RULES AND REGULATIONS

Title 52—PUBLIC UTILITIES

PENNSYLVANIA PUBLIC UTILITY COMMISSION

[52 PA. CODE CHS. 5 AND 102]

[L-00070185/57-256]

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

The Pennsylvania Public Utility Commission on May 1, 2008, adopted a final-form 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, (717) 783-2812.

Executive Summary

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 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. See 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 (relating to confidential security information) 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 § 5.423 (relating to orders to limit availability of proprietary information) by adding a new subsection (g) whose sole purpose is to refer the reader to the new Chapter 102.

.

Public Meeting held
May 1, 2008

Commissioners Present: Wendell F. Holland, Chairperson; James H. Cawley, Vice Chairperson; Tyrone J. Christy; Kim Pizzingrilli

Final Rulemaking Regarding Implementation of the Public Utility Confidential Security Information Disclosure Protection Act;
Doc. No. L-00070185

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 at 37 Pa.B. 6421 (December 8, 2007). 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-form 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 *Pennsylvania 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 the 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 in § 102.3 (relating to filing procedure) 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).[1] 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, and the like, are current and up-to-date, and through the performance of management audits under section 516 of the Public Utility Code. See 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 under 52 Pa. Code § 101.5 (relating to confidentiality self certification form).

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, and the like remains the current plan, map, and the like 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 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. See 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)—(f) as the new (e)—(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 Department of Environmental Resources (Department) 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 Department 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

[1] For the same reason, we have made the identical change in § 102.4(a)(2)(i) and (iii).

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 refiling 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 refiled 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 under the self-certification process discussed previously.

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 refile unmarked records is already established in subsection (e).[2]

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

Section 102.4 (relating to challenge procedures to confidentiality designation) 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.

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.[3] 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 previous 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 the 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.

The OAG, IRRC and the PNA each raise concerns about requiring the challenger or requester to provide his Social Security number 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

[2] 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.

[3] At the same time, the phrase "if not a statutory advocate or Commission employee" was added in § 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.

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 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.[4]

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 the need of an individual. IRRC raises a further concern that the rulemaking does not use the "reasonable grounds" test expressed in section 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, and the like, *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. See 52 Pa. Code § 5.423 (relating to orders to limit availability of proparitary information).

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 1—6 of the Public Utility Confidential Security Information Disclosure Protection Act (35 P. S. §§ 2141.1—2141.6); 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 and 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 That:

1. 52 Pa. Code Chapters 5 and 102 are hereby amended by amending § 45.423 and adding §§ 102.1—102.4 to read as set forth in Annex A.

2. The Secretary shall certify this Order and Annex A and deposit them with the Legislative Reference Bureau for publication in the *Pennsylvania Bulletin*.

3. The Secretary shall submit this Order and Annex A to the Office of Attorney General for approval as to legality.

4. The Secretary shall submit this Order and Annex A to the Governor's Budget Office for review of fiscal impact.

5. The Secretary shall submit this Order and Annex A for review by the designated standing committees of both

[4] 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.

houses of the General Assembly and for review and approval by the Independent Regulatory Review Commission.

6. 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. The final-form regulations embodied in Annex A shall become effective upon publication in the *Pennsylvania Bulletin*.

JAMES J. MCNULTY,
Secretary

(*Editor's Note*: For the text of the order of the Independent Regulatory Review Commission relating to this document, see 38 Pa.B. 4045 (July 26, 2008).)

Fiscal Note: Fiscal Note 57-256 remains valid for the final adoption of the subject regulations.

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.

(a) *General rule for adversarial proceedings*. A petition for protective order to limit the disclosure of a trade secret or other confidential information on the public record will be granted only when a party demonstrates that the potential harm to the party of providing the information would be substantial and that the harm to the party if the information is disclosed without restriction outweighs the public's interest in free and open access to the administrative hearing process. A protective order to protect trade secrets or other confidential information will apply the least restrictive means of limitation which will provide the necessary protections from disclosure. In considering whether a protective order to limit the availability of proprietary information should issue, the Commission or the presiding officer should consider, along with other relevant factors, the following:

(1) The extent to which the disclosure would cause unfair economic or competitive damage.

(2) The extent to which the information is known by others and used in similar activities.

(3) The worth or value of the information to the party and to the party's competitors.

(4) The degree of difficulty and cost of developing the information.

(5) Other statutes or regulations dealing specifically with disclosure of the information.

(b) *General rule for nonadversarial proceedings*. A petition for protective order limiting the disclosure of a trade secret or other confidential information in a nonadversarial proceeding shall be referred to the Law Bureau for recommended disposition by the Commission. The Commission will not disclose any material that is the subject of a protective order under this provision during the pendency of such a request.

(c) *Restrictions*.

(1) A protective order to restrict disclosure of proprietary information may require that a party receive, use or disclose proprietary information only for the purposes of preparing or presenting evidence, cross-examination or argument in the proceeding, or may restrict its inclusion in the public record.

(2) A protective order may require that parts of the record of a proceeding which contain proprietary information including, but not limited to, exhibits, writings, direct testimony, cross-examination, argument and responses to discovery, will be sealed and remain sealed unless the proprietary information is released from the restrictions of the protective order by agreement of the parties, or pursuant to an order of the presiding officer or the Commission.

(3) A public reference to proprietary information by the Commission or by a party afforded access thereto shall be to the title or exhibit reference in sufficient detail to permit persons with access to the proprietary information to fully understand the reference and not more. The proprietary information shall remain a part of the record, to the extent admitted, for purposes of administrative or judicial review.

(4) Prior to the issuance of a protective order, a party may not refuse to provide information which the party reasonably believes to be proprietary to a party who agrees to treat the information as if it were covered by a protective order until the presiding officer or the Commission issues the order or determines that issuance of the order would not be appropriate. The party claiming the privilege shall file a petition for protective order under subsection (a) within 14 days of the date the request for information was received.

(5) A party receiving proprietary information under this section retains the right, either before or after receipt of the information, to challenge the legitimacy of the claim that the information is proprietary, and to challenge the admissibility of the proprietary information.

(d) *Access to representatives of parties*. Proprietary information provided to a party under this section shall be released to the counsel and eligible outside experts of the receiving party unless the party who is releasing the information demonstrates that the experts or counsel previously violated the terms of a recent protective order issued by the Commission. To be eligible to receive proprietary information, the expert, subject to the following exception, may not be an officer, director, stockholder, partner, owner or employee of a competitor of the producing party. An expert will not be ineligible on account of being a stockholder, partner or owner of a competitor or affiliate unless the ownership interest is valued at more than $10,000 or constitutes a more than 1% interest, or both. No other persons may have access to the proprietary information except as authorized by order of the Commission or of the presiding officer.

(e) *Special restrictions*. A protective order which totally prohibits the disclosure of a trade secret or other confidential information, limits the disclosure to particular

parties or representatives of parties—except as permitted by subsection (c)—or which provides for more restrictive rules than those permitted in subsections (b) and (c), will be issued only in extraordinary circumstances and only when the party from whom the information is sought demonstrates that a greater restriction is necessary to avoid severe and extreme prejudice.

(f) *Return of proprietary information.* A party providing proprietary information under this section may request that the parties receiving the information return the information and the copies thereof to the party at the conclusion of the proceeding, including appeals taken.

(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).

Subpart E. PUBLIC UTILITY SECURITY PLANNING AND READINESS

CHAPTER 102. CONFIDENTIAL SECURITY INFORMATION

Sec.

§ 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 confiden-

tial 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.

[Pa.B. Doc. No. 08-1521. Filed for public inspection August 22, 2008, 9:00 a.m.]

Title 58—RECREATION

GAME COMMISSION

[58 PA. CODE CHS. 139 AND 141]

Seasons and Bag Limits and Hunting and Trapping

To effectively manage the wildlife resources of this Commonwealth, the Game Commission (Commission), at its June 24, 2008, meeting, adopted the following rulemaking:

Amend § 141.1 (relating to special regulations areas) to permit hunters in the special regulation areas to harvest more than one deer at a time without first lawfully tagging previous harvests, provided all deer harvested are lawfully tagged immediately thereafter. Also amend §§ 139.2 and 141.41 (relating to definitions; and general) to relocate the prohibition against successive takings of deer prior to lawfully tagging a deer previously harvested from § 139.2 to § 141.41 where it is more appropriately located.

The final-form rulemaking will have no adverse impact on the wildlife resources of this Commonwealth.

The authority for the final-form rulemaking is 34 Pa.C.S. (relating to Game and Wildlife Code) (code).

Notice of proposed rulemaking was published at 38 Pa.B. 3243 (June 14, 2008).

1. *Purpose and Authority*

Formerly, § 139.2 defined "field possession limit for deer" in such a manner so as to prohibit the harvest of a second deer (when multiple harvests per day are authorized) before tagging a deer previously harvested. In light of its continuing efforts to find solutions to the overabundant deer populations in the urban environments found in the Special Regulation Areas, the Commission amended § 141.1 to allow a hunter to harvest more than one deer at a time without first lawfully tagging previous harvests, provided all deer harvested are lawfully tagged immediately thereafter. For all other areas of the Commonwealth outside of the Special Regulations Areas, the traditional "tag before second harvest" requirement remains the same, but has been relocated from § 139.2 to § 141.41 where it is more appropriately located.

Section 2102(a) of the code (relating to regulations) provides that "The commission shall promulgate such regulations as it deems necessary and appropriate concerning game or wildlife and hunting or furtaking in this Commonwealth, including regulations relating to the protection, preservation and management of game or wildlife and game or wildlife habitat, permitting or prohibiting hunting or furtaking, the ways, manner, methods and means of hunting or furtaking, and the health and safety of persons who hunt or take wildlife or may be in the vicinity of persons who hunt or take game or wildlife in this Commonwealth." The amendments to §§ 139.2, 141.1 and 141.41 were adopted under this authority.

2. *Regulatory Requirements*

The final-form rulemaking amended § 141.1 to allow a hunter in the Special Regulation Areas to harvest more than one deer at a time without first lawfully tagging previous harvests, provided all deer harvested are lawfully tagged immediately thereafter. The final-form rulemaking also amended §§ 139.2 and 141.41 to relocate the general prohibition against successive takings of deer

prior to lawfully tagging a deer previously harvested from § 139.2 to § 141.41, where it is more appropriately located.

3. *Persons Affected*

Persons wishing to hunt or trap white-tailed deer within this Commonwealth may be affected by the final-form rulemaking.

4. *Comment and Response Summary*

There were no official comments received regarding this final-form rulemaking.

5. *Cost and Paperwork Requirements*

The final-form rulemaking should not result in any additional cost or paperwork.

6. *Effective Date*

The final-form rulemaking will be effective upon final publication in the *Pennsylvania Bulletin* and will remain in effect until changed by the Commission.

7. *Contact Person*

For further information regarding the final-form rulemaking, contact Richard R. Palmer, Director, Bureau of Wildlife Protection, 2001 Elmerton Avenue, Harrisburg, PA 17110-9797, (717) 783-6526.

Findings

The Commission finds that:

(1) Public notice of intention to adopt the administrative amendments adopted by this order has been given under sections 201 and 202 of the act of July 31, 1968 (P. L. 769, No. 240) (45 P. S. §§ 1201 and 1202) and the regulations thereunder, 1 Pa. Code §§ 7.1 and 7.2.

(2) The adoption of these amendments of the Commission in the manner provided in this order is necessary and appropriate for the administration and enforcement of the authorizing statute.

Order

The Commission, acting under authorizing statute, orders that:

(a) The regulations of the Commission, 58 Pa. Code Chapters 139 and 141, are amended by amending §§ 139.2, 141.1 and 141.41 to read as set forth at 37 Pa.B. 3243.

(b) The Executive Director of the Commission shall certify this order, 37 Pa.B. 3243 and deposit them with the Legislative Reference Bureau as required by law.

(c) This order shall become effective upon final-form publication in the *Pennsylvania Bulletin*.

CARL G. ROE,
Executive Director

Fiscal Note: Fiscal Note 48-269 remains valid for the final adoption of the subject regulations.

[Pa.B. Doc. No. 08-1522. Filed for public inspection August 22, 2008, 9:00 a.m.]