

<b>Regulatory Analysis Form</b>		This space for use by IRRC
<b>(1) Agency</b>  Pennsylvania Public Utility Commission		<div style="font-size: 2em; font-weight: bold; margin-bottom: 10px;">RECEIVED</div> <div style="font-weight: bold; margin-bottom: 10px;">2008 MAY 28 PM 1: 37</div> <div style="font-weight: bold; margin-bottom: 10px;">INDEPENDENT REGULATORY REVIEW COMMISSION</div> <div style="font-weight: bold;">IRRC Number: <span style="font-family: cursive; font-size: 1.2em;">2651</span></div>
<b>(2) I.D. Number (Governor*s Office Use)</b>  L-00070185/57-256		
<b>(3) Short Title</b>  Final Rulemaking Re: Implementation of the Public Utility Confidential Security Information Disclosure Protection Act		
<b>(4) PA Code Cite</b>  52 Pa. Code §§ 102.1-102.4 and 52 Pa. Code § 5.243(g)	<b>(5) Agency Contacts &amp; Telephone Numbers</b>  Primary Contact: Carl S. Hisiro (legal), 717-783-2812  Secondary Contact:	
<b>(6) Type of Rulemaking (check one)</b>  <input type="checkbox"/> Proposed Rulemaking <input checked="" type="checkbox"/> Final Order Adopting Regulation <input type="checkbox"/> Final Order, Proposed Rulemaking Omitted	<b>(7) Is a 120-Day Emergency Certification Attached?</b>  <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes: By the Attorney General <input type="checkbox"/> Yes: By the Governor	
<b>(8) Briefly explain the regulation in clear and nontechnical language.</b>  The final 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.		
<b>(9) State the statutory authority for the regulation and any relevant state or federal court decisions.</b>  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 final 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 final 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.

The rulemaking went through an advance notice and a proposed rulemaking order that were published in the Pennsylvania Bulletin. Comments for the advance notice 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. Comments for the proposed rulemaking were received from all the parties listed above and additionally from the Office of Small Business Advocate, the Pennsylvania Newspaper Association, and Philadelphia Gas Works.

(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 final 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 and also some minimal costs to re-file previously-filed unmarked records with the appropriate "confidential security information" stamp to ensure protection.

## 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 final regulation by the Commission will be minimal. There may also be some incidental costs to destroy old records that were previously-filed without the "confidential security information" stamp on them. 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
<b>SAVINGS:</b>	\$ N/A	\$	\$	\$	\$	\$
<b>Regulated Community</b>						
<b>Local Government</b>						
<b>State Government</b>						
<b>Total Savings</b>						
<b>COSTS:</b>						
<b>Regulated Community</b>	minimal	minimal	minimal	minimal	minimal	minimal
<b>Local Government</b>	N/A					
<b>State Government</b>	minimal	minimal	minimal	minimal	minimal	minimal
<b>Total Costs</b>						
<b>REVENUE LOSSES:</b>	N/A					
<b>Regulated Community</b>						
<b>Local Government</b>						
<b>State Government</b>						
<b>Total Revenue Losses</b>						

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

The final 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 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

2008 MAY 28 PM 1:38

INDEPENDENT REGULATORY  
REVIEW COMMISSION

DO NOT WRITE IN THIS SPACE

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

BY \_\_\_\_\_  
(DEPUTY ATTORNEY GENERAL)

\_\_\_\_\_  
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 May 1, 2008

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

5-16-08  
DATE OF APPROVAL

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

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

The Pennsylvania Public Utility Commission on May 1, 2008, adopted a final 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

Final 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 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 agencies such as 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 and proposed rulemaking published in the Pennsylvania Bulletin, and the Commission received comments from a number of interested parties. The final regulations at 52 Pa. Code §§ 102.1-102.4 spell out the purpose of the new regulations; provide a series of definitions that are mostly identical to the corresponding definitions in the CSI Act; and address the filing and challenge procedures contemplated by the CSI Act. The final 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 final 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 May 1, 2008

**Commissioners Present:**

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

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

**FINAL RULEMAKING ORDER**

**BY THE COMMISSION:**

On September 4, 2007, the Commission entered an order proposing to adopt regulations that establish 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. The Commission proposed these regulations in response to the enactment of the Public Utility Confidential Security Information Disclosure Protection Act, 35 P.S. §§ 2141.1-2141.6 ("CSI Act"). The CSI Act directs state agencies such as the Commission to create procedures that will safeguard confidential security information filed with the Commission by public utilities from disclosure that may compromise security against sabotage or criminal or terrorist acts.

The September 4, 2007 Order was published December 8, 2007 at 37 Pa.B. 6421. On or about January 7, 2008, comments were received from the Office of Consumer Advocate (“OCA”), the Office of Small Business Advocate (“OSBA”), the National Association of Water Companies, Pennsylvania Chapter (“NAWC”), the Pennsylvania Newspaper Association (“PNA”), the Energy Association of Pennsylvania (“EAPA”), and the Philadelphia Gas Works (“PGW”). The Commission also received comments from the Independent Regulatory Review Commission (“IRRC”) and the Office of Attorney General (“OAG”).

This Final Rulemaking Order discusses the comments received and sets forth, in Annex A, final amendments to the Commission’s regulations establishing procedures for public utilities to follow when filing confidential security information with the Commission and for members of the public to follow when challenging the utility’s designations or requesting review of records containing confidential security information.

## **Section 102.2. Definitions**

Four changes were made in the definitions section of the regulation. First, to improve clarity, IRRC recommends as to the definition of “confidential security information” that we should simply reference the definition in the statute rather than repeat the definition in its entirety in the PA Code. We agree with this recommendation and also apply it to other definitions in the section – “facilities,” “mass destruction,” “public utility,” and “terrorist act” -- that are identical to the statutory definition.

The second change was to include definitions for “challenger” and “requester” for the sake of clarity as recommended by EAPA and PGW in their respective comments. The third change we made is to the definition of “member of the public.” Both the OAG and IRRC raised concerns about limiting it to “any citizen of the Commonwealth” and we have agreed to broaden it “to a legal resident of the United States,” which is also

consistent with the definition of a “requester” in the Commonwealth’s new Right-to-Know-Law. 2008 Pa. Legis. Serv. Act 2008-3 (S.B. 1) (65 P.S. §§ 67.101-67.3104). Finally, the fourth change was to update the definition of the “Right-to-Know-Law” to reference the newly-enacted law.

### **Section 102.3. Filing Procedures**

The regulation at section 102.3 addresses the filing procedures mandated by the CSI Act. For clarity and consistency, we have changed the word “staff” to “employee” in subsection (a)(3).<sup>1</sup> Additionally, PNA raises the concern that the transmittal letter referenced in subsection (b)(1) must be a public document available to a person seeking to challenge a designation or request to review the confidential security information; otherwise members of the public will not have any knowledge that such a document even exists. PNA fears that without this change, the regulation may have the effect of encouraging public utilities to over-classify documents as confidential security information with no meaningful public oversight. We agree with the PNA’s concern here and have added a sentence to subsection (b)(1) that makes clear that the transmittal letter will be treated as a public document.

IRRC raises several issues in its comments concerning subsection (a). First, IRRC asks in relation to subsection (a)(1) how the Commission will monitor “onsite maintenance” to verify that utilities are correctly classifying information as “confidential security information.” The Commission will monitor compliance the same way it monitors compliance with Chapter 101 now: through onsite visits of the utility to review current operating procedures, which includes verifying that the utility’s cyber security plans, emergency response plans, etc. are current and up-to-date, and through the

---

<sup>1</sup> For the same reason, we have made the identical change in section 102.4(a)(2)(i) and (iii).

performance of management audits pursuant to section 516 of the Public Utility Code. 66 Pa. C.S. § 516.

Second, in regard to subsection (a)(2), which requires a utility to certify that the record is present and up-to-date and references Chapter 101 (relating to public utility preparedness through self certification), IRRC asks if information would need to be added to the Self-Certification Form described in Chapter 101, and if so, what happens if confidential security information is added directly onto the Chapter 101 Form. Currently, we do not see any need to amend the Chapter 101 Form as we believe the current Form is sufficient; however, we will monitor the use of this Form and if we believe language needs to be added for clarity purposes, we will do so. As to what happens if confidential security information is added directly to the Form, the utility should label the Form consistent with subsection (b) of the final regulation; but in any event, even if the utility neglects to do so, the Form itself is not a public document and is automatically treated as a confidential document pursuant to 52 Pa. Code § 101.5.

IRRC also asks how long a utility is required to maintain confidential security records. Generally, for most of the type of records that will be labeled as containing “Confidential Security Information,” such as vulnerability assessments, emergency response plans, cyber security plans, maps showing the location of community drinking wells and surface water intakes and the like, the utility must maintain those records onsite so long as that particular plan, map, *etc.* remains the current plan, map, *etc.* of the utility. Once the older version has been replaced or revised by a newer version, it will be subject to the utility’s document retention program and may be destroyed consistent with that program. For any other documents or records marked as containing confidential security information and maintained by the utility onsite, the retention period will be, at a minimum, whatever the utility’s document retention program requires unless the Commission has directed a different retention period. As all these types of documents

already exist and are subject to the retention policies outlined herein, we did not see the necessity of adding language to the final regulation addressing this issue further.

Finally, in regard to subsection (a), IRRC asks whether the utility is required to follow the same filing requirements that the CSI Act sets forth for public agencies and which requirements are the subject of this final regulation. For example, IRRC asks, does the regulation establish a “document tracking system” for utilities as required by the CSI Act? The simple answer is no; the CSI Act only applies to documents filed with a state agency such as the Commission and not to documents that are retained by the public utility. The final regulation, therefore, only addresses the procedures public utilities must use when they file records containing confidential security information with the Commission and challengers and requesters must use, respectively, to challenge designations of documents or to request review of documents containing confidential security information.

In subsection (b)(3), IRRC states the word “affected page” is ambiguous. To the extent that this language may be interpreted to protect entire pages that may contain confidential security information when such information may only be on part of the page, IRRC questions why redaction is not considered an option. We agree with IRRC’s concern and have removed the word “affected” in subsection (b)(3). We have also added a new subsection (b)(4) to clarify that redaction is to be used to eliminate confidential security information from a page in order to allow the rest of the page to be made public, consistent with the statutory language that directs state agencies to use redaction of confidential security information before disclosure. 35 P.S. § 2141.3(e).

In subsection (c), IRRC is concerned that using the word “will” in the third sentence is overly broad because not every record may be accessible under the Right-to-Know Law. IRRC suggests using “may” instead. We agree and have made that change.

We also added a new subsection (d) in response to concerns raised by the OCA, which has the effect of renumbering the old subsections (d), (e), and (f) as the new (e), (f), and (g). The OCA states that as originally drafted, the proposed regulation appeared to only provide for after-the-fact challenges to confidential security information designations, but that there should be some review by Commission staff when the records are first filed with the Commission. This initial review is necessary, according to the OCA, to ensure that only records that actually fall within the definition of confidential security information will be subject to the restrictions of the CSI Act. The OCA suggests that the Commission adopt the internal procedure already in use by the Pennsylvania Department of Environmental Resources ("DEP") to help ensure that records marked as "Confidential Security Information" have been properly designated. The new subsection (d) does incorporate, to a large extent, the recommended DEP procedures. We believe this new subsection provides a reasonable approach to the stated concern of the OCA and the PNA that without any upfront mechanism to examine confidential security information claims made by public utilities, utilities may be tempted to over-classify records as containing confidential security information knowing the records would be protected unless a party made a challenge at some later date.

In regard to subsection (e) regarding the status of previously-filed unmarked records, IRRC, EAPA, and PGW each raise a concern with the administration of this process in terms of what will happen to previously-filed records that are replaced with new records that are properly stamped as containing confidential security information. In this regard, IRRC especially asks what guarantee will the Commission provide that the old files are now secure or have been destroyed and further asks the Commission to review and develop cost estimates for the fiscal impact of this requirement on the public utilities.



Consistent with the proposal offered by both EAPA and PGW, a new sentence is added at the end of subsection (e) that provides that within 30 days of re-filing the new records, the Commission will either destroy the original records filed or will return them by a secure method to the utility. This change also addresses IRRC's concern as to how the Commission would guarantee that the old files have been securely returned or properly destroyed. As for developing cost estimates, it is impossible for the Commission to determine how many records may be required to be re-filed in order to receive the protections of this provision that would allow us to determine the fiscal impact of this provision. Our general sense, however, is that the impact may be modest at best on the utility industry because most records that contain confidential security information are not filed with the Commission but are in the hands of the utilities pursuant to the self-certification process discussed above.

Similarly, the Commission has added clarifying language to subsection (f) to remove any ambiguity as to the Commission's responsibility with unmarked records. In this regard, two changes were made. First, we make clear that the Law Bureau will provide the affected public utility "with written notification of its determination" that already filed records may contain confidential security information. Second, a new last sentence is added that provides that the failure of the public utility to act within 15 days from the date of this written notice will be deemed a negative response from the utility and the existing record will, therefore, remain in the public file. Additionally, we deleted the first sentence pursuant to IRRC's request because the sentence was redundant as subsection (c) already makes clear that the protections of the CSI Act and this final regulation do not apply when the public utility fails to designate a record as containing

confidential security information and because the requirement that utilities are to re-file unmarked records is already established in subsection (e).<sup>2</sup>

Finally, subsection (g) dealing with electronic submissions has been changed to address concerns submitted by IRRC. IRRC states that the proposed language was framed more as an announcement than a regulation defining current practice. IRRC suggests that the language should be rewritten to set clear compliance standards, which should explicitly prohibit the submission of confidential security information in any electronic form. IRRC adds that when the Commission is ready and able to accept filings electronically while maintaining their confidentiality and security, the Commission will then be able to amend the regulation to allow utilities to file electronically. The final form regulation adopts IRRC's position on this issue.

#### **Section 102.4. Challenge Procedures to Confidentiality Designation**

The regulation at section 102.4 addresses challenge procedures to confidentiality designations and requests to review records containing confidential security information. Subsection (a) spells out the general procedures that will be followed whenever there is a challenge or request to review. In the opening paragraph of subsection (a), the OAG and OSBA raise concerns about the language excluding "a statutory advocate or Commission staff" from challenging the public utility's designation of confidential security information in the first sentence and about the meaning of the last two sentences. In regard to the latter concern, the OAG and IRRC question the Commission's authority under the CSI Act to create the exception that records maintained onsite by the utility are not subject to challenge or requests to review.

---

<sup>2</sup> IRRC also raises a concern about the second part of subsection (f) establishing what it describes as internal procedures for the Commission as opposed to establishing rules or standards that apply to a regulated utility. We believe with the added clarifying language noted above to this subsection, the subsection now more clearly establishes standards that directly pertain to regulated utilities.

We agree that the questioned language in both these cases should be stricken from the regulation. It was never our intent to exclude Commission staff or statutory advocates from challenging improper designations of confidential security information but that was the effect of the original language.<sup>3</sup> As for the last two sentences, while it was our intent to try to make clear that only records filed with the Commission are subject to this provision, the last two sentences are not necessary to accomplish this interpretation. The CSI Act only applies to records filed with the Commission. To the extent that records are maintained onsite by the utility, the CSI Act does not address this situation. Our proposed language, however, created an explicit exception where none existed in the CSI Act. We agree with the OAG and IRRC that this language could allow a public utility to define broadly confidential security information without any legal recourse if the information is not filed with the Commission. We did not intend this result and so have removed the language objected to by the OAG and IRRC.

The above concerns have also led us to remove subsection (a)(1) and to create a new subsection (h) to address situations where confidential security information is requested by a party in litigation pending before the Commission. Based on these same comments and a closer reading of the CSI Act, we have concluded that the challenge and request to review procedures were only intended to apply in nonadversarial proceedings before the Commission and not in litigated proceedings. In the latter instance, existing time-honored safeguards are already in place through the issuance of protective orders by the presiding officer, to protect such records. The CSI Act and these regulations are not meant to be applicable in litigated proceedings and we have amended the regulation to accomplish this intent.

---

<sup>3</sup> At the same time, the phrase “if not a statutory advocate or Commission employee” was added in section 102.4(a)(2)(iii), because subsections (f) and (g) do alter the applicable rules for requesting records containing confidential security information for review if you are a statutory advocate or Commission employee, respectively.

The OAG, IRRC, and the PNA each raise concerns about requiring the challenger or requester to provide his or her social security number in order to challenge a designation or review confidential security information. In originally requiring social security numbers be provided, the Commission relied in part on the fact that the Federal Energy Regulatory Commission (“FERC”) regulations relating to critical energy infrastructure information contained a similar requirement at 18 CFR § 388.113(d)(3)(i). However, by final rule issued October 30, 2007 at 121 FERC ¶ 61,107 Dkt. No. RM06-23-000, FERC has amended its regulation at 18 CFR § 388.113(d)(3)(i) to eliminate the request for social security numbers in order to obtain critical energy infrastructure information. FERC found from experience that social security numbers are not needed to determine the legitimacy of requesters and that this change would also minimize privacy concerns without compromising security regarding release of critical energy infrastructure information. In light of this finding, we have similarly amended our language to remove social security numbers as an identification mechanism and have added requiring the use of “a valid photo identification” in its place as suggested by IRRC.<sup>4</sup>

Subsection (b) addresses the relevant factors the Commission will consider in determining whether to approve a challenge or request to review records containing confidential security information. Both IRRC and the OAG raise in their comments the question of whether the CSI Act even contemplates a balancing test like the one contained in the proposed rulemaking. The OAG further asks whether such a test, even if contemplated, is appropriate in regard to a challenge to a security designation, which, the OAG asserts, goes to whether a particular document meets the statutory definition and not

---

<sup>4</sup> Another concern raised by IRRC in this subsection is that subsections (a)(2)(iv) and (v) mention a 15-day time limit and it asks whether this is a reasonable amount of time. We believe the answer is yes given the fact that the CSI Act creates a 60-day deadline on the Commission to provide a written notification of its decision. 35 P.S. § 2141.3(c)(5). The two individual 15-day time limits ensure that the Commission can meet its 60-day statutory obligation to render its decision when one factors in that the Commission procedures require that any recommendations or proposed orders be provided to the Commissioners at least 9 days prior to the public meeting date and the fact that there are usually no more than two public meetings scheduled per month.

the need of an individual. IRRC raises a further concern that the rulemaking does not use the “reasonable grounds” test expressed in section 2141.3(c)(4), 35 P.S. § 2141.3(c)(4), and that the Commission should provide a test that is consistent with this language of the CSI Act.

While we agree that the use of a balancing test is not expressly contemplated in the CSI Act, it is not expressly excluded either. *See, e.g., Elite Indus. v. Pa. Pub. Util. Comm’n*, 832 A.2d 428, 431-32 (Pa. 2003) (an agency has discretion to devise regulations that interpret its statutory mandates). In this regard, a review of other state and federal regulations addressing the protection of confidential information reveals that use of a balancing test is common in this type of situation. FERC, for example, has created a similar balancing test in its regulations for determining when to release critical energy infrastructure information. 18 CFR § 388.113(d)(3)(ii). Our own general rule for handling confidential information uses a balancing test that has worked well over time. 52 Pa. Code § 5.423.

We agree, on the other hand, that the OAG’s concern about applying a balancing test to challenges is not needed and have amended the language in the final rulemaking to remove this test for challenges. Similarly, we have incorporated the “reasonable grounds” test used in the CSI Act as suggested by IRRC in the final regulation.

EAPA and PGW also offer several suggested changes that have been incorporated into subsection (b). In applying the balancing test, we have added “or to the public” after “the potential harm to the public utility” to make clear that we must take into consideration potential harm to the public in evaluating requests to review confidential security information. Terrorist acts are mainly directed at harming or intimidating the general public so including the public interest as part of the analysis is appropriate. We also incorporated, for clarification purposes, many of the language changes EAPA and

PGW offered for subsection (b)(1), (2), and (3). Similarly for clarification purposes, we incorporated the sentence suggested by EAPA and PGW for subsection (c) dealing with written notification of disposition.

As for subsection (d) relating to appeals of Commission decisions, both IRRC and the OAG question the necessity of the last two sentences that address how the Commonwealth Court will handle records allegedly containing confidential security information. We agree that since the last two sentences address procedures before Commonwealth Court and not the Commission and, in any event, the language merely repeats the statutory requirements, these last two sentences can be removed altogether from the regulation.

Finally, subsection (f) addresses how confidential security information is to be accessed by the statutory advocates. Both OSBA and the OCA raise concerns with this subsection. For example, OSBA complains that the use of the word “employee” limits the statutory advocate’s ability to obtain access to confidential security information for consultants and other expert witnesses hired by the statutory advocates as independent contractors. The OCA suggests that the regulation should be amended to require: (1) the statutory advocate to justify its need for the information to the Commission and not to the public utility, (2) the statutory advocate to execute the access agreement with the Commission and not with the public utility, and (3) the Commission to provide written notice to the public utility prior to disclosure. We agree with OSBA and the OCA that modifications are necessary and have incorporated amended language into the final rulemaking that addresses each concern.

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 find that the regulations establishing procedures for filing, challenging, and requesting confidential security information at 52 Pa. Code §§ 102.1-102.4 should be approved as set forth in Annex A, attached hereto; **THEREFORE,**

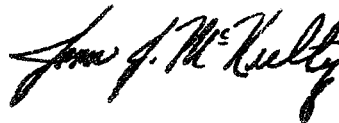
**IT IS ORDERED:**

1. That 52 Pa. Code Chapter 5 is hereby amended as set forth in Annex A hereto and that 52 Pa. Code Chapter 102 is hereby adopted as set forth in Annex A.
2. That the Secretary shall certify this Order and Annex A and deposit them with the Legislative Reference Bureau for publication in the *Pennsylvania Bulletin*.
3. That the Secretary shall submit this Order and Annex A to the Office of Attorney General for approval as to legality.
4. That the Secretary shall submit this Order and Annex A to the Governor's Budget Office for review of fiscal impact.
5. That the Secretary shall submit this Order and Annex A for review by the designated standing committees of both houses of the General Assembly and for review and approval by the Independent Regulatory Review Commission.
6. That a copy of this Order and Annex A shall be served upon the National Association of Water Companies, Pennsylvania Chapter; the Pennsylvania Newspaper

Association; 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.; Meckley's Limestone Products, Inc.; American Expediting Company; the Office of Trial Staff; the Office of Consumer Advocate; and the Small Business Advocate.

7. That the final regulations embodied in Annex A shall become effective upon publication in the *Pennsylvania Bulletin*.

BY THE COMMISSION



James J. McNulty  
Secretary

(SEAL)

ORDER ADOPTED: May 1, 2008

ORDER ENTERED: MAY 02 2008



**ANNEX A**

**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 IN NONADVERSARIAL PROCEEDINGS are addressed in Chapter 102 (relating to confidential security information).

**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 under Act 156 ("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:

Act 156 -- The Public Utility Confidential Security Information Disclosure Protection Act (35 P.S. §§ 2141.1-2141.6).

Commission -- The Pennsylvania Public Utility Commission.

**CHALLENGER -- A MEMBER OF THE PUBLIC THAT CHALLENGES A PUBLIC UTILITY RECORD AS CONSTITUTING CONFIDENTIAL SECURITY INFORMATION.**

Confidential security information -- THE TERM AS DEFINED IN 35 P.S.

§ 2141.2. ~~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 the following:~~

(i) ~~A vulnerability assessment which is submitted to the Environmental Protection Agency or 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 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 definition may 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 --* THE TERM AS DEFINED IN 35 P.S. § 2141.2.

~~(i) The plant and equipment of a public utility, including tangible and intangible real and personal property without limitation, and any 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.~~

~~(ii) The term also includes electric power generation.~~

*MASS DESTRUCTION --* THE TERM AS DEFINED IN 35 P.S. § 2141.2.

*Member of the public --* Includes A LEGAL RESIDENT OF THE UNITED STATES, ~~any citizen of this Commonwealth,~~ a public utility certified by the Commission,

the Office of Consumer Advocate, the Office of Small Business Advocate, the Office of Trial Staff or AUTHORIZED Commission EMPLOYEES. prosecutory staff.

Public utility -- THE TERM AS DEFINED IN 35 P.S. § 2141.2. 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 also includes 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 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.

*REQUESTER* -- A MEMBER OF THE PUBLIC THAT REQUESTS TO EXAMINE A PUBLIC UTILITY'S CONFIDENTIAL SECURITY INFORMATION BUT WHO IS NOT CHALLENGING SUCH DESIGNATION.

*Right-to-Know Law* -- 2008 PA. LEGIS. SERV. ACT 2008-3 (S.B. 1) (65 P.S. §§67.101-67.3104), OR ANY AMENDMENTS THERETO. ~~The act of June 21, 1957 (P.L. 390, No. 212) (65 P.S. §§ 66.1-66.9).~~

*Secretary* -- The Secretary of the Commission.

*Terrorist act* -- THE TERM AS DEFINED IN 35 P.S. § 2141.2. ~~An act constituting a violent offense intended to do one or more of the following:~~

~~(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 onsite. Unless required by order or other directive from the Commission or its staff that records containing confidential security information shall be filed with the Commission, public utilities shall do the following:

(1) Maintain any record containing confidential security information onsite.

(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 EMPLOYEES. ~~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. THE TRANSMITTAL LETTER WILL BE TREATED AS A PUBLIC RECORD AND MAY NOT CONTAIN ANY CONFIDENTIAL SECURITY INFORMATION.

(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.

(ii) Records that are to be treated as containing confidential security information and not subject to the Right-to-Know Law.

(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 LABELED AS CONTAINING CONFIDENTIAL SECURITY INFORMATION in a separate envelope marked "Confidential Security Information."

(4) REDACT THE PORTION OF THE RECORD THAT CONTAINS CONFIDENTIAL SECURITY INFORMATION FOR PURPOSES OF INCLUDING THE REDACTED VERSION OF THE RECORD IN THE PUBLIC FILE.

(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 (b), MAY will be made available to the public under the Right-to-Know Law.

(D) *COMMISSION'S RESPONSIBILITY WITH MARKED RECORDS.* WHEN A PUBLIC UTILITY FILES A RECORD CONTAINING CONFIDENTIAL SECURITY INFORMATION, THE UNOPENED ENVELOPE WILL BE GIVEN TO THE COMMISSION EMPLOYEE AUTHORIZED TO REVIEW THE FILING. THE AUTHORIZED PERSON WILL MAKE A PRELIMINARY DETERMINATION WHETHER THE INFORMATION HAS BEEN PROPERLY DESIGNATED IN ACCORDANCE WITH THE DEFINITION OF CONFIDENTIAL SECURITY INFORMATION UNDER ACT 156. IF THE MARKED INFORMATION IS DEEMED TO HAVE BEEN IMPROPERLY DESIGNATED, THE AUTHORIZED PERSON WILL GIVE THE SUBMITTER AN OPPORTUNITY TO RESUBMIT THE RECORD WITHOUT THE IMPROPER DESIGNATION. IF THE SUBMITTER DISAGREES WITH THIS PRELIMINARY DETERMINATION AND ADVISES THE AUTHORIZED PERSON, THE AUTHORIZED PERSON MAY SUBMIT THE DISPUTE TO THE LAW BUREAU FOR DETERMINATION AS A CHALLENGE IN ACCORDANCE WITH SECTION 102.4.

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

WITHIN 30 DAYS OF REFILING THE RECORDS CONTAINING CONFIDENTIAL SECURITY INFORMATION, THE COMMISSION WILL DESTROY THE ORIGINAL PRE-ACT 156 FILED RECORDS, WITH A CERTIFICATION OF DESTRUCTION PROVIDED TO THE PUBLIC UTILITY, OR WILL RETURN THE RECORDS TO THE PUBLIC UTILITY BY A SECURE METHOD.

(F)(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 section. 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 MAY CONTAIN contains confidential security information, the Law Bureau will PROVIDE advise the affected public utility WITH WRITTEN NOTICE OF ITS DETERMINATION and give it an opportunity to resubmit and replace the record with a copy that is marked "Confidential Security Information" pursuant to subsection (E)(d). FAILURE BY THE PUBLIC



UTILITY TO RESPOND TO THE WRITTEN NOTICE WITHIN 15 DAYS FROM THE DATE OF THE NOTICE SHALL BE DEEMED A NEGATIVE RESPONSE AS TO WHETHER THE RECORD CONTAINS CONFIDENTIAL SECURITY INFORMATION.

(G)(f) Electronic submissions. THE COMMISSION DOES NOT AUTHORIZE THE USE OF E-MAIL OR ANY OTHER ELECTRONIC MAIL SYSTEM TO TRANSMIT RECORDS CONTAINING CONFIDENTIAL SECURITY INFORMATION. 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, the information submitted electronically will be made available to the public under the Right-to-Know Law.

**§ 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 WITHIN 5 DAYS 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 onsite 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 will be referred to the Office of Administrative Law Judge for recommended disposition by the Commission.

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

(2)(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 EMPLOYEE staff, shall provide his full name, address, telephone number and A VALID PHOTO IDENTIFICATION 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, IF NOT A STATUTORY ADVOCATE OR COMMISSION EMPLOYEE, 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 will 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 FOR REQUESTS TO REVIEW.* 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 OR TO THE PUBLIC of disclosing information relating to THE PUBLIC UTILITY'S ~~its security is less than the challenger's or requester's need for the~~ information. IF THE COMMISSION DETERMINES THAT THERE ARE REASONABLE GROUNDS TO BELIEVE DISCLOSURE MAY RESULT IN A SAFETY RISK, INCLUDING THE RISK OF HARM TO ANY PERSON, OR MASS

DESTRUCTION, THEN THE COMMISSION WILL DENY THE REQUEST. 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 PREPARED BY THE LAW BUREAU. THE AGREEMENT SHALL BE EXECUTED PRIOR TO ANY RELEASE OF CONFIDENTIAL SECURITY INFORMATION.

(2) The requester's willingness to CONSENT ~~be subjected~~ to a criminal background check.

(3) The conditions, if any, to place on release of the information AND THE REQUESTER'S WILLINGNESS TO CONSENT IN WRITING TO COMPLY WITH SUCH CONDITIONS.

(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 REQUEST FOR REVIEW WILL BE GRANTED, THIS GRANT MAY NOT

INVALIDATE OR OTHERWISE AFFECT THE RECORD'S DESIGNATION AS CONTAINING CONFIDENTIAL SECURITY INFORMATION FOR ANY OTHER PURPOSE, REQUEST, OR CHALLENGE. ~~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 under 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 COMMISSION public utility with a justification for the need of the information and execute access agreements WITH THE COMMISSION that summarize responsibilities and personal liabilities when confidential security information is knowingly or recklessly released.

published or otherwise disclosed. THE COMMISSION WILL PROVIDE WRITTEN NOTICE TO THE AFFECTED PUBLIC UTILITY PRIOR TO DISCLOSURE OF THE CONFIDENTIAL SECURITY INFORMATION TO THE REQUESTING STATUTORY ADVOCATE.

(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 will 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.

(H) *DISCOVERY REQUESTS IN ADVERSARIAL PROCEEDINGS.* THE CHALLENGE AND REQUEST TO REVIEW PROCEDURES DESCRIBED IN THIS CHAPTER DO NOT APPLY TO EXCHANGES OF DOCUMENTS AMONG PARTIES IN ADVERSARIAL PROCEEDINGS PENDING BEFORE THE COMMISSION. IN ADVERSARIAL PROCEEDINGS, A PARTY WISHING TO LIMIT AVAILABILITY OF RECORDS CONTAINING CONFIDENTIAL SECURITY

INFORMATION MUST MOVE FOR AN APPROPRIATE PROTECTIVE ORDER  
BEFORE THE PRESIDING OFFICER IN ACCORDANCE WITH ACCEPTED RULES  
AND PROCEDURES FOR ISSUING PROTECTIVE ORDERS.

\* \* \* \* \*

ERIK A ROSS  
DEWEY & LEBOEUF LLP  
1101 NEW YORK AVE NW  
SUITE 1100  
WASHINGTON DC 20005-4213

SHAUN A SPARKS  
OFFICE OF CONSUMER  
ADVOCATE  
555 WALNUT ST 5<sup>TH</sup> FLOOR  
FORUM PLACE  
HARRISBURG PA 17101-1923

DONNA M J CLARK  
ENERGY ASSN OF PA  
800 NORTH THIRD STREET  
SUITE 301  
HARRISBURG PA 17102

DANIEL CLEARFIELD ESQ  
WOLF BLOCK SCHORR &  
SOLIS-COHEN LLP  
213 MARKET ST 9<sup>TH</sup> FLOOR  
P O BOX 865  
HARRISBURG PA 17108-0865

MELISSA BEVAN MELEWSKY  
PA NEWSPAPER ASSN  
3899 N FRONT STREET  
HARRISBURG PA 17110

WILLIAM R LLOYD JR  
SMALL BUSINESS ADVOCATE  
OFFICE OF SMALL BUSINESS  
ADVOCATE  
SUITE 1102 COMMERCE BLDG  
300 NORTH SECOND STREET  
HARRISBURG PA 17101





PENNSYLVANIA PUBLIC UTILITY COMMISSION  
COMMONWEALTH OF PENNSYLVANIA  
HARRISBURG, PENNSYLVANIA

May 28, 2008

WENDELL F. HOLLAND  
CHAIRMAN

The Honorable Arthur Coccodrilli  
Chairman  
Independent Regulatory Review Commission  
14th Floor, Harristown II  
333 Market Street  
Harrisburg, PA 17101

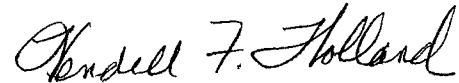
Re: L-00071085/57-256  
Final Rulemaking  
Re Implementation of the Public  
Utility Confidential Security  
Information Disclosure Protection Act  
52 Pa. Code Chapter 102

Dear Chairman Coccodrilli:

Enclosed please find one (1) copy of the regulatory documents concerning the above-captioned rulemaking. Under Section 745.5(a) of the Regulatory Review Act, the Act of June 30, 1989 (P.L. 73, No. 19) (71 P.S. §§745.1-745.15) the Commission, on November 21, 2007, submitted a copy of the Notice of Proposed Rulemaking to the House Committee on Consumer Affairs, the Senate Committee on Consumer Protection and Professional Licensure and to the Independent Regulatory Review Commission (IRRC). This notice was published at 37 Pa.B. 6421, on December 8, 2007. In compliance with Section 745.5(b.1) copies of all comments received were provided to your Commission and the Committees.

In preparing this final form rulemaking, the Public Utility Commission has considered all comments received from the Committees, IRRRC and the public.

Very truly yours,

A handwritten signature in cursive script, reading "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  
Regulatory Coordinator DelBiondo  
Assistant Counsel Hisiro  
Judy Bailets, Governor's Policy Office

TRANSMITTAL SHEET FOR REGULATIONS SUBJECT  
TO THE REGULATORY REVIEW ACT

ID Number: L-00070185/57-256

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

Pennsylvania Public Utility Commission

RECEIVED  
2008 MAY 28 PM 1:38  
INDEPENDENT REGULATORY  
REVIEW COMMISSION

TYPE OF REGULATION

- ☐ 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

Date

Signature

Designation

5/28/08

*Marion Santoro*

HOUSE COMMITTEE (Preston)

Consumer Affairs

5/28/08

*Mary Walmer*

SENATE COMMITTEE (Tomlinson)

Consumer Protection and  
Professional Licensure

5/28/08

*Kathy Cooper*

Independent Regulatory  
Review Commission

Attorney General

Legislative Reference  
Bureau