

**Subpart E. PUBLIC UTILITY SECURITY
PLANNING AND READINESS**

CHAPTER 102. CONFIDENTIAL SECURITY INFORMATION

- Sec.
102.1. Purpose.
102.2. Definitions.
102.3. Filing procedures.
102.4. Challenge procedures to confidentiality designation.

Authority

The provisions of this Chapter 102 issued under the Public Utility Confidential Security Information Disclosure Protection Act (35 P. S. §§ 2141.1—2141.6); and 66 Pa.C.S. 501 and 1501, unless otherwise noted.

Source

The provisions of this Chapter 102 adopted August 22, 2008, effective August 23, 2008, 38 Pa.B. 4608, unless otherwise noted.

Cross References

This chapter cited in 52 Pa. Code § 5.423 (relating to orders to limit availability of proprietary 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 section 2 of Act 156 (35 P. S. § 2141.2).

Facilities—The term as defined in section 2 of Act 156.

Mass destruction—The term as defined in section 2 of Act 156.

Member of the public—The term includes a legal resident of the United States, a public utility certified by the Commission, the Office of Consumer Advocate, the Office of Small Business Advocate or authorized Commission employees.

Public utility—The term as defined in section 2 of Act 156.

Requester—A member of the public that requests to examine a public utility's confidential security information but who is not challenging the designation.

Right-to-Know Law—65 P. S. §§ 67.101—67.3104.

Secretary—The Secretary of the Commission.

Terrorist act—The term as defined in section 2 of Act 156.

§ 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.

(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 page of the record containing confidential security information with the words "Confidential Security Information" and place all 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 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 § 102.4 (relating to challenge procedures to confidentiality designation).

(e) *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) *Commission's responsibility with unmarked records.* 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 confidential security information, the Law Bureau will provide 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). 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) *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.

§ 102.4. Challenge procedures to confidentiality designation.

(a) *General rule for challenges or requests to review.* When a member of the public 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.

(1) The matter will be referred to the Law Bureau for recommended disposition by the Commission.

(2) 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, shall provide his full name, address, telephone number and a valid photo identification 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 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 requester's need for the information. Applying this balancing test, a 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 security is less than the 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, the Commission will deny the request. In determining whether to grant a written request to review a record containing confidential security information, the Commission or the Law Bureau will consider, along with other relevant factors, the following:

(1) The requester's willingness to sign a nondisclosure 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 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 these 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.

(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.

(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 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.

Cross References

This section cited in 52 Pa. Code § 102.3 (relating to filing procedures).