

Regulatory Analysis Form

This space for use by IRRC

Rec'd 11/21/07
1:31 pm

(1) Agency

Pennsylvania Public Utility Commission

(2) I.D. Number (Governor*s Office Use)

L-00070185/57-256

IRRC Number:

2651

(3) Short Title

Proposed Rulemaking Re: Implementation of the Public Utility Confidential Security Information Disclosure Protection Act

(4) PA Code Cite

52 Pa. Code §§ 102.1-102.4 and 52 Pa. Code § 5.243(g)

(5) Agency Contacts & Telephone Numbers

Primary Contact: Carl S. Hisiro (legal), 717-783-2812

Secondary Contact:

(6) Type of Rulemaking (check one)

- Proposed Rulemaking
 Final Order Adopting Regulation
 Final Order, Proposed Rulemaking Omitted

(7) Is a 120-Day Emergency Certification Attached?

- No
 Yes: By the Attorney General
 Yes: By the Governor

(8) Briefly explain the regulation in clear and nontechnical language.

The proposed regulation creates filing procedures for public utilities to follow when submitting records containing confidential security information to the Commission and procedures to address challenges to a utility's designation of confidential security information or requests to examine records containing confidential security information.

(9) State the statutory authority for the regulation and any relevant state or federal court decisions.

35 P.S. §§ 2141.1-2141.6; 66 Pa.C.S. § 501

Regulatory Analysis Form

(10) Is the regulation mandated by any federal or state law or court order, or federal regulation? If yes, cite the specific law, case or regulation, and any deadlines for action.

Yes. 35 P.S. §§ 2141.1-2141.6. No deadlines are mandated.

(11) Explain the compelling public interest that justifies the regulation. What is the problem it addresses?

The adoption of this proposed regulation will allow the Commission to fulfill its statutory duty to create protocols and procedures to help ensure the safeguarding of confidential security information filed with the Commission from disclosure that could compromise security against sabotage or criminal or terrorist acts.

(12) State the public health, safety, environmental or general welfare risks associated with nonregulation.

Without this regulation, there is an increased risk that otherwise confidential security information could fall into criminal or terrorist hands to the potential detriment of the public health and safety. This concern by the legislature prompted enactment of the Public Utility Confidential Security Information Disclosure Protection Act.

(13) Describe who will benefit from the regulation. (Quantify the benefits as completely as possible and approximate the number of people who will benefit.)

All public utilities that have occasion to file confidential security information with the Commission will benefit by offering a clear means of protecting such information from possible disclosure. All citizens of the Commonwealth will benefit indirectly as well to the extent the regulation is effectively enforced and prevents the reckless or knowing disclosure of this information to criminal or terrorist elements.

Regulatory Analysis Form

(14) Describe who will be adversely affected by the regulation. (Quantify the adverse effects as completely as possible and approximate the number of people who will be adversely affected.)

No person or entity will be adversely affected by this regulation.

(15) List the persons, groups or entities that will be required to comply with the regulation. (Approximate the number of people who will be required to comply.)

All Pennsylvania public utilities that file confidential security information with the Commission will be required to comply with the proposed regulation in order to protect the information from unwanted disclosure. In practice, however, it is expected that few public utilities will actually file this type of information with the Commission so that the procedures will only be infrequently used.

(16) Describe the communications with and input from the public in the development and drafting of the regulation. List the persons and/or groups who were involved, if applicable.

To date, the rulemaking has had one advance notice published in the Pennsylvania Bulletin. Comments were received from the Energy Association of PA, Office of Consumer Advocate, PECO Energy Company, and the National Association of Water Companies, Pennsylvania Chapter, and the same parties except NAWC filed reply comments.

(17) Provide a specific estimate of the costs and/or savings to the regulated community associated with compliance, including any legal, accounting or consulting procedures which may be required.

Costs of compliance with the proposed regulation will be minimal. Utilities may be expected to incur some outside legal expenses to review designated documents and legal papers prior to filing to ensure compliance with the regulation's provisions.

Regulatory Analysis Form

(18) Provide a specific estimate of the costs and/or savings to local governments associated with compliance, including any legal, accounting or consulting procedures which may be required.

Not applicable.

(19) Provide a specific estimate of the costs and/or savings to state government associated with the implementation of the regulation, including any legal, accounting, or consulting procedures which may be required.

Additional legal or accounting costs associated with the implementation of this proposed regulation by the Commission will be minimal. There will be no savings to the Commission as a result of implementing this proposed regulation.

Regulatory Analysis Form

(20) In the table below, provide an estimate of the fiscal savings and costs associated with implementation and compliance for the regulated community, local government, and state government for the current year and five subsequent years.

	Current FY Year	FY +1 Year	FY +2 Year	FY +3 Year	FY +4 Year	FY +5 Year
SAVINGS:	\$ N/A	\$	\$	\$	\$	\$
Regulated Community						
Local Government						
State Government						
Total Savings						
COSTS:						
Regulated Community	minimal	minimal	minimal	minimal	minimal	minimal
Local Government	N/A					
State Government	minimal	minimal	minimal	minimal	minimal	minimal
Total Costs						
REVENUE LOSSES:	N/A					
Regulated Community						
Local Government						
State Government						
Total Revenue Losses						

(20a) Explain how the cost estimates listed above were derived.

The proposed regulation is not expected to result in any revenue losses, savings or costs to local governments. No revenue losses or savings are expected for the regulated community or state government. Costs associated with the preparation and filing of confidential security information for the regulated community and the Commission are expected to be minimal.

Regulatory Analysis Form

(20b) Provide the past three year expenditure history for programs affected by the regulation.

Program	FY -3	FY -2	FY -1	Current FY
Not applicable.				

(21) Using the cost-benefit information provided above, explain how the benefits of the regulation outweigh the adverse effects and costs.

Not applicable.

(22) Describe the nonregulatory alternatives considered and the costs associated with those alternatives. Provide the reasons for their dismissal.

Not applicable.

(23) Describe alternative regulatory schemes considered and the costs associated with those schemes. Provide the reasons for their dismissal.

Not applicable.

Regulatory Analysis Form

(24) Are there any provisions that are more stringent than federal standards? If yes, identify the specific provisions and the compelling Pennsylvania interest that demands stronger regulation.

No.

(25) How does this regulation compare with those of other states? Will the regulation put Pennsylvania at a competitive disadvantage with other states?

Comparison with other states was not directly made. However, as the costs to implement should be minimal for public utilities, the regulation should not place Pennsylvania at a competitive disadvantage.

(26) Will the regulation affect existing or proposed regulations of the promulgating agency or other state agencies? If yes, explain and provide specific citations.

No.

(27) Will any public hearings or informational meetings be scheduled? Please provide the dates, times, and locations, if available.

No.

Regulatory Analysis Form

(28) Will the regulation change existing reporting, record keeping, or other paperwork requirements? Describe the changes and attach copies of forms or reports which will be required as a result of implementation, if available.

No.

(29) Please list any special provisions which have been developed to meet the particular needs of affected groups or persons including, but not limited to, minorities, elderly, small businesses, and farmers.

Not applicable.

(30) What is the anticipated effective date of the regulation; the date by which compliance with the regulation will be required; and the date by which any required permits, licenses or other approvals must be obtained?

The proposed regulation will become final following publication in the Pennsylvania Bulletin after review of all comments submitted to the Commission and approval by the Independent Regulatory Review Commission. The Commission hopes to have final form regulations to receive all necessary approvals by the summer of 2008.

(31) Provide the schedule for continual review of the regulation.

After taking effect, the final regulation will be reviewed and revised as is necessary.

FACE SHEET
FOR FILING DOCUMENTS
WITH THE LEGISLATIVE REFERENCE BUREAU

(Pursuant to Commonwealth Documents Law)

RECEIVED
2007 NOV 21 PM 1:31
INDEPENDENT REGULATORY
BUREAU OF CONSUMER
PROTECTION

DO NOT WRITE IN THIS SPACE

Copy below is hereby approved as to form and legality. Attorney General.

BY *Amy M. Elliott*
(DEPUTY ATTORNEY GENERAL)

OCT 30 2007

DATE OF APPROVAL

Check if applicable
Copy not approved. Objections attached

Copy below is hereby certified to be true and correct copy of a document issued, prescribed or promulgated by:

Pennsylvania Public Utility Commission
(AGENCY)

DOCUMENT/FISCAL NOTE NO. L-00070185/57-256

DATE OF ADOPTION August 30, 2007

BY *James J. McNulty*
James J. McNulty

TITLE *Secy*
(SECRETARY)

Copy below is hereby approved as to form and legality. Executive or independent Agencies.

BY *Bohdan R. Pankiw*
Bohdan R. Pankiw
Chief Counsel

8-30-07
DATE OF APPROVAL

Check if applicable. No Attorney General approval or objection within 30 days after submission.

L-00070185/57-256
Proposed Rulemaking
Regarding Implementation of the Public Utility Confidential
Security Information Disclosure Protection Act
52 Pa. Code, Chapter 102

The Pennsylvania Public Utility Commission on August 30, 2007, adopted a proposed rulemaking order which establishes protocols and procedures to be followed when public utilities file records with the Commission containing confidential security information and challenges to the utility's designations or requests to examine records containing confidential security information are made. The contact person is Carl Hisiro, Law Bureau, 783-2812.

EXECUTIVE SUMMARY

L-00070185/57-256
Proposed Rulemaking
Re: Confidential Security Information Safeguards
for all Public Utilities
52 Pa. Code, Chapters 5 and 102

On November 29, 2006, Governor Edward Rendell signed into law the Public Utility Confidential Security Information Disclosure Act (“CSI Act”), 35 P.S. §§ 2141.1-2141.6. The CSI Act provides safeguards for confidential security information of public utilities that is provided to state agencies such as the Commission from disclosure that may compromise security against sabotage or criminal or terrorist acts. In creating this mandate of nondisclosure of confidential security information, the CSI Act directs the Commission to develop, among other things: (1) filing protocols and procedures for public utilities to follow when submitting records containing confidential security information; and (2) protocols and procedures to address challenges to the designations or requests to examine records containing confidential security information. 35 P.S. § 2141.3.

The rulemaking went through an advance notice published in the Pennsylvania Bulletin on May 5, 2007, and the Commission received comments and reply comments from several parties. The proposed regulations at 52 Pa. Code §§ 102.1-102.4 spell out the purpose of the new regulations; provide a series of definitions that are identical to the corresponding definitions in the CSI Act, except for “member of the public,” which is defined in a way to be consistent with Pennsylvania’s Right-to-Know Law, 65 P.S. § 66.2; and address the filing and challenge procedures contemplated by the CSI Act. The proposed regulations address issues such as how a utility is to label confidential security information to be filed with the Commission, how the Commission is to handle previously-filed unmarked records in its possession, and how electronic submissions will

be treated. The proposed regulations also amend 52 Pa. Code § 5.423 by adding a new subsection (g) whose sole purpose is to refer the reader to the new Chapter 102.

The contact person is Carl S. Hisiro (717) 783-2812 in the Law Bureau.

**PENNSYLVANIA
PUBLIC UTILITY COMMISSION
Harrisburg, PA. 17105-3265**

Public Meeting held August 30, 2007

Commissioners Present:

Wendell F. Holland, Chairman
James H. Cawley, Vice Chairman
Terrance J. Fitzpatrick
Tyrone J. Christy
Kim Pizzingrilli

Proposed Rulemaking Regarding Implementation of the Public Utility Confidential Security Information Disclosure Protection Act. L-00070185

Implementation of the Public Utility Confidential Security Information Disclosure Protection Act. M-00072014

PROPOSED RULEMAKING ORDER

BY THE COMMISSION:

This proposed rulemaking establishes, in furtherance of the Public Utility Confidential Security Information Disclosure Protection Act, 35 P.S. §§ 2141.1-2141.6 (“CSI Act”), protocols and procedures that must be followed when (1) public utilities file records with the Commission that contain confidential security information and (2) challenges to the utility’s designations or requests to examine records containing confidential security information are made by members of the public.

A. Background and Procedural History

On April 20, 2007, the Commission entered an order at this docket directing an Advance Notice of Proposed Rulemaking be issued to solicit comments regarding the

development of the regulations necessary to implement the CSI Act. As stated in the April 20, 2007 Order, the purpose of the CSI Act is to create mechanisms for the safeguarding of confidential security information of public utilities that is provided to various state agencies such as the Commission from disclosure that may compromise security against sabotage or criminal or terrorist acts.

In creating this mandate of nondisclosure of confidential security information, the CSI directs the Commission to develop: (1) filing protocols and procedures for public utilities to follow when submitting records containing confidential security information; (2) protocols and procedures to address challenges to the designations or requests to examine records containing confidential security information; and (3) protocols and procedures to protect public utility records or portions thereof that contain confidential security information from prohibited disclosure by Commission employees. 35 P.S. § 2141.3.

It is the first two protocols listed above – filing requirements for confidential security information and procedures to address challenges to or requests to review confidentiality designations – we concluded were most appropriate for our rulemaking process because they are procedures to be followed by outside parties such as utilities, ratepayers, and the statutory advocates. In the Advance Notice, we particularly asked for comments on the following issues: (1) the factors that should be used to determine whether a public utility's designation of a record or portion thereof as "confidential security information" should be upheld by the Commission in the face of a challenge; (2) when InfoMAP is implemented by the Commission, whether electronic filing of documents containing confidential security information should be allowed (or should only hard copies be filed), and if the answer is yes, whether any special rules need to be implemented for electronic filings; and (3) the procedures that should be followed for the statutory advocates to obtain access to the confidential security information when they

have a legitimate need to such access.

The Advance Notice was published in the *Pennsylvania Bulletin* on May 5, 2007 (37 Pa.B. 2098), with a 45-day comment period and a 30-day reply comment period. Comments were received from four parties: the Office of Consumer Advocate (“OCA”), PECO Energy Company (“PECO”), the National Association of Water Companies, Pennsylvania Chapter (“NAWC”), and the Energy Association of Pennsylvania (“EAPA”). Reply comments were received from OCA, PECO, and EAPA. These comments and reply comments are discussed in the “Comments and Responses Document” attached to this Order as Appendix A.

B. Discussion

We are proposing today a comprehensive set of regulations that will be applicable to all public utilities in the Commonwealth relating to the filing requirements and challenge procedures outlined in the CSI Act that each state agency is directed to create to help ensure the safeguarding of confidential security information from unwanted disclosure. These proposed regulations reflect our consideration of all the comments and reply comments filed pursuant to the Advance Notice, while attempting to satisfy the legislative intent and meaning of the various provisions of the CSI Act. We appreciate and thank all the commenting parties who provided worthwhile suggestions to aid the Commission in the development of its proposed regulations.

As an initial matter, we believe that the proposed regulations fit naturally as a new chapter in Subpart E of our existing regulations dealing with Public Utility Security Planning and Readiness. However, it is also probable that parties in the future may try to find our confidential security information rules under our existing process in Subpart A, Chapter 5 for determining the availability of proprietary information, specifically 52 Pa.

Code § 5.423. We have, therefore, suggested adding in our proposed regulations a new subsection (g) in section 5.423 that refers the reader to the new chapter in Subpart E to ensure that the proper process is used from the outset.

The proposed regulation at section 102.1 spells out the purpose of the new regulations, which is to establish the filing requirements and challenge procedures relating to confidential security information as mandated by the CSI Act. The proposed regulation at section 102.2 provides a series of definitions that are identical to the corresponding definitions in the CSI Act, except for “member of the public,” which is not specifically defined in the statute. We have defined “member of the public” to be consistent with Pennsylvania’s Right-to-Know Law, 65 P.S. § 66.2, which gives access to public records to “any citizen of the Commonwealth of Pennsylvania.” However, given that confidential security information may be relevant in litigation pending before the Commission, including rate cases and safety-related cases, we believe it is appropriate to clarify that “member of the public” also includes public utilities certified by the Commission, the statutory advocates who represent Pennsylvania consumers and small businesses, and the Commission’s own Office of Trial Staff and prosecutory staff, all of who regularly participate in litigation before the Commission.

The proposed regulation at section 102.3 addresses the filing procedures mandated by the CSI Act. Subsection (a), which has its genesis from recommendations made by EAPA and PECO in their respective comments, requires utilities, unless directed by the Commission or its staff to do otherwise, to maintain any record containing confidential security information on site and to rely on the Commission’s self-certification process described in chapter 101 of the Commission’s regulations. We also believe this recommended procedure will minimize the Commission’s storage costs and Commission staff’s exposure to possible sanctions that could result from mishandling confidential security information filed with the Commission. These were some of the concerns

expressed by the OCA in advocating that the Commission should take a stringent view of what type of information should be categorized as confidential security information.

Subsection (b) spells out requirements that are already in the CSI Act, except that subpart (3) spells out further how a public utility shall label confidential security information to be filed with the Commission to ensure that it is properly handled by Commission staff. Similarly, subsection (c) is consistent with the mandates of the CSI Act, which places the burden on the public utility to identify records that contain confidential security information or lose the protections afforded by the statute. The proposed regulation in the last sentence makes clear that any record not properly identified as confidential security information will be treated as a public document and be made available under the Right-to-Know Law.

Subsections (d) and (e) relating to the status of previously-filed unmarked records and the Commission's responsibility for handling unmarked records that may contain confidential security information both come from suggestions made by NAWC in its comments to address areas not expressly covered by the CSI Act, but which nevertheless pose potentially serious liability issues for Commission employees. We believe the proposed regulations contain common sense approaches to dealing with the two issues that protect our employees while maximizing the protections afforded by the statute in areas not expressly covered by the statute.

Subsection (f) deals expressly with one of the areas we asked for specific comments in the Advance Notice – electronic submissions. The proposed regulation acknowledges the Commission's inability at present to handle electronic submissions that would ensure the confidentiality of the filed information and, therefore, provides that until the Commission develops adequate safeguards and notifies the public utility industry that it has developed such safeguards, electronic submissions will be treated as public

filings. This proposed regulation is consistent with the unanimous recommendation of all the commenting parties of not supporting electronic filing until appropriate encryption and special software is implemented by the Commission. It is also consistent with the internal procedures recently prepared by the Pennsylvania Department of Environmental Resources Policy Office that became effective May 29, 2007, addressing the same issue.

The final new proposed regulation at section 102.4 addresses challenge procedures to confidentiality designations and requests to review records containing confidential security information. Proposed subsection (a) spells out the general procedures that will be followed whenever there is a challenge or request to review. This provision makes clear that only records filed with the Commission are subject to this provision while records maintained on-site by the utility are not subject to this provision. The proposed regulation would require the Commission to issue a Secretarial Letter to notify the public utility of the challenge or request to review. In adversarial cases the matter will be referred to the Office of Administrative Law Judge, while in nonadversarial proceedings the matter will go to the Law Bureau for recommended disposition. Because we are dealing with purported security-related information, the proposed regulation would require the challenger or requester to provide certain basic information including his or her social security number if an individual and its certification number if another Pennsylvania public utility. Finally, subsection (a) would give the public utility that has designated the information as confidential security information 15 days to respond to the challenge or request to review, and it would give the administrative law judge or the Law Bureau 15 days from the date the utility's response is filed to issue its recommended decision.

Subsection (b) provides that the Commission will apply a balancing test that weighs the sensitivity of the designated confidential security information and the potential harm resulting from its disclosure against the challenger's or requester's need for the

information and also lists several factors that will be relevant in the Commission's consideration of whether to grant a request to review confidential security information.

Consistent with the CSI Act, subsection (c) provides that the Commission shall have 60 days to issue its decision in writing. Failure to act within this 60-day window will be deemed a denial of the challenge or request to review. Similarly, subsections (d) and (e) closely track the language in the CSI Act relating to appeals of Commission decisions and to treatment of records allegedly containing confidential security information during the pendency of any Commission review or court appeal. Finally, subsections (f) and (g) address how confidential security information is to be accessed by the statutory advocates, another area we asked for specific comments, and by Commission staff.

Accordingly, under sections 2141.1-2141.6 of the Public Utility Confidential Security Information Disclosure Protection Act, 35 P.S. §§ 2141.1-2141.6; sections 501 and 1501 of the Public Utility Code, 66 Pa. C.S. 501 and 1501; sections 201 and 202 of the Act of July 31, 1968, P.L. 769 No. 240, 45 P.S. §§ 1201-1202, and the regulations promulgated thereunder at 1 Pa. Code §§ 7.1, 7.2, and 7.5; section 204(b) of the Commonwealth Attorneys Act, 71 P.S. § 732.204(b); section 745.5 of the Regulatory Review Act, 71 P.S. § 745.5; and section 612 of The Administrative Code of 1929, 71 P.S. § 232, and the regulations promulgated thereunder at 4 Pa. Code §§ 7.231-7.234, we are considering adopting the proposed regulations set forth in Annex A, attached hereto; **THEREFORE,**

IT IS ORDERED:

1. That the proposed rulemaking at L-00070185 will consider the regulations set forth in Annex A.

2. That the Secretary shall submit this Order, Annex A, and Appendix A to the Office of Attorney General for review as to form and legality and to the Governor's Budget Office for review of fiscal impact.

3. That the Secretary shall submit this Order, Annex A, and Appendix A for review and comment to the Independent Regulatory Review Commission and the Legislative Standing Committees.

4. That the Secretary shall certify this Order and Annex A and deposit them with the Legislative Reference Bureau to be published in the *Pennsylvania Bulletin*. The Secretary shall specify publication of the Order in accordance with 45 Pa. C.S. § 727.

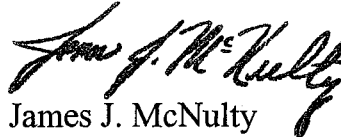
5. That an original and 15 copies of any comments referencing the docket number of the proposed regulations be submitted within 30 days of publication in the *Pennsylvania Bulletin* to the Pennsylvania Public Utility Commission, Attn: Secretary, P.O. Box 3265, Harrisburg, PA 17105-3265.

6. That the contact person for this rulemaking is Carl S. Hisiro, Assistant Counsel, Law Bureau, (717) 783-2812. Alternate formats of this document are available to persons with disabilities and may be obtained by contacting Sherri DelBiondo, Regulatory Coordinator, Law Bureau, 717-772-4579.

7. That a copy of this Order, Annex A, and Appendix A shall be served upon the National Association of Water Companies, Pennsylvania Chapter; the Energy Association of Pennsylvania, PECO Energy Company; Philadelphia Gas Works; FirstEnergy Corporation; Equitable Gas Company; Nisource Corporate Services Company; Duquesne Light Company; Dominion Peoples; UGI Corporation; UGI Utilities, Inc.; UGI Penn Natural Gas, Inc.; Allegheny Power; PPL Services Corporation;

National Fuel Distribution Corporation; Nauman Global Enterprises, LLC; Dart Container Corporation of California d/b/a DTX Inc.; McClymonds Supply & Transit Co., Inc.; the Office of Trial Staff; the Office of Consumer Advocate; and the Small Business Advocate.

BY THE COMMISSION



James J. McNulty
Secretary

(SEAL)

ORDER ADOPTED: August 30, 2007

ORDER ENTERED: **SEP 04 2007**

ANNEX A

TITLE 52. PUBLIC UTILITIES PART I. PUBLIC UTILITY COMMISSION SUBPART E. PUBLIC UTILITY SECURITY PLANNING AND READINESS CHAPTER 102. CONFIDENTIAL SECURITY INFORMATION

§ 102.1. Purpose.

This chapter establishes procedures for public utilities to follow when filing records with the Commission containing confidential security information pursuant to the Public Utility Confidential Security Information Disclosure Protection Act, enacted on November 29, 2006, as Act 156, P.L. 1435, No. 156, 35 P.S. §§ 2141.1-2141.6 ("Act 156"), and procedures to address challenges by members of the public to a public utility's designation of confidential security information or requests to examine records containing confidential security information in both adversarial and nonadversarial proceedings pending before the Commission.

§ 102.2. Definitions.

The following words and terms, when used in this chapter, have the following meanings, unless the context clearly indicates otherwise:

Confidential security information -- Information contained within a record maintained by the Commission in any form, 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, public property or public utility facilities, including, but not limited to, all of the following:

(i) A vulnerability assessment which is submitted to the Environmental Protection Agency or any other Federal, State or local agency.

(ii) Portions of emergency response plans that are submitted to the Pennsylvania Department of Environmental Protection, the Commission or any other Federal, State or local agency dealing with response procedures or plans prepared to prevent or respond to emergency situations, except those portions intended for public disclosure, the disclosure of which would reveal vulnerability assessments, specific tactics, specific emergency procedures or specific security procedures. Nothing in this term shall be construed to relieve a public utility from its public notification obligations under other applicable Federal and State laws.

(iii) A plan, map or other drawing or data which shows the location or reveals location data on community drinking water wells and surface water intakes.

(iv) A security plan, security procedure or risk assessment prepared specifically for the purpose of preventing or for protection against sabotage or criminal or terrorist acts.

(v) Specific information, including portions of financial statements, about security devices or personnel, designed to protect against sabotage or criminal or terrorist acts.

Nothing in this definition shall be construed to prevent the disclosure of monetary amounts.

Facilities -- All the plant and equipment of a public utility, including all tangible and intangible real and personal property without limitation, and any and all means and

instrumentalities in any manner owned, operated, leased, licensed, used, controlled, furnished or supplied for, by or in connection with the business of any public utility. The term shall also include electric power generation.

Member of the public – Includes any citizen of the Commonwealth of Pennsylvania, public utility certified by the Commission, the Office of Consumer Advocate, the Office of Small Business Advocate, the Office of Trial Staff, or Commission prosecutory staff.

Public utility -- Any person, corporation, municipality or municipal authority or corporation now or hereafter owning or operating in this Commonwealth equipment or facilities for:

(i) Producing, generating, transmitting, distributing or furnishing natural or artificial gas, electricity or steam for the production of light, heat or power to the public for compensation. The term shall also include electric power generation.

(ii) Diverting, developing, pumping, impounding, distributing or furnishing water to or for the public for compensation.

(iii) Using a canal, turnpike, tunnel, bridge, wharf and the like for the public for compensation.

(iv) Transporting or conveying natural or artificial gas, crude oil, gasoline or petroleum products, materials for refrigeration or oxygen or nitrogen or other fluid substance, by pipeline or conduit, for the public for compensation.

(v) Conveying or transmitting messages or communications by telephone or telegraph or domestic public land mobile radio service, including, but not limited to, point-to-point microwave radio service for the public for compensation.

(vi) Collecting, treating or disposing sewage for the public for compensation.

(vii) Transporting passengers or property as a common carrier.

Terrorist act -- Any act or acts constituting a violent offense intended to:

(i) Intimidate or coerce a civilian population.

(ii) Influence the policy of a government by intimidation or coercion.

(iii) Affect the conduct of a government.

§ 102.3. Filing procedures.

(a) Maintenance of records on site. Unless required by order or other directive from the Commission or its staff that records containing confidential security information must be filed with the Commission, public utilities shall do the following:

(1) Maintain any record containing confidential security information on site.

(2) Certify that the record is present and up-to-date consistent with chapter 101 (relating to public utility preparedness through self certification).

(3) Make the record containing confidential security information available for review upon request by authorized Commission staff.

(b) Filing requirements. When a public utility is required to submit a record that contains confidential security information to the Commission, the public utility shall do the following:

(1) Clearly state in its transmittal letter to the Commission that the record contains confidential security information and explain why the information should be treated as confidential.

(2) Separate the information being filed into at least two categories:

(i) Records that are public in nature and subject to the Right-to-Know Law, 65 P.S. §§ 66.1-66.9.

(ii) Records that are to be treated as containing confidential security information and not subject to the Right-to-Know Law, 65 P.S. §§ 66.1-66.9.

(3) Stamp or label each affected page of the record containing confidential security information with the words “Confidential Security Information” and place all affected pages in a separate envelope marked “Confidential Security Information.”

(c) *Public utility’s responsibility.* The public utility has the responsibility to identify records as containing confidential security information. When the public utility fails to designate a record as containing confidential security information, it does not obtain the protections offered in this chapter and in Act 156. Any record that is not identified, stamped and separated as set forth in subsection 102.3(b), will be made available to the public under the Right-to-Know Law, 65 P.S. §§ 66.1-66.9.

(d) *Status of previously-filed unmarked records.* Records containing what would otherwise be deemed confidential security information already on file at the Commission prior to May 29, 2007, the effective date of Act 156, are not covered by the protections offered in this chapter and in Act 156. In order to obtain such protections, the public

utility shall resubmit and replace the existing records by following the filing procedures provided for in this subsection. When a public utility's filing is intended to replace pre-Act 156 filed records, the Commission will waive any otherwise applicable filing fee.

(e) *Commission's responsibility with unmarked records.* The Commission and its staff are under no legal obligation to protect confidential security information already on file with the Commission that has not been marked "Confidential Security Information," following the procedures provided for in this subsection. When a request is made by a member of the public for an existing record that is not marked "Confidential Security Information" and Commission staff has reason to believe that it contains confidential security information, staff will refer the requested record to the Law Bureau for review. If the Law Bureau determines the record contains confidential security information, the Law Bureau will advise the affected public utility and give it an opportunity to resubmit and replace the record with a copy that is marked "Confidential Security Information" pursuant to subsection 102.3(d).

(f) *Electronic submissions.* The Commission does not yet have the ability to handle electronically submitted confidential security information in the manner required by this chapter or Act 156. The Commission will notify the public utility industry when it develops the ability to handle electronic submissions of confidential security information. Until the Commission develops the ability to handle electronic submissions of confidential security information, all information submitted electronically will be made available to the public under the Right-to-Know Law, 65 P.S. §§ 66.1-66.9.

§ 102.4. Challenge procedures to confidentiality designation.

(a) General rule for challenges or requests to review. When a member of the public other than a statutory advocate or Commission staff challenges the public utility's designation of confidential security information or requests in writing to examine confidential security information, the Commission will issue a Secretarial Letter to the public utility notifying the public utility of the challenge to its designation or the request to examine records containing confidential security information. Only records filed with the Commission as confidential security information are subject to a challenge or written request to review under this subsection and Act 156. Records maintained on site by the public utility are not subject to challenge or request to review.

(1) When a challenge or written request to review occurs in an adversarial proceeding, the matter shall be referred to the Office of Administrative Law Judge for recommended disposition by the Commission.

(2) When a challenge or written request to review occurs in a nonadversarial proceeding, the matter shall be referred to the Law Bureau for recommended disposition by the Commission.

(3) The Commission will have up to 60 days from the date the challenge or written request to review is filed with the Secretary's Bureau to render a final decision. During the 60-day review period, the following process shall be used:

(i) For identification purposes, the challenger or requester, if not a statutory advocate or Commission staff, shall provide his or her full name, address, telephone

number, and social security number if an individual and its certification number, address, and telephone number if it is a Pennsylvania utility.

(ii) For challenges, the challenger shall provide at the time it files the challenge a detailed statement explaining why the confidential security information designation should be denied.

(iii) For requests to review, the requester shall provide at the time it files the request 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.

(iv) The public utility shall have 15 days from the date the challenge or request to review is filed with the Secretary's Bureau to respond to the challenger's or requester's detailed statement in support of its position.

(v) The presiding officer or the Law Bureau shall have 15 days from the date the public utility's response is filed with the Secretary's Bureau to issue its recommended disposition to the Commission.

(b) *Relevant factors to be considered.* The Commission will apply a balancing test that weighs the sensitivity of the designated confidential security information and the potential harm resulting from its disclosure against the challenger's or requester's need for the information. Applying this balancing test, a challenge to a public utility's designation of confidential security information or written request to review a record containing confidential security information will be granted only upon a determination by

the Commission that the potential harm to the public utility of disclosing information relating to its security is less than the challenger's or requester's need for the information.

In determining whether to grant a written request to review a record containing confidential security information, the Commission, the presiding officer, or the Law Bureau will consider, along with other relevant factors, the following:

- (1) The requester's willingness to sign a non-disclosure agreement.
- (2) The requester's willingness to be subjected to a criminal background check.
- (3) The conditions, if any, to place on release of the information.

(c) *Written notification of disposition.* The Commission will provide, within the 60-day period, written notification of its decision on confidentiality to the public utility and the member of the public that requested to examine the records containing confidential security information or challenged the designation made by the public utility. Failure by the Commission to act within the 60-day period will be deemed a denial of the challenge or the request to review. In the written notification, the Commission will affirmatively state whether the disclosure would compromise the public utility's security against sabotage or criminal or terrorist act. When the Commission determines that a record contains confidential security information and information that is public, the confidential portion will be redacted before disclosure.

(d) *Appeal of Commission decision.* The Commission's decision on confidentiality under this chapter will be issued by order adopted at a public meeting. The public utility and member of the public shall have up to 30 days following entry of this order to file an

appeal in Commonwealth Court. The Commonwealth Court will review any records containing the disputed confidential security information in camera to determine whether the information should be protected from disclosure pursuant to this chapter. During the pendency of the in camera review, the records subject to this review may not be made part of the public court filing.

(e) Treatment of records during pendency of review. During the challenge, request to review, or an appeal of the Commission's final determination, the Commission will continue to honor the confidential security information designation by the public utility.

(f) Access for statutory advocates. Authorized individuals, as provided for in Act 156, employed by the statutory advocates shall be provided with access to confidential security information on file with the Commission when they provide the public utility with a justification for the need of the information and execute access agreements that summarize responsibilities and personal liabilities when confidential security information is knowingly or recklessly released, published or otherwise disclosed.

(g) Access for Commission staff. Unopened envelopes marked "Confidential Security Information" filed with the Commission will be given only to Commission employees authorized to review the information as provided for in Act 156. Authorized Commission employees shall execute access agreements that summarize responsibilities and personal liabilities when confidential security information is knowingly or recklessly released, published or otherwise disclosed. Commission employees may decline designation as authorized individuals. Commission employees that agree to the designation will have

their names added to the Authorized Access List maintained by the Commission's Secretary's Bureau. The Commission will withdraw designations when the employee no longer requires access to confidential security information because of a change in duties or position or when the employee fails to attend required training.

* * * * *

**TITLE 52. PUBLIC UTILITIES
PART I. PUBLIC UTILITY COMMISSION
SUBPART A. GENERAL PROVISIONS
CHAPTER 5. FORMAL PROCEEDINGS**

Subchapter E. EVIDENCE AND WITNESSES

§ 5.423. Orders to limit availability of proprietary information.

* * * * *

(g) Confidential security information. Challenges to a public utility's designation of confidential security information or requests in writing to examine confidential security information are addressed in chapter 102 (relating to confidential security information).

APPENDIX A

Proposed Rulemaking Regarding Implementation
of the Public Utility Confidential Security
Information Disclosure Protection Act

Docket No. L-00070185

Implementation of the Public Utility
Confidential Security Information Disclosure
Protection Act

Docket No. M-00072014

COMMENTS AND RESPONSES DOCUMENT

By Order entered April 20, 2007, at Docket No. L-00070185, the Commission issued an Advanced Notice of Proposed Rulemaking to seek comments on the nature and scope of what should be included in the filing and challenge procedures that must be followed under the newly enacted Public Utility Confidential Security Information Disclosure Protection Act, 35 P.S. §§ 2141.1-2141.6 ("CSI Act"). Specifically, the Advanced Notice asked for comments on the following issues: (1) the factors that should be used to determine whether a public utility's designation of a record or portion thereof as "confidential security information" should be upheld by the Commission in the face of a challenge; (2) when InfoMAP is implemented by the Commission, whether electronic filing of documents containing confidential security information should be allowed (or should only hard copies be filed), and if the answer is yes, whether any special rules need to be implemented for electronic filings; and (3) the procedures that should be followed for the statutory advocates to obtain access to the confidential security information when they have a legitimate need to such access.

Comments were submitted by the Office of Consumer Advocate (“OCA”), PECO Energy Company (“PECO”), the National Association of Water Companies, Pennsylvania Chapter (“NAWC”), and the Energy Association of Pennsylvania (“EAPA”). Reply comments were received from OCA, PECO, and EAPA.

A. Comments to Advance Notice of Proposed Rulemaking

1. Confidential Security Information Designations

PECO suggests reviewing existing Federal Energy Regulatory Commission (“FERC”) regulations for safeguarding confidential security information. FERC has two processes for such: National Security Information (“NSI”), and Critical Energy Infrastructure Information (“CEII”). PECO Comments of June 19, 2007, at 2-3.

PECO recommends that the Commission adopt some blend of NSI and CEII. Under NSI, confidential security information is exempt from the Freedom of Information Act. PECO explains that NSI must be labeled “Top Secret,” “Secret,” or “Confidential,” depending on the degree of significance to national security and requires a special stamp on all confidential security information detailing the classification level of the document, when it becomes subject to declassification, and the date. *Id.* at 3. Only select federal government officials can access this information. The second process, CEII is designed to allow certain types of access. The purpose of CEII is to protect security interests of the utility while permitting public access. Under CEII, information designated as confidential is not necessarily presumed and is subject to a process of approval for

designations (however, the CSI Act provides that the designation by a utility is accepted unless a successful challenge is made). *Id.* at 3.

EAPA recommends that the Commission adopt portions of the CEII process. EAPA Comments of June 19, 2007, at 5. EAPA suggests creating distinctions between secure information, which would remain on the utility's premises and not be filed with the Commission, and confidential information, which should be marked as such by the utility and follow the Commission's current self-certification process. *Id.* EAPA states that only information filed as confidential be subject to a challenge.

The OCA, on the other hand, advocates for the judicious application of confidential security information designations as the handling of these documents imposes significant risks and responsibilities to those who come in contact with them. The OCA further comments that confidential security information designations should be limited and proposes "stringent standards" before confidential security information designations are granted by the Commission. The OCA asserts:

The Commission should not permit utilities to impose this serious burden without a thorough substantiation of each and every item for which a CSI [confidential security information] classification is sought. The OCA submits that the Commission must designate either personnel or an office that has as its role the examination CSI requests and filings and the determination of whether the submitted information is in fact CSI.

OCA Comments of June 19, 2007, at 4. The OCA is also concerned that an excess of confidential security information classifications could interfere with the timely adjudication of "base rate cases and other time-sensitive proceedings." *Id.* at 7.

Finally, the NAWC remarks that the CSI Act allows state agencies flexibility by providing a “threshold of public safety requirement.” NAWC Comments of June 15, 2007, at 10. The NAWC states that it is the public utility’s responsibility to reduce risks and uphold security measures with regard to confidential security information designations, while it is the state agency’s responsibility to balance the practical benefits of public disclosure with the risks of sabotage, criminal, or terrorist acts. EAPA Comments of June 19, 2007, at 10. Additionally, NAWC recommends that state agencies should allow public utilities to resubmit and replace existing records if they contain confidential security information, without having to pay a new filing fee. *Id.* at 5. The NAWC further suggests that the Commission provide a procedure where staff can refer requested pre-CSI Act documents to the Law Bureau for review if it is suspected that the documents contain confidential security information. If the Law Bureau finds that a document *contains* confidential security information, it should consult with the affected public utility. *Id.* at 5-6.

2. Handling of Confidential Security Information

All of the commentators assert that once a confidential security information designation is established for a public utility, certain precautionary measures must be practiced. For instance, PECO states that all confidential security information should be stored in a secure location separate from public records and general utility documents. PECO Comments of June 19, 2007, at 9. PECO, the OCA, and EAPA agree that the Commission should implement a document tracking system in order to monitor the possible migration of these documents. PECO Comments of June 19, 2007, at 9; OCA

Comments of June 19, 2007, at 14; EAPA Comments of June 19, 2007, at 9-10. Each of the four commenting parties suggest that utilities keep these files on site for review by the Commission. Both EAPA and PECO state that this policy would be consistent with the current Commission practices allowing for self-certification to prevent inadvertent release of confidential security information. PECO Comments of June 19, 2007, at 7 & 10; EAPA Comments of June 19, 2007, at 5.

The NAWC's comments suggest looking at the United States Environmental Protection Agency "Protocol to Secure Vulnerability Assessments Submitted by Community Water Systems to EPA" to help in the Commission's development of regulations to protect confidential security information. NAWC Comments of June 19, 2007, at 12. NAWC further advocates that existing databases be password protected and that they be made accessible only to authorized individuals who have signed a confidentiality agreement, an access agreement, or memorandum of understanding ("MOU") to protect against disclosure of records containing confidential security information. *Id.* at 6.

The OCA's comments raise several issues relating to the handling of confidential security information. From the OCA's perspective, the handling of confidential security information exposes state agencies and their employees to a high degree of risk given the significant penalties imposed by the CSI Act. For this reason, the OCA asserts that the burden of showing that a confidential security information designation is justified should rest on the public utility. The OCA acknowledges that this approach is different than the procedures the Commission currently uses for proprietary information at 52 Pa. Code

§ 5.423. Under section 5.423, the Commission grants proprietary treatment simply upon the utility's claim that the information is proprietary, without requiring more. The OCA asserts that the CSI Act's requirements on a utility to justify a confidential security information classification and to segregate information into "confidential" and "public" classifications, coupled with the significant costs and penalties imposed on state agencies and employees, should preclude all but the most sensitive information from confidential security information protection. OCA Comments of June 19, 2007, at 3-9.

3. Challenges to Confidential Security Information Designations

With regard to the challenges filed by members of the public, PECO comments that, although the public utility is the initial designator for confidential security information, the Commission is responsible for determining whether a challenge to the designation will be heard and, ultimately, whether access will be granted. PECO Comments of June 19, 2007, at 6. Both PECO and EAPA assert that the burden of proof should lie with the requester and that upon submission, the requester should be required to submit a detailed statement demonstrating that the need for access is greater than the need to protect the information, sign a nondisclosure agreement (NDA) when access is granted, and undergo a criminal background check. PECO Comments of June 19, 2007, at 6-7; EAPA Comments of June 19, 2007, at 6. PECO also asserts that the Secretary's Bureau should provide written notification to the public utility when a challenge to the confidential security information designation or a request to examine the

confidential security information has been submitted. PECO Comments of June 19, 2007, at 7.

EAPA recommends that *only* information filed with the Commission as confidential should be potentially subject to challenge. EAPA also urges that a balancing test (similar to current practice) should be applied to confidential security information challenges. EAPA Comments of June 19, 2007, at 5-6. PECO agrees with this approach. PECO Comments of June 19, 2007, at 6.

Similarly, NAWC comments that it is the Commission's responsibility to determine if the practical benefits of public disclosure outweigh those risks associated with sabotage or criminal or terrorist acts and also recommends the use of a balancing test. NAWC Comments of June 15, 2007, at 10. NAWC further comments that challenges made by a member of the public should be submitted to the Commission, as the "agency in which the records were originally submitted," and not to OCA or to the Office of Small Business Advocate ("OSBA"). *Id.* at 12. Finally, the NAWC claims that the Commission should not be held responsible for disclosing records containing confidential security information under 35 P.S. § 2141.5, if the utility has not first identified such records upon submission to an agency. *Id.* at 5.

The OCA advocates a two-step test in designating confidential security information. The first step is whether the utility has met its burden of proof in claiming that the information it filed is confidential security information. The second step concerns how another party may challenge the confidential security

information designation. OCA Comments of June 19, 2007, at 8. The OCA believes that the Office of Administrative Law Judge is the most appropriate branch of the Commission to resolve challenges to confidential security information designations. OCA Comments of June 19, 2007, at 16.

4. Electronic Filing of Confidential Security Information

PECO recommends that electronic filing requirements for confidential security information be flexible in order to allow the utility discretion and provide for potential changes in technology, especially keeping in mind the eminent implementation of InfoMAP. PECO Comments of June 19, 2007, at 7. PECO asserts that whether confidential security information can be electronically filed should be at the discretion of the Commission whereas whether sensitive information is electronically filed should be the decision belonging to the public utility. *Id.* Finally, PECO argues that e-mail transmission of confidential security information should be prohibited unless encrypted or special software is used. *Id.*

EAPA recommends that confidential security information *not* be filed electronically for security purposes, but if it is permitted, encryption and special software should be implemented. EAPA Comments of June 19, 2007, at 7. EAPA also comments that the Commission should look to already-implemented FERC rules and regulations in order to provide for electronic filing protocols. *Id.* at 6.

Similarly, the NAWC asserts that only “public” information should be filed electronically unless or until the InfoMAP system can securely handle confidential security information documents. NAWC Comments of June 15, 2007, at 11. The

NAWC opines that if confidential security information designated materials are eventually filed electronically, this information should be password protected and only accessible to authorized individuals. *Id.* at 11.

The OCA similarly advocates that the Commission should not *initially* allow for the electronic filing of confidential security information due to the sensitive nature of the information; therefore confidential security information as well as confidential security information requests and challenges should be made on paper. The OCA recommends that the Commission implement InfoMAP and test its ability to handle less sensitive, yet still “restricted” material and proprietary information. OCA Comments of June 19, 2007, at 10.

5. Access for Statutory Advocates

PECO asserts that statutory advocate requests to view confidential security information should balance security concerns and impose “stringent controls” where the information is released. PECO recommends that the statutory advocate sign an NDA and be subject to strict penalties for violation of the agreement and for the release of confidential security information. PECO points out that the only exception to the protections set forth in the CSI Act is for the release of information necessary for construction, renovation, or remodeling on any public building, upon consultation with the utility. PECO states that the Commission’s regulations allow the Commission to direct appropriate treatment of documents containing confidential security information; however, the regulations do not

provide detailed procedures governing the Commission's protocols. PECO Comments of June 19, 2007, at 9.

EAPA agrees with PECO's assessments. Additionally, EAPA recommends that the Commission look to existing FERC regulations when formulating policy. EAPA Comments of June 19, 2007, at 8. EAPA specifically cites FERC Docket Nos. RM02-4-000 and PL02-1-000 when highlighting potential protocol analysis. *Id.* at 10.

The NAWC agrees with PECO and EAPA that an NDA be signed by statutory advocates. The NAWC also recognizes the legitimate need of the OCA and OSBA to access confidential security information as statutory advocates and further comments that, although the CSI Act does not explicitly mention it, interagency cooperation is important and should not be excluded in rulemaking. If the language of the statute is insufficient, the NAWC recommends that state agencies adopt an MOU to protect public utility records containing confidential security information, and that a legislative amendment to 35 P.S. § 2141.5(b) be enacted detailing an exception for interagency sharing of records containing confidential security information while protecting them from disclosure under the Right-to-Know Law. NAWC Comments of June 15, 2007, at 9-10.

Finally, the OCA agrees that interagency cooperation is important and should be considered by the Commission. The OCA comments that "statutory advocates are entitled to access discoverable information in Commission proceedings and the Commission should *not* impose any additional 'legitimacy'

standards beyond the certification of authorized persons provided for in the Act.” OCA Comments of June 19, 2007, at 10. The OCA recommends that statutory advocates be provided with access to confidential security information only if they have a legitimate need. The OCA asserts that costs of confidential security information access for statutory advocates should be “reasonable” and “cost-effective” and that the OCA is entitled to review all discoverable information relating to a utility’s rate requests before the Commission. *Id.* At 11-12. The OCA recommends that the Commission provide a tracking method for those who have accessed the materials in compliance with 35 P.S. § 2141.3(d)(5). *Id.* at 14.

B. Reply Comments to Advance Notice of Proposed Rulemaking

PECO asserts that because the CSI Act is designed to assure security for confidential documents without imposing undue administrative burden, the Commission should adhere to the statutory language and reject proposals to impose additional burdens on utilities prior to a formal designation challenge. PECO Reply Comments of July 19, 2007, at 2. PECO claims that the OCA misinterpreted the statute by arguing that a confidential security information designation by a utility should be subject to overview by the ALJ. *Id.* at 3. EAPA echoes these recommendations and states that the submission of confidential security information does *not* trigger agency review and that confidential security information designations actually *limit* risk to state employees. EAPA Reply Comments of July 19, 2007, at 1-2.

PECO also suggests that the CSI Act calls for security measures with confidential security information designations, therefore OCA's concerns about storage burdens and sanctions for state employees are baseless. PECO Reply Comments of July 19, 2007, at 4. PECO further argues that allowing utilities to "self-certify" would eliminate excessive storage burdens placed on the Commission staff. *Id.* at 5. Similarly, EAPA recommends that regulations should *not* be based on the presumption that confidential security information designations will be abused and therefore prevent access to statutory advocates. EAPA accordingly suggests that the Commission review the comments of NAWC in this regard. EAPA Reply Comments of July 19, 2007, at 2.

In disagreement with PECO and EAPA, the OCA reasserts that the utilities should have the burden of proof when designating information as confidential security information and that the Commission should not assume these designations are valid. OCA Reply Comments of July 19, 2007, at 3. The OCA claims that this procedure will promote administrative efficiency, relieve unnecessary burden on state agencies, and remain in accordance with Pennsylvania law. *Id.* at 4. The OCA further argues that EAPA and PECO wrongly state that the statutory advocates are entitled to confidential security information on the same terms as a public requestor or challenger. Labeled as such, they will have to utilize the same procedures and will not be able to view classified information if the confidential security information designation is upheld. *Id.* at 8. The OCA also claims that customized protective agreements

could be useful in allowing utilities to provide confidential security information to statutory advocates and that PECO and EAPA fail to distinguish between the release of confidential security information to statutory advocates by the utility and a release of confidential security information to public requesters. *Id.* at 8-9.



PENNSYLVANIA PUBLIC UTILITY COMMISSION
COMMONWEALTH OF PENNSYLVANIA
HARRISBURG, PENNSYLVANIA

WENDELL F. HOLLAND
CHAIRMAN

November 21, 2007

The Honorable John R. McGinley, Jr.
Chairman
Independent Regulatory Review Commission
14th Floor, Harristown II
333 Market Street
Harrisburg, PA 17101

Re: L-00070185/57-256
Proposed Rulemaking
Implementation of the Public Utility Confidential
Security Information Disclosure Protection Act
52 Pa. Code, Chapter 102

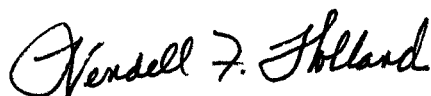
Dear Chairman McGinley:

Enclosed please find one (1) copy of the proposed rulemaking and the Regulatory Analysis Form prepared in compliance with Executive Order 1996-1, "Regulatory Review and Promulgation." Pursuant to Section 5(a) of the Regulatory Review Act of June 30, 1989 (P.L. 73, No. 19) (71 P.S. §§745.1-745.15) the Commission is submitting today a copy of the proposed rulemaking and Regulatory Analysis Form to the Chairman of the House Committee on Consumer Affairs and to the Chairman of the Senate Committee on Consumer Protection and Professional Licensure.

The purpose of this proposal is to establish protocols and procedures to be followed when public utilities file records with the Commission containing confidential security information. The contact person is Carl Hisiro, Law Bureau, 783-2812.

The proposal has been deposited for publication with the Legislative Reference Bureau.

Very truly yours,

A handwritten signature in cursive script that reads "Wendell F. Holland".

Wendell F. Holland
Chairman

Enclosures

cc: The Honorable Robert M. Tomlinson
The Honorable Lisa Boscola
The Honorable Robert Godshall
The Honorable Joseph Preston, Jr.
Legislative Affairs Director Perry
Chief Counsel Pankiw
Assistant Counsel Hisiro
Regulatory Coordinator DelBiondo
Judy Bailets, Governor's Policy Office

TRANSMITTAL SHEET FOR REGULATIONS SUBJECT
TO THE REGULATORY REVIEW ACT

ID Number: L-00070185/57-256

Subject: Regarding Implementation of the Public Utility
Confidential Security Information Disclosure
Protection Act.

Pennsylvania Public Utility Commission

TYPE OF REGULATION

- X Proposed Regulation
- Final Regulation with Notice of Proposed Rulemaking Omitted.
- Final Regulation
- 120-day Emergency Certification of the Attorney General
- 120-day Emergency Certification of the Governor

FILING OF REPORT

<u>Date</u>	<u>Signature</u>	<u>Designation</u>
<u>11-21-07</u>	<u><i>ABauer</i></u>	<u>HOUSE COMMITTEE (Preston)</u> Consumer Affairs
<u>11/21</u>	<u><i>Michelle Krueger</i></u>	<u>SENATE COMMITTEE (Tomlinson)</u> Consumer Protection and Professional Licensure
<u>11/21</u>	<u><i>Small MW</i></u>	<u>Independent Regulatory Review Commission</u> Attorney General
<u> </u>	<u> </u>	<u>Legislative Reference Bureau</u>