PHONE: (717) 783-5417
FAX: (717) 783-2664
irrc@irrc.state.pa.us
http://www.irrc.state.pa.us

INDEPENDENT REGULATORY REVIEW COMMISSION
333 MARKET STREET, 14TH FLOOR, HARRISBURG, PA 17101

August 18, 2004

Honorable Terrance J. Fitzpatrick, Chairman
Pennsylvania Public Utility Commission
Keystone Building, 3rd Floor
400 North Street
Harrisburg, PA 17105

Re: Regulation #57-234 (IRRC #2404)
Pennsylvania Public Utility Commission
Public Utility Security Planning and Readiness

Dear Chairman Fitzpatrick:

Enclosed are the Commission's comments for consideration when you prepare the final version of this regulation. These comments are not a formal approval or disapproval of the regulation. However, they specify the regulatory review criteria that have not been met.

The comments will be available on our website at www.irrc.state.pa.us. If you would like to discuss them, please contact my office at 783-5417.

Sincerely,

Robert E. Nyce
Executive Director
evp
Enclosure
cc: Honorable Robert J. Flick, Majority Chairman, House Consumer Affairs Committee
Honorable Joseph Preston, Jr., Democratic Chairman, House Consumer Affairs Committee
Honorable Robert M. Tomlinson, Chairman, Senate Consumer Protection and Professional Licensure Committee
Honorable Lisa M. Boscola, Minority Chairman, Senate Consumer Protection and Professional Licensure Committee

Comments of the Independent Regulatory Review Commission

on

Pennsylvania Public Utility Commission Regulation #57-234 (IRRC #2404)

Public Utility Security Planning and Readiness

August 18, 2004

We submit for your consideration the following comments that include references to the criteria in the Regulatory Review Act (71 P.S. § 745.5b) which have not been met. The Pennsylvania Public Utility Commission (PUC) must respond to these comments when it submits the final-form regulation. The public comment period for this regulation closed on July 19, 2004. If the final-form regulation is not delivered within two years of the close of the public comment period, the regulation will be deemed withdrawn.

1. Section 101.1. Purpose. – Timetable for compliance; Clarity.

This section establishes the purpose of Chapter 101, relating to public utility preparedness through self certification. It uses the terms "jurisdictional utility" and "infrastructure." These terms are not defined. The PUC should either define these terms in Section 101.2, relating to definitions, or include a cross-reference to where these definitions can be found.

2. Section 101.2. Definitions. – Clarity.

Business continuity plan, contingency planning, business resumption and emergency response plan

This section uses three phrases to describe potential service interruptions. These include "change or unforeseen circumstances" in the definitions of "business continuity plan" and "contingency planning"; "natural causes or sabotage" in the definition of "emergency response plan"; and "disaster" in the definition of "business resumption." Based on the executive summary included with the regulatory package, the aforementioned terms are subsumed under the defined term of "abnormal operating conditions." Therefore, we recommend that these phrases be replaced with that defined term.

Business continuity plan, cyber security plan, emergency response plan and physical security plan

These definitions all contain a brief description of the term and duties for jurisdictional utilities to perform. As substantive provisions, the duties should not be included in these definitions. Rather, they should be moved to Section 101.3, relating to plan requirements.

Business recovery

The phrase "less time-sensitive business operations" is included in this definition. The PUC should include examples of "less time-sensitive business operations," in the preamble or the final-form regulation.

Critical Functions

This definition includes the phrase "several business days." This time frame is vague. The PUC should replace this phrase with a specific time frame.

Cyber security plan

The phrase "appropriate backup" is contained in the definition of "cyber security plan." The PUC should provide examples of "appropriate backup," or define this phrase in the final-form regulation.

Paragraph (iv) begins with the phrase "a recognition of." This phrase is superfluous, and should be deleted.

Emergency response plan

This definition includes the phrase "emergency management system." What is the "emergency management system"? The PUC should either define this term in the final-form regulation or include an appropriate cross-reference.

3. Section 101.3. Plan requirements. – Economic impact; Clarity.

Subsection (a)

This subsection requires jurisdictional utilities to develop and maintain written physical security, cyber security, emergency response and business continuity plans. Do these four plans have to be independent, or can they be one single plan? The PUC should explain what would be an acceptable format for maintaining these plans.

Subsection (c)

This subsection requires utilities to "maintain a testing schedule of these plans." Subsection (d) requires that utilities submit The Physical and Cyber Security Planning Self Certification Form (form), which asks if the various plans have been tested. However, as currently written, this regulation does not require utilities to actually test their plans.

The PUC has indicated that the intent of this regulation is to require annual testing of each plan. Why is annual testing needed? If the PUC justifies the need for annual testing of each plan, the final-form regulation should be amended to reflect this requirement. Also, we recommend that a definition of the term "test" be added to Section 101.2, relating to definitions.

4. Subsection 101.5. Confidentiality of self certification form. – Clarity.

This section refers to the form filed with the PUC as a "Physical and Cyber Security Self Certification Form." In Appendix A, the form is titled, "Physical and Cyber Security *Planning* Self Certification." (Emphasis added.) Section 101.1, relating to purpose, also refers to the form as the "Physical and Cyber Security *Planning* Self Certification." (Emphasis added.) For consistency, the PUC should add the word "Planning" to the form referenced in this section.

5. Section 101.6. Compliance. – Clarity.

Subsections (b) and (c)

These subsections state that the PUC may review the plans of a utility and inspect a utility's facility. We have two concerns. First, the PUC should explain the manner in which it will make

a request when it elects to review the plans or facilities of a utility. For instance, will the PUC make a written request to the utility to review its plans or facilities?

Second, the PUC should explain the procedures involved with inspecting the facilities of a utility. Will the PUC conduct their inspection during normal business hours, and will the utility have notice that an inspection will occur?

Subsection (d)

This subsection allows a jurisdictional utility to submit a business continuity plan, cyber security plan, emergency response plan and physical security plan prepared for another entity if the other authority requires a "substantially similar plan." We have two concerns.

First, if the other entity requires information not prescribed by the PUC, will that information be considered public or proprietary information? The PUC should explain.

Second, the phrase "substantially similar plan" is vague. The PUC should include specific guidelines in the final-form regulation for a jurisdictional utility to determine whether the plan it must file for another entity could be used to fulfill the requirements set forth in this regulation, or replace the existing phrase with "meets the requirements of."

6. Appendix A. Physical and cyber security planning self certification. – Reasonableness: Clarity.

Appendix A contains the form utilities are required to submit to the PUC. We have three concerns.

First, Item Nos. 2, 5, 9 and 12 ask if specific plans have been "reviewed *and* updated in the past year." (Emphasis added.) If no update is necessary, would a utility's review suffice? The PUC should consider changing the above-mentioned lines to include the phrase "reviewed and updated as needed."

Second, Item No. 7 asks the following question: "Has your company performed a vulnerability or risk assessment analysis as it relates to physical and/or cyber security?" In order for the regulated community to understand what is expected during a "vulnerability or risk assessment analysis," that phrase should be defined in Section 101.2 of the regulation. In addition, the inclusion of the phrase "and/or" would make it difficult for the regulated community to know what is expected of them. Does the PUC expect each company to perform an analysis of their physical *and* cyber security each year? The final-form regulation should clarify this provision.

Finally, can this form be electronically filed with the PUC, or will utilities have to submit the form by mail, hand delivery or fax? The PUC should consider allowing electronic submission of this form.

7. Miscellaneous clarity.

Section 101.3, relating to plan requirements, contains two subsections labeled (d). The final-form regulation should correct this typographical error.

Facsimile Cover Sheet

Kristine M. Shomper
Administrative Officer

Phone: (717) 783-5419
Fax #: (717) 783-2664
E-mail: kriss@irrc.state.pa.us
Website: www.irrc.state.pa.us

INDEPENDENT REGULATORY REVIEW COMMISSION
333 MARKET STREET, 14TH FLOOR, HARRISBURG, PA 17101

2004 AUG 18 PM 12:

To: Sherri A. DelBiondo
Regulatory Review Coordinator
Law Bureau
Agency: Pennsylvania Public Utility Commission
Phone: 2-4597
Fax: 3-3458
Date: August 18, 2004
Pages: 5

Comments: We are submitting the Independent Regulatory Review Commission's comments on the Pennsylvania Public Utility Commission's regulation #57-234 (IRRC #2404). Upon receipt, please sign below and return to me immediately at our fax number 783-2664. We have sent the original through interdepartmental mail. You should expect delivery in a few days. Thank you.

Accepted by: S DelBiondo **Date:** 8-18-04

Fax5

RECEIVED TIME AUG. 18. 11:32AM PRINT TIME AUG. 18. 11:33AM