yes
Oklahoma	Yes	Yes
Oregon	Yes	Yes
Pennsylvania	No	Yes
South Carolina	No	No
Texas	Yes	Yes
Vermont	No	Yes
Washington	Yes	Yes
West Virginia	Yes	Yes

Source: State commission responses to the 2004-2005 NARUC Energy Assurance Inventory by NARUC. See *NARUC Inventory on State Energy Assurance Planning* (Technical Brief No. 7 in this series).

Florida. Section 366.093 (1) and (3)(c) of the commission’s Rules of Practice and Procedure contains a specific exemption for security-related information of both public utility companies and their affiliated companies. The section defines “*Confidential Information*” as “material that has been determined, pursuant to this rule, to be proprietary confidential business information.” “Proprietary confidential business information includes, but is not limited to, *security measures, systems, or procedures.*”

Second, state FOIA exemptions are given to CI information that is exempt under Federal statute or rule. This default approach provides consistency with federal agencies, and allows for exemptions to be granted without the state commission having to make a determination on the criticality of the information. Examples include:

Arizona. In 2003, A.R.S. § 39-126 was added to Arizona’s public records title to address non-disclosure of infrastructure risk assessments of a risk assessment that is performed by or on behalf of a federal agency to evaluate *critical energy, water or telecommunications infrastructure to determine its vulnerability to sabotage or attack*

Georgia. Georgia has an exemption for confidential federal records and, more specifically to the public utility sector, exemptions for critical infrastructure information at O.C.G.A. 50-18-72. Section 72 (a) (1) provides “that public disclosure shall not be required for records that are specifically required by the federal government to be kept confidential.”

Indiana. IC 5-14-3-4 which was amended by P.L.173-2003, SEC.5 and provides that public records may not be disclosed by a public agency if declared confidential by (1) *state statute*, (2) *rule adopted by a public Agency* under specific authority to classify public records as confidential or (3) by *federal law*.

Third, notwithstanding protection offered under categories (1) and (2) above, states have also passed “generic” exemptions for information disclosure related to general vulnerabilities or threats. In this case, no specific utility sector is specified. In such an approach, CI information relating to the vulnerability of any regulated utility under state commission jurisdiction could be exempted. Examples include:

Maine. Section 1311-B provides that “If the Commission, on its own motion or on petition of any person or entity, determines that public access to specific information about *public utility technical operations in the State* could compromise the *security* of public utility systems to the detriment of the public interest, the commission shall issue an order designating that information as confidential. *Information designated as confidential pursuant to this section may include, but is not limited to, emergency response plans and network diagrams.* Information designated as confidential under this section is not a public record.”

Michigan. Michigan amended their State FOIA law in March 2002 to exempt a range of utility and security-related information from disclosure. Section 13 (1) (y) (MCL 15.243) protects “Records or information of measures designed to protect the security or safety of persons or property, whether public or private, including, but not limited to, building, *public works, and public water supply designs to the extent that those designs relate to the ongoing security measures of a public body, ... emergency response plans, risk planning documents, threat assessments, and domestic preparedness strategies...*”

West Virginia. Section 29B-1-4 (a) (10) of the West Virginia Code provides for security-related exemptions including “those portions of records containing specific or unique *vulnerability assessments* or specific or unique *response plans, data, databases, and inventories of goods or materials collected or assembled to respond to terrorist acts; and communication codes or deployment plans of law enforcement or emergency response personnel.*” Paragraph (14) also protects “security or disaster recovery plans, risk assessments, tests, or the results of those tests.”

Four, protection and exemptions are provided for each utility sector directly under State FOIA exclusive of federal exemptions. Based a review of select states participating in the NARUC Energy Assurance Inventory²⁵, the data suggests that State FOIA exemptions are becoming increasingly more specific and detailed. In addition, certain states have mirrored federal rules which automatically classify CI information as protected. Such information can be disclosed upon specific action or order of the commission. Coupled with the other categories of exemptions above, such rules provide for the greatest protection of CI information while also protecting the public’s right-to-know. Examples include:

Arizona. Concerning energy infrastructure, Section 40-360.02 requires the filing of plans for transmission and generation facilities, including transmission routes, capacities, capacity factors and power flow and stability analyses. These detailed technical data are protected from disclosure in Section 40-204 which provides for review process in a hearing for disclosing certain information, and also provides for penalties associated with inappropriate disclosure. In contrast to states where a determination is made regarding confidentiality, Arizona has moved to automatically protect information from disclosure. Specifically, paragraph (C) of Section 40-204 states that “*No information furnished to the Commission by a public service corporation, except matters specifically required to be open to public inspection, shall be open to public inspection or made public except on order of the Commission entered after notice to the affected public service corporation, or by the commission or a commissioner in the course of a hearing or proceeding.*”

Indiana. Of the states examined, Indiana’s code contains one of the most detailed descriptions of records exempted from disclosure requirements at IC 5-14-3-4 which was amended by P.L.173-2003, SEC.5. Paragraph (19) exempts “a record or a part of a record, the public disclosure of which would have a reasonable likelihood of threatening public safety by *exposing a vulnerability* to terrorist attack.” These records include:

- “(A) a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under IC 35-47-12-1 or an act of agricultural terrorism under IC 35-47-12-2;
- (B) *vulnerability assessments*;
- (C) *risk planning documents*;
- (D) needs assessments;
- (E) *threat assessments*;
- (F) domestic preparedness strategies;
- (G) *the location of community drinking water wells and surface water intakes*;
- (H) the emergency contact information of emergency responders and volunteers;
- (I) infrastructure records that disclose the configuration of critical systems such as communication, electrical, ventilation, water, and wastewater systems.”

Iowa. All information filed with Iowa Homeland Security and Emergency Management Division can be deemed vital to security and shielded from the Iowa Open Records law. However, most Board records are not protected. Therefore, the Board has adopted a policy of not collecting security type information in writing. Notwithstanding the inability of the Board to exempt disclosure of certain CI information, Section 22, Paragraphs 45 and 46 of the Iowa Code provide a detailed listing of *publicly-owned infrastructure* which is afforded confidentiality. Iowa also automatically protects CI information keeping certain records “confidential, unless otherwise ordered by a court, by the lawful custodian of the records, or by another person duly authorized to release such information.”

Paragraph 46 provides for a mechanism to share CI information as long as the need is associated with *emergency planning or response*. As contained in FERC Order No. 630, state and local governments are recognized as having reasonable “right-to-know” CI information. Specifically, “*The homeland security and emergency management division may provide all or part of the critical asset plan to federal, state, or local governmental agencies which have emergency planning or response functions if the administrator is satisfied that the need to know and intended use are reasonable*. An agency receiving critical asset protection plan information from the division shall not disseminate the information without prior approval of the administrator.”

Maine. Section 1311-B mirrors a number of the disclosure rules found in the DHS Interim Rule. In particular, similarities are found regarding notification of the person submitting the information, release of information to other

agencies, and subsequent release of the information by the agency receiving the information from the commission.

The section also provides for sharing CI information with other State agencies in Maine. The section states that “The Commission may release information designated as confidential ...or require the release of that information by a public utility to another state agency to the extent necessary to support emergency preparedness or response, law enforcement or other public health and safety activities.” However, “*The Commission shall consult with a public utility before releasing or requiring the release of confidential information about that utility to a state agency unless the Commission determines that the public health and welfare require immediate release without such consultation.*” Lastly, the documents received from the commission must be returned “to the Commission or the public utility, as appropriate.”

New Jersey. A proposed new rule in New Jersey (N.J.A.C. 13:1F-1.4) is the most comprehensive rulemaking in any of the seventeen states responding to the NARUC Inventory on Energy Assurance Planning²⁵. The purpose of the proposed new rule is “to establish standards for use at all levels of government for determining questions of access to a government record on a record specific and/or request specific basis where there is a bona fide security concern”. N.J.A.C. 13:1F-1.4 provides for automatic exemptions as “categories of records which will be deemed confidential and not subject to public access” in order to “protect and defend the State and its citizens against acts of sabotage or terrorism, or which, if disclosed, would materially increase the risk or consequences of potential acts of sabotage or terrorism.”

The rule includes an exclusion for “critical infrastructure, government-owned or operated buildings,... public utilities, emergency response facilities,...where disclosure would substantially interfere with the State’s ability to protect and defend the State and its citizens against acts of sabotage or terrorism, or where disclosure would materially increase the risk or consequence of such acts.”

The rule also provides specific exemptions for ... “any records regarding the infrastructure and security of computer and *telecommunication networks* consisting of security passwords, security access codes, security recovery plans, security risk assessments and security test results.” Further, “records of *public utilities and municipal utilities* authorities including but not limited to *energy, telecommunications, water and sewage networks, and records of other entities with energy generation, production, distribution, transmission or storage facilities in the State, or entities with transportation lines or facilities?*” are protected as are “*overlay or analysis generated using GIS for the purpose of evaluating or securing the State’s critical infrastructure...*”

Importantly, the public’s right-to-know is protected in the rule if “there is a bona fide need for public access to the records as long as “appropriate limitations or conditions upon such authorized disclosure. Appropriate limitations or conditions may include, but are not limited to, redacting certain information, establishing controlled conditions for access to the records or permitting

inspection or examination and as appropriate and agreed to by the state agency the copying of the records.”

Oregon. Oregon exemptions for the disclosure of CI and security related information enumerates specific utility sectors and processes (generation, storage and conveyance) in Oregon Revised Statutes Section 195.502 (32) covers CI information relating to the security of “*generation, storage or conveyance of electricity; gas in liquefied or gaseous form... petroleum products, sewage, water, telecommunication systems, including cellular, wireless or radio systems, and data transmissions* by whatever means provided.”

CI INFORMATION SHARING PROTOCOLS

Since September 11, 2001, substantial resources and efforts have been expended by federal, state and local governments, as well as the private sector, developing processes and rules to reduce the vulnerability of Nation’s CI. Protection of CI Information from unjustified public disclosure represents one the most important and challenging regulatory issues facing state commissions. The review of the federal and state efforts presented in this paper suggests that programmatic inefficiencies and inconsistencies in developing CI information disclosure rules and procedures. This is most probably a direct result of the complexity of the issue, the numerous jurisdictions involved and the “uncharted” character of the problem.

Therefore, given the inconsistencies between the DHS Interim Rule and FERC Order No.630, and subsequent amendments, what administrative or legal procedures should state commissions consider to efficiently share and utilize CI information with these agencies and other state commissions? Additionally, what protocols should state commissions consider to efficiently and effectively harmonize public utility regulation given the diversity of State rules on disclosure of critical infrastructure information?

The suggested information management protocols for state commissions address:

- Implementation of State FOIA Exemption Rules
- Designation of a Security Information Coordinator
- Cooperative Efforts with FERC and DHS
- Coordination with Non-Governmental Organizations

IMPLEMENTATION OF STATE FOIA EXEMPTION RULES

State Commissions should seek to implement forward-looking FOIA Exemption Rules which properly address broad utility sectors and associated processes.

The review of state FOIA exemptions reveals considerable variability in state approaches to the problem. Certain states retain a traditional regulatory non-disclosure approach such as a Commission's Rules of Practice and Procedure placing CI in the same category as business information. Others provide exemptions if federal statutes exempting disclosure, and others such as Arizona, Indiana and New Jersey have detailed categories of exemptions.

While state and even regional differences in FOIA exemptions are acceptable, a need clearly exists to improve upon the enumeration of categories and CI information sharing processes in these rules. Therefore, state commissions should seek to implement forward-looking FOIA Exemption Rules which properly address broad utility sectors and associated processes. This can be accomplished by working with state legislatures and also in state commissions' rules of practice and procedure. To facilitate this process, NARUC should develop a Model FOIA Exemption Rule in collaboration with other state-based organizations. These could include the National Governors Association, the National Conference of State Legislatures, and the National Association of State Energy Offices, among others. At a minimum, the FOIA Exemption Rule should:

1. Provide for automatic protection of CI information conforming to a predetermined criteria or categorization. CI information could be released following an examination of the need and reasonableness of the request.
2. The State FOIA and/or rules of practice and procedure should include multiple methods or categories of protection such as traditional non-disclosure capabilities, exemption of CI information exempted under federal statute or rule, and explicit, detailed exemptions for individual public utility sectors and processes.
3. Explicitly enumerate individual public utility sectors to avoid any confusion over exemptions, including a consideration of the interdependencies within the sectors.
4. Explicitly define and include utility-related processes and their associated analytical elements including, but not limited to, long and short term planning, vulnerability analysis, normal and emergency operations, network analysis or geographic system mapping and analysis.
5. Define the role of state commissions in collecting, storing, managing and distributing public utility CI information. Data distribution should not only include static [historical] data but also dynamic data generated during emergency events or utility outages.

6. Develop a consistent state process to facilitate access to CI information, including appropriate disclosure protections between intrastate agencies concerned with CI. In addition, the process should address CI information sharing among state commissions for CI information that is regional in scope. This process would be directly applicable to electric transmission, natural gas pipeline systems, regional phone networks and regional water and wastewater systems.
7. Model non-disclosure agreement (NDA) templates should also be examined under the presumption that such standardization would encourage both FERC and DHS to distribute CI information to state commissions working on regional CI issues. A number of state FOIA exemptions already include provisions for data exchange, sharing and return of the CI information once released which could be used for this purpose.
8. Provide for penalties for any person or entity that releases protected CI information.

DESIGNATION OF A SECURITY INFORMATION COORDINATOR

State commissions and/or regional state committees should appoint a security information coordinator to manage CI information.

State commissions and/or regional state committees should appoint a security information coordinator and an inter-sector utility team to manage CI information. As referenced earlier within this report, at least twenty-two state commissions have designated a staff member to act as a security coordinator. This position could also be responsible for managing CI information. Designation of such a position is important for two reasons. First, the coordinator could represent the state commission(s) in cooperative efforts with State Homeland Security, State Emergency Management Agency and/or the Governor's Office.

Second, the coordinator's position provides a mechanism for implementation of DHS's State Protected CII Officer concept while also providing a standard or known point of contact with the FERC on CEII requests. Additionally, state commissions should seek funding from DHS to facilitate the implementation and ongoing training of State Protected CII Officers.

As an example, state commission staff serving as Energy Emergency Assurance Coordinators (EEAC) would become part of an inter-sector utility team to manage CI information. The EEAC System was officially launched in February 2004 and serves as a communications network for key State personnel to exchange information and coordinate with each other and the DOE during energy emergencies. The EEAC is currently comprised of about 150 personnel involved with energy markets and operations at the state level.

Lastly, in a similar manner to the Maine Commission's FOIA responsibilities, all state commissions should be assigned the responsibility of examining the need to distribute CI information pertaining to jurisdictional utilities. State commissions should become the [default] expert on energy, telecommunications and investor-owned water and wastewater utilities.

COOPERATIVE EFFORTS WITH FERC AND DHS

State commissions, regional state committees, NARUC, or NARUC-affiliated regional associations should initiate the development of memorandum of understanding, or other appropriate instrument, with the FERC and DHS regarding CI information sharing.

Federal Energy Regulatory Commission

As discussed in paragraph 51 of FERC Order No. 630 the FERC emphasized that "its goal is to cooperate as fully as possible with the State Commissions" ... "to ensure that CEII does not get into the wrong hands." The FERC also recognized that the CEII provided to FERC is "similar or identical information" that is provided to state commissions.³⁶ Importantly, in paragraph 53, FERC acknowledged that "State Commissions will be presumed to have a need to know information within their state involving issues within their responsibilities" and further, that state commissions "may submit requests for information regarding entities outside of their jurisdictions with an explanation of the need." However, FERC emphasized that the "release of CEII to State Commissions and other State Agencies will normally be subject to signing an NDA."³⁷

Given these presumptions, state commissions, regional state committees, NARUC, or NARUC-affiliated regional associations, commissioners should initiate the development of a memorandum of understanding, or other appropriate instrument, with the FERC regarding sharing of CEII. Notwithstanding the simplicity of the FERC CEII Request Form found in Appendix A, the designated state commission Security Coordinator could be "registered" with the FERC to avoid the repetitive task of providing the requestor's information. Changes in the person holding the security coordinators' position would be reported to FERC. With such a change in procedure, emphasis could be placed on a description of information requested and on the statement explaining need and intended use of the information. For state commission docketed matters, the docket number and/or case name could be used to justify the need and intended use of the CEII. Such information could ultimately be utilized to "track" or create a chain of possession" of the disclosed CEII either by FERC or the state commission. Because state commission docket numbers can be referenced to some "jurisdictional matter", this would also assist in

³⁶ FERC Order No. 630, p. 43.

³⁷ Ibid.

standardizing the agreed upon “right to know” of the state commission. It is believed that such a modification would reduce the “Public Reporting Burden”. Refer to the bottom of the FERC CEII Request Form.

Department of Homeland Security

Unlike FERC Order No. 630, the DHS Interim Rule does not contain a similar “right to know” provision. As discussed earlier in this paper, an oversight mechanism to [implicitly] improve information access by state commissions can be found in Section 29.4 (c) of the DHS Interim Rule. The Protected CII Program Manager is to establish procedures to ensure that any DHS component or other Federal, State, or local entity that works with Protected CII appoints one or more employees to serve as a Protected CII Officer. Persons appointed to these positions are to be fully familiar with these procedures. A major objective of the Protected CII program Manager is to “ensure the expeditious and secure sharing of Protected CII with federal, state and local agencies.”

State commissions, regional state committees, NARUC, or NARUC-affiliated regional associations should initiate the development of a memorandum of understanding, or other appropriate instrument, with the DHS regarding sharing of CII to include the following elements:

1. State commissions should seek for DHS to recognize the “right to know” on the part of state commissions regarding CI information. As referenced above, a template is already available in the Iowa FOIA. Refer to page 25 of this report.
2. Consistent with NARUC’s comments on the DHS Proposed Rule on Handling Critical Infrastructure Information, state commission jurisdictional responsibilities including, but not limited to, certification hearings, general rate hearings, security-related cost recovery hearings, siting, and reliability and vulnerability assessments should be included in the DHS definition of CII. To that end, state statutes and/or regulations could be amended to explicitly include certain state commission proceedings, or portions of those proceedings, as meeting the definition of “critical infrastructure” as defined by federal rule or statute. Such a provision would be analogous to State FOIA exemptions for CI information exempted by federal statute or rule.
3. As proposed under the FERC section above, the designated state commission security coordinator could also serve as the State Protected CII Officer. Establishment of a designated liaison between state commissions and/or regional state committees would formalize the process of information sharing.

4. Consistent with Section 29.4 (b) (3) and (4) of the DHS Interim Rule, “to facilitate the expeditious and secure sharing” of CII with state entities and to promote the training of State Protected CII Officers (state commission security coordinators) State commissions should seek funding from DHS to facilitate the implementation and ongoing training of State Protected CII Officers.

COORDINATION WITH NON-GOVERNMENTAL ORGANIZATIONS

State Commissions, regional state committees, NARUC, or NARUC-affiliated regional associations should initiate the development of a memorandum of understanding, or other appropriate instrument, with NERC regarding CI information sharing.

During the past two years, the [North American Electric Reliability Council](#) (NERC) and a broad coalition of industry, state, and consumer organizations have promoted federal legislation that would create a self-regulatory electric reliability organization (ERO) to develop and enforce compliance with mandatory reliability rules. The legislation creates of an ERO that spans North America, with FERC oversight in the United States, and which expressly protects the important roles of the states and regional entities.³⁸ In preparation for the potential passage of the legislation, Version 0 of the reliability standards were approved by NERC in January 2005.

NERC continues to strive for the appropriate inclusion of regulatory entities in its process. For example, in June 2003, NERC published the findings of the Resource and Transmission Adequacy Task Force (RTATF) investigation of NERC’s role in resource adequacy and transmission adequacy determinations of the North American interconnected bulk electric systems.³⁹ The report presented a number of resource and transmission adequacy recommendations that NERC should initiate to enhance the reliability (adequacy) of the interconnected bulk electric systems. The Report recommended that

NERC and the Regions should encourage greater regulatory (state/province commissions and multi-state/province commissions) and stakeholder participation throughout the resource planning and assessment processes to help ensure informed resource adequacy decisions.

These planning and assessment processes contain detailed regional analyses of reserve and capacity margins, loss of load expectations and transmission power

³⁸ The North American Electric Reliability Council, www.nerc.com/about/legislation.html.

³⁹ The North American Electric Reliability Council Planning Committee, Resource and Transmission Adequacy Task Force, “Resource and Transmission Adequacy Recommendations” (June 15, 2004).

flow analysis to verify that resources identified by load serving entities to meet resource adequacy requirements are simultaneously deliverable to the LSEs' loads. Under the current FERC, DHS and State FOIA exemption rules, much of this information could be considered protected CI information. In certain situations and depending upon the level of participation by state commissions as recommended in the RTATF Report, CI information disclosure concerns could arise.

Therefore, state commissions, regional state committees, NARUC, or NARUC-affiliated regional associations should initiate the development of a memorandum of understanding, or other appropriate instrument, with NERC regarding CI information sharing. Assuming the passage of some form of federal reliability legislation, state commissions could have a need to review various information developed and maintained by NERC or the NERC Regions. This review could occur in undocketed meetings implementing the RTATF Report recommendation, or under certain scenarios, state commissions could potentially have jurisdiction regarding compliance with subsequent versions of the NERC (or ERO) reliability standards. Docketed hearings would require access to resource and transmission assessments and analyses not only from in-state jurisdictional utilities, but also potentially from out-of-state non-jurisdictional utilities. NERC and NERC Regional assessments, and the underlying analyses supporting these assessments, would be required to adequately evaluate electric system reliability and any associated cost-recovery.

COMMISSION PROCEDURES FOR PROTECTING SENSITIVE INFORMATION

In addition to protocols regarding sharing of CI information and strong FOIA exemptions to protect it, the state public utility commissions can implement a number of additional procedures to ensure that sensitive information legally and physically protected and properly handled.⁴⁰

The procedures for CI information management should be defined in writing, ideally before taking possession of the information, and these protocols should be known, understood and followed by all parties having access to the information. Proper procedures will provide assurances to utilities that the information they share in confidence will be protected and handled appropriately by regulators. Specifically, commissions developing CI information procedures will want to consider the following.

1. The commissions should clearly define and state the legal authority that will be used to protect the information from disclosure. As discussed in this

⁴⁰ This section was prepared by J. Pillon for the NARUC Ad Hoc Committee on Critical Infrastructure.

paper, this assurance can be provided through an exemption from disclosure under the state's FOIA or Sunshine laws. Other state or federal legal authority may be applicable and used to protect the information. Some FOIA laws exempt from disclosure information that is already exempted by other statutes which could include state or federal laws. If this is the case, and the information is confidential under federal law, then it may be exempt by extension under state law. Protective orders under administrative rules may be another option. If the information is very sensitive, multiple provisions might be cited.

2. Procedures and practices should reinforce the importance of not overreaching by trying to protect information that may not fall within an existing exemption. These provisions should not be used as a means of withholding information that legitimately falls within the public domain. Many FOIA laws have exemptions which require that information meet the test of whether the public good of disclosure outweighs the public good of withholding the information. This means that withholding the information could be challenged in the courts and one needs to be sure that there is sufficient legal foundation to protect the information.
3. Parties and the commission should ensure that information is dated and labeled as sensitive in a header or footer on each page. For information not developed by the agency, a stamp could be used for this purpose. For example: "Exempt from FOIA Disclosure," "Homeland Security Sensitive," "Law Enforcement Sensitive," or "For Official Use Only." Use of these labels should correspond with the state or federal legal authority used to protect the information. In addition, it may be useful at the beginning of the document to include a full reference to the authority being used to protect the information.
4. Parties must be aware that information that is already in the public domain may not be subject to protection. However, not all information should necessarily be readily accessible. Web sites provide a good example. Just because information is already in the public domain does not mean that it should be posted on a website which is accessible continuously from anywhere in the world. If someone needs to specifically request a piece of information, some discretion can be exercised over the type of individual or organization the information is provided to.
5. Commission procedures should specify clearly who within the organization is allowed access to the information and for what reasons access is provided. This access should be limited to those that have a real need to know and that can take action based on the information. Some individuals may want access just for informational purposes without a real need to know. It would be preferable not to share sensitive information with those individuals who have nothing more than a general interest in seeing it. The

same is true of individuals who have management responsibilities. Just because the information may be within their management purview does not necessarily mean that they should have access to the information. The fewer people that have access the better.

6. Commission procedures should ensure that the information is kept in a secure location when not otherwise in use. When in use it should always be within the sight or possession of the individual using it. Materials should not be left on a desk when an office is not occupied. A locked file cabinet, locked room, or a safe should be used for storage. Again, the individuals that have access to the keys or combination should be limited and the physical location of the information only known by those individuals.

7. Commission procedures should ensure that information stored on digital media should not be stored within a computer network, on a computer hard drive or in an online system. Storage should be on removable media such as a floppy disk, CD, or USB drive. This media should be kept in the secured location. While not recommended, if for some reason the information is stored on a computer or network, very good cyber security should be employed and tested regularly.

8. Commission procedures should clarify the conditions and manner by which information is held and shared by the public utility commission and the state's homeland security office.

9. As discussed throughout this paper, sharing information with the federal government may be governed by federal procedures such as the DHS Interim Rule or the FERC CEII procedures. State commissions must follow these federally defined procedures and ensure that any additional procedures for handling sensitive information at the state level are consistent with the rules.

APPENDIX A: FERC CEII REQUEST FORM

CEII REQUEST FORM Submit form to CEII Coordinator 888 First Street, NE Washington, DC 20426 Or via facsimile at 202-208-2106	
REQUESTER'S INFORMATION	EMPLOYER/CLIENT INFORMATION
Requester's name & title:	Name of entity on whose behalf request is filed:
Any other names, e.g., maiden name, used by requester and dates used:	Address of entity listed above:
Requester's address:	Phone number of entity listed above:
Requester's phone number:	
Requester's date of birth:*	
Requester's place of birth:*	
Requester's social security number (optional):*	
Description of information requested:	
Statement explaining need and intended use of the information:	
Are you willing to sign and abide by an appropriate agreement limiting your use and disclosure of the information requested? Yes <input type="checkbox"/> No <input type="checkbox"/>	
Signature:	Date:
* This information is not required from requesters filing requests on behalf of a Federal agency.	

Where to Send Comments on Public Reporting Burden:

The public reporting burden for this collection of information is estimated to average 15 minutes per response including the time for reviewing instructions, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any aspect of this collection, including suggestions for reducing this burden to the Federal Energy Regulatory Commission, 888 First St., NE, Washington, DC 20426 (Attn: Mr. Michael Miller) and to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503 (Attn: Desk Officer for the Federal Energy Regulatory Commission).

APPENDIX B: Selected State FOIA Exemptions⁴¹

ARIZONA

In 2003, a statute (A.R.S. § 39-126) was added to Arizona's public records title to address non-disclosure of infrastructure risk assessments done by or on behalf of a federal agency. The section states

Section 39-126. Federal risk assessments of infrastructure; confidentiality

Nothing in this chapter requires the disclosure of a risk assessment that is performed by or on behalf of a federal agency to evaluate *critical energy, water or telecommunications infrastructure to determine its vulnerability to sabotage or attack.*

In addition, Section 40-360.02 requires the filing of plans for transmission and generation facilities, including transmission routes, capacities, capacity factors and power flow and stability analyses. These detailed technical data are protected from disclosure in paragraph D

Section 40-360.02. Plans; filing; failure to comply; classification

D. The information in the plan reported to the commission in subsection B of this section is not open to public inspection and shall not be made public if disclosure of the information in the plan could give a material advantage to competitors. The information in the plan protected as *confidential* under subsection B of this section is any information that is similar to the information that would be *confidential* under section 40-204. An officer or employee of the commission who knowingly divulges information in the plan in violation of this subsection is guilty of a class 2 misdemeanor.

Regarding general reporting to the commission, Section 40-204 provides for review process in a hearing for disclosing certain information, and also provides for penalties associated with inappropriate disclosure

Section 40-204. *Reports by public service corporations to commission; duty of corporation to deliver documents to commission; confidential nature of information furnished; exception; classification.*

A. Every public service corporation shall furnish to the commission, in the form and detail the commission prescribes, tabulations, computations, annual reports, monthly or periodical

⁴¹ Emphasis added.

reports of earnings and expenses, and all other information required by it to carry into effect the provisions of this title and shall make specific answers to all questions submitted by the commission. If a corporation is unable to answer any question, it shall give a good and sufficient reason therefore.

B. When required by the commission, a public service corporation shall deliver to the commission copies of any maps, profiles, contracts, franchises, books, papers and records in its possession, or in any way relating to its property or affecting its business, and also a complete inventory of all its property in the form the commission directs.

C. No information furnished to the commission by a public service corporation, except matters specifically required to be open to public inspection, shall be open to public inspection or made public except on order of the commission entered after notice to the affected public service corporation, or by the commission or a commissioner in the course of a hearing or proceeding.

D. Any officer or employee of the commission who knowingly divulges any such information is guilty of a class 2 misdemeanor.

FLORIDA

Section 366.093 (1) and (3)(c) of the commission's Rules of Practice and Procedure contains a specific exemption for security-related information of both public utility companies and their affiliated companies. Specifically,

RULES OF THE FLORIDA PUBLIC SERVICE COMMISSION, CHAPTER 25-22, RULES GOVERNING PRACTICE AND PROCEDURES, PART I -GENERAL PROVISIONS

25-22.006 Confidential Information.

(1) Definitions.

(a) "*Confidential Information*" means material that has been determined, pursuant to this rule, to be proprietary confidential business information under Section 350.121, 364.183, 366.093, or 367.156, F.S.

366.093 Public utility records; confidentiality.—

(1) The commission shall continue to have reasonable access to all public utility records and records of the utility's affiliated companies, including its parent company, regarding transactions or cost allocations among the utility and such affiliated companies, and such records necessary to ensure that a utility's

ratepayers do not subsidize nonutility activities. Upon request of the public utility or other person, any records received by the commission which are shown and found by the commission to be *proprietary confidential business information shall be kept confidential and shall be exempt* from Section. [119.07](#) (1).

(3) Proprietary confidential business information means information, regardless of form or characteristics, which is owned or controlled by the person or company, is intended to be and is treated by the person or company as private in that the disclosure of the information would cause harm to the ratepayers or the person's or company's business operations, and has not been disclosed unless disclosed pursuant to a statutory provision, an order of a court or administrative body, or private agreement that provides that the information will not be released to the public. Proprietary confidential business information includes, but is not limited to:

(c) *Security measures, systems, or procedures.*

GEORGIA

Georgia has an exemption for confidential federal records and, more specifically to the public utility sector, exemptions for critical infrastructure information at O.C.G.A. 50-18-72. Section 72 (a) (1) provides

- (a) Public disclosure shall not be required for records that are:
- (1) Specifically required by the federal government to be kept confidential;

And Section 72 (a) (15) provides

(15)(A) Records, the disclosure of which would compromise security against sabotage or criminal or terrorist acts and the nondisclosure of which is necessary for the protection of life, safety, or public property, which shall be limited to the following:

(i) *Security plans and vulnerability assessments for any public utility, technology infrastructure, building, facility, function, or activity in effect at the time of the request for disclosure or pertaining to a plan or assessment in effect at such time;*

(ii) Any plan for protection against terrorist or other attacks, which plan depends for its effectiveness in whole or in part upon a lack of general public knowledge of its details;

(iii) Any document relating to the existence, nature, location, or

function of security devices designed to protect against terrorist or other attacks, which devices depend for their effectiveness in whole or in part upon a lack of general public knowledge; and

(iv) Any plan, blueprint, or other material which if made public could compromise security against sabotage, criminal, or terroristic acts.

INDIANA

Of the states examined, Indiana's code contains one of the most detailed descriptions of records excepted from disclosure requirements at IC 5-14-3-4 which was amended by P.L.173-2003, SEC.5. The section reads

Sec. 4. (a) The following public records are excepted from section 3 of this chapter and may not be disclosed by a public agency, unless access to the records is specifically required by a state or federal statute or is ordered by a court under the rules of discovery:

- (1) Those declared confidential by *state statute*.
- (2) Those declared confidential by *rule adopted by a public Agency* under specific authority to classify public records as confidential granted to the public agency by statute.
- (3) Those required to be kept confidential by *federal law*.

Paragraph (19) contains the specific reference to records and reads

(19) A record or a part of a record, the public disclosure of which would have a reasonable likelihood of threatening public safety by *exposing a vulnerability* to terrorist attack. A record described under this subdivision includes:

(A) a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under IC 35-47-12-1 or an act of agricultural terrorism under IC 35-

47-12-2;

(B) *vulnerability assessments*;

(C) *risk planning documents*;

(D) needs assessments;

(E) *threat assessments*;

(F) domestic preparedness strategies;

(G) *the location of community drinking water wells and surface water intakes*;

(H) the emergency contact information of emergency responders and volunteers;

(I) *infrastructure records that disclose the configuration of critical systems such as communication, electrical, ventilation, water, and wastewater*

systems; and

This subdivision does not apply to a record or portion of a record pertaining to a location or structure owned or protected by a public agency in the event that an act of terrorism under IC 35-47-12-1 or an act of agricultural terrorism under IC 35-47-12-2 has occurred at that location or structure, *unless release of the record or portion of the record would have a reasonable likelihood of threatening public safety by exposing a vulnerability of other locations or structures to terrorist attack.*

IOWA

All information filed with Iowa Homeland Security and Emergency Management Division (HLSEM) can be deemed vital to security and shielded from the Iowa Open Records law. However, most Board records are not protected. Therefore, the Board has adopted a policy of not collecting security type information in writing. Notwithstanding the inability of the Board to exempt disclosure of certain CI information, Section 22, Paragraphs 45 and 46 of the Iowa Code provide a detailed listing of publicly-owned infrastructure which is afforded confidentiality. Section 22 reads

SUBTITLE 9 RESTRAINTS ON GOVERNMENT
Section 22 EXAMINATION OF PUBLIC RECORDS (OPEN RECORDS) Section 22.7 Confidential records.

The following public records shall be kept confidential, unless otherwise ordered by a court, by the lawful custodian of the records, or by another person duly authorized to release such information:

45. Records of a public airport, municipal corporation, *municipal utility, jointly owned municipal utility, or rural water district organized under chapter 357A, where disclosure could reasonably be expected to jeopardize the security or the public health and safety of the citizens* served by a public airport, municipal corporation, municipal utility, jointly owned municipal utility, or rural water district organized under chapter 357A. Such records include but are not limited to *vulnerability assessments and information included within such vulnerability assessments; architectural, engineering, or construction diagrams; drawings, plans, or records pertaining to security measures such as security and response plans, security codes and combinations, passwords, passes, keys, or security or response procedures; emergency response protocols; and records disclosing the configuration of critical systems or infrastructures* of a public airport, municipal corporation, municipal utility, jointly owned municipal utility, or rural water district organized under chapter 357A. This subsection is repealed effective June 30, 2007.

46. The critical asset protection plan or any part of the plan prepared pursuant to section 29C.8 and any information held by the homeland security and emergency management division that was supplied to the division by a public or private agency or organization and used in the development of the critical asset protection plan to include, but not be limited to, surveys, lists, maps, or photographs. However, the administrator shall make the list of assets available for examination by any person. A person wishing to examine the list of assets shall make a written request to the administrator on a form approved by the administrator. The list of assets may be viewed at the division's offices during normal working hours. The list of assets shall not be copied in any manner. Communications and asset information not required by law, rule, or procedure that are provided to the administrator by persons outside of government and for which the administrator has signed a nondisclosure agreement are exempt from public disclosures. *The homeland security and emergency management division may provide all or part of the critical asset plan to federal, state, or local governmental agencies which have emergency planning or response functions if the administrator is satisfied that the need to know and intended use are reasonable.* An agency receiving critical asset protection plan information from the division shall not disseminate the information without prior approval of the administrator.

MAINE

Section 1311-B mirrors a number of the disclosure rules found in the DHS Interim Rule. In particular, similarities are found regarding notification of the person submitting the information, release of information to other agencies, and subsequent release of the information by the agency receiving the information from the commission. The section also provides for specific protection of public utility information and states

§1311-B. Security of certain utility information

1. Designation of information as confidential. If the commission, on its own motion or on petition of any person or entity, determines that public access to specific information about *public utility technical operations in the State* could compromise the security of public utility systems to the detriment of the public interest, the commission shall issue an order designating that information as confidential. *Information designated as confidential pursuant to this section may include, but is not limited to, emergency response plans and network diagrams.* Information designated as confidential under this section is not a public record under Title 1, section 402, subsection 3. [2001, c. 135, §1 (new).]

2. Treatment of information by commission; generally. Except as otherwise provided in this section, the commission may not release information designated as confidential under subsection 1 and shall take appropriate steps to protect such information in its possession. [2001, c. 135, §1 (new).]
3. Access to information by parties in proceeding. Designation of information as confidential under subsection (1) does not limit the right of a party in a proceeding before the commission to obtain discovery of that information. Notwithstanding section 1311-A, subsection 1, paragraphs A and C, *the commission may issue a protective order limiting discovery of information designated as confidential pursuant to subsection 1 if the commission finds that specific limits are necessary to protect the public interest.* [2001, c. 135, §1 (new).]
4. Release of information to other state agencies. The commission may release information designated as confidential pursuant to subsection 1 or require the release of that information by a public utility to another state agency to the extent necessary to support emergency preparedness or response, law enforcement or other public health and safety activities. *The commission shall consult with a public utility before releasing or requiring the release of confidential information about that utility to a state agency unless the commission determines that the public health and welfare require immediate release without such consultation.* The commission shall notify a public utility within 2 business days of providing information about that utility to a state agency pursuant to this subsection. As soon as practicable after receiving notice from a state agency pursuant to subsection 5, paragraph B of the agency's intent to release the information, the commission shall notify the public utility of the agency's intent. [2001, c. 135, §1 (new).]
5. Release by other state agencies. A state agency that receives information about a public utility pursuant to subsection 4:
[2001, c. 135, §1 (new).]
 - A. *May not use that information for any purpose other than for the support of emergency preparedness or response, law enforcement or other public health and safety activities;*
[2001, c. 135, §1 (new).]
 - B. May not release that information to any other person or entity without prior notice to the commission unless the agency determines that immediate release of the information to one or more persons or entities is

necessary for the protection of public health and safety;
and
[2001, c. 135, §1 (new).]

C. Shall, when finished with the use of any documents received from the commission or from a public utility pursuant to subsection 4, return the documents to the commission or the public utility, as appropriate.
[2001, c. 135, §1 (new).]

MICHIGAN

Michigan amended their State FOIA law in March 2002 to exempt a range of utility and security-related information from disclosure. Section 13 (1) (y) (MCL 15.243) states

“Records or information of measures designed to protect the security or safety of persons or property, whether public or private, including, but not limited to, building, *public works*, and *public water supply designs to the extent that those designs relate to the ongoing security measures of a public body*, capabilities and plans for responding to a violation of the Michigan anti-terrorism act, chapter LXXXIII-A of the Michigan penal code, 1931 PA 328, MCL 750.543 to 750.543z, *emergency response plans, risk planning documents, threat assessments, and domestic preparedness strategies*, unless disclosure would not impair a public body’s ability to protect the security or safety of persons or property or unless the public interest in disclosure outweighs the public interest in nondisclosure in the particular instance.”

NEW JERSEY

A proposed new rule in New Jersey (N.J.A.C. 13:1F-1.4) is the most comprehensive rulemaking in any of the seventeen states responding to the NARUC Inventory on Energy Assurance Planning. The purpose of the proposed new rule is “to establish standards for use at all levels of government for determining questions of access to a government record on a record specific and/or request specific basis where there is a bona fide security concern”. N.J.A.C. 13:1F-1.4 identifies “categories of records which will be deemed confidential and not subject to public access” in order to “protect and defend the State and its citizens against acts of sabotage or terrorism, or which, if disclosed, would materially increase the risk or consequences of potential acts of sabotage or terrorism.”

Highlights of the rule include:

Paragraph 1 includes an exclusion for “critical infrastructure, government-owned or operated buildings,... public utilities, emergency response facilities,... where disclosure would substantially interfere with the State’s ability to protect and defend the State and its citizens against acts of sabotage or terrorism, or where disclosure would materially increase the risk or consequence of such acts.”

Paragraph 7 “excludes from public access ... any records regarding the infrastructure and security of computer and telecommunication networks consisting of security passwords, security access codes, security recovery plans, security risk assessments and security test results.”

Sections of the rule relevant to State Public Service Commissions include

LAW AND PUBLIC SAFETY DOMESTIC SECURITY PREPAREDNESS

Access to Records, Proposed New Rules: N.J.A.C. 13:1F.

Authority: N.J.S.A. 47:1A-1, Executive Order No. 9 (Hughes 1963) and Executive Order No. 21 (McGreevey 2002).

13:1F-1.2 Definitions

The words and terms as used in this section shall have the following meaning, unless the context clearly requires otherwise:

“*Critical infrastructure*” means any system or asset, including but not limited to, *communications*, financial, computers, transportation, military, government services, emergency services, *water, waste water, and energy and public utility services*, vital to this State such that the incapacity or destruction of such systems and assets or parts thereof would have an impact on the physical or economic security and public health or safety of any combination of those matters of this State.

13:1F-1.4 Records Exempt from Access

(a) The following records shall not be deemed to be Government Records subject to public access, inspection, examination or copying pursuant to the provisions of N.J.S.A. 47:1A-1, as amended and supplemented, if the inspection, examination or copying of that record would substantially interfere with the State’s ability to protect and defend the State and its citizens against acts of sabotage or terrorism, or which, if disclosed, would materially increase the risk or consequences of potential acts of sabotage or terrorism:

- (1)(a) Records or portions thereof regarding building plans, blueprints, schematic drawings, diagrams, and operational manuals, where disclosure would reveal the specific location of life safety and support systems, load bearing structural elements, surveillance techniques, alarm or security systems or technologies, operational and transportation plans or protocols or personnel deployments;
- b) records of airports, mass transit facilities, bridges, tunnels, *public utilities, municipal utilities authorities;*
- c) *records of critical infrastructure, including but not limited to energy, telecommunications, water and sewage networks, and records of other entities with energy generation, production, distribution, transmission or storage facilities in the State, or entities with transportation lines or facilities;*
- d) emergency response facilities or structures;
- e) buildings where hazardous materials are stored;
- f) arenas and stadiums;
- g) any building or structure owned or operated by the State or any of its political subdivisions

(6) That portion of any *overlay or analysis generated using GIS* for the purpose of evaluating or securing the State's critical infrastructure or domestic security preparedness;

(7) Records or portions thereof regarding the *infrastructure and security of computer and telecommunication networks*, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities;

Notwithstanding the provisions of N.J.A.C. 13:1F-1.4, upon submission to and approval by the Domestic Security Preparedness Task Force, heads of Cabinet-level agencies of State government shall have the authority to allow disclosure of government records, exempt from disclosure under N.J.A.C. 13:1F-1.4(a)(1) through (a)(10), in whole or in part, where the agency head determines that there is a bona fide need for public access to the *records and imposes appropriate limitations or conditions upon such authorized disclosure. Appropriate limitations or conditions may include, but are not limited to, redacting certain information, establishing controlled conditions for access to the records or permitting inspection or examination and as appropriate and agreed to by the state agency the copying of the records.*

OREGON

Oregon exemptions for the disclosure of CI and security related information enumerates specific utility sectors and processes (generation, storage and conveyance) in Oregon Revised Statutes Section 192.502 (32) which provides

192.502. Other public records exempt from disclosure. The following public records are exempt from disclosure under ORS 192.410 to 192.505:

(32) Information about review or approval of programs relating to the security of:

(a) *Generation, storage or conveyance of:*

(A) *Electricity;*

(B) *Gas in liquefied or gaseous form;*

(C) Hazardous substances as defined in ORS 453.005 (7)(a), (b) and (d);

(D) Petroleum products;

(E) *Sewage; or*

(F) *Water.*

(b) *Telecommunication systems*, including cellular, wireless or radio systems.

(c) Data transmissions by whatever means provided.

WEST VIRGINIA

Section 29B-1-4 of the West Virginia Code provides for specific security- related exemptions although energy systems are not explicitly mentioned:

Section 29B-1-4. Exemptions.

(a) The following categories of information are specifically exempt from disclosure under the provisions of this article:

(10) Those portions of records containing specific or unique *vulnerability assessments* or specific or unique *response plans, data, databases*, and inventories of goods or materials collected or assembled to respond to terrorist acts; and communication codes or deployment plans of law enforcement or emergency response personnel;

(13) *Computing, telecommunications and network security records*, passwords, security codes or programs used to respond to or plan against acts of terrorism which may be the subject of a terrorist act;

(14) Security or disaster recovery plans, risk assessments, tests, or the results of those tests;

[blank page]