

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

Chap.		Sec.
101.	PUBLIC UTILITY SECURITY PLANNING AND READINESS	101.1
102.	CONFIDENTIAL SECURITY INFORMATION	102.1

**CHAPTER 101. PUBLIC UTILITY PREPAREDNESS
THROUGH SELF CERTIFICATION**

Sec.	
101.1.	Purpose.
101.2.	Definitions.
101.3.	Plan requirements.
101.4.	Reporting requirements.
101.5.	Confidentiality of self certification form.
101.6.	Compliance.
101.7.	Applicability.

Authority

The provisions of this Chapter 101 issued under the Public Utility Code, 66 Pa.C.S. §§ 501, 504—506 and 1501, unless otherwise noted.

Source

The provisions of this Chapter 101 adopted June 10, 2005, effective June 11, 2005, 35 Pa.B. 3299, unless otherwise noted.

Cross References

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

§ 101.1. Purpose.

This chapter requires a jurisdictional utility to develop and maintain appropriate written physical security, cyber security, emergency response and business continuity plans to protect this Commonwealth’s infrastructure and ensure safe, continuous and reliable utility service. A jurisdictional utility shall submit a Self Certification Form to the Commission documenting compliance with this chapter.

§ 101.2. Definitions.

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

Abnormal operating condition—A condition possibly showing a malfunction of a component or deviation from normal operations that may:

- (i) Indicate a condition exceeding design limits.
- (ii) Result in a hazard to person, property or the environment.

Business continuity plan—A written plan that will ensure the continuity or uninterrupted provision of operations and services through arrangements and procedures that enable a utility to respond to an event that could occur by abnormal operating conditions.

Business recovery—The process of planning for and implementing expanded operations to address less time-sensitive business operations immediately following an abnormal operating condition.

Business resumption—The process of planning for and implementing the restarting of defined business operations following an abnormal operating condition, usually beginning with the most critical or time-sensitive functions and continuing along a planned sequence to address all identified areas required by the business.

Contingency planning—The process of developing advance arrangements and procedures that enable a jurisdictional utility to respond to an event that could occur by abnormal operating conditions.

Critical functions—Business activities or information that cannot be interrupted or unavailable for several business days without significantly jeopardizing operations of the organization.

Cyber security—The measures designed to protect computers, software and communications networks that support, operate or otherwise interact with the company's operations.

Cyber security plan—A written plan that delineates a jurisdictional utility's information technology disaster plan.

Emergency response plan—A written plan describing the actions a jurisdictional utility will take if an abnormal operating condition exists.

Infrastructure—The systems and assets so vital to the utility that the incapacity or destruction of the systems and assets would have a debilitating impact on security, economic security, public health or safety, or any combination of those matters.

Jurisdictional utility—A utility subject to the reporting requirements of § 27.10, § 29.43, § 31.10, § 33.103, § 57.47, § 59.48, § 61.28, § 63.36 or § 65.19.

Mission critical—A term used to describe essential equipment or facilities to the organization's ability to perform necessary business functions.

Physical security—The physical (material) measures designed to safeguard personnel, property and information.

Physical security plan—A written plan that delineates the response to security concerns at mission critical equipment or facilities.

Responsible entity—The person or organization within a jurisdictional utility designated as the security or emergency response liaison to the Commission.

Self Certification Form—The Public Utility Security Planning and Readiness Self Certification Form.

Test—A trial or drill of physical security, cyber security, emergency response and business continuity plans. Testing may be achieved through a sum of continuous partial testing rather than one distinct annual drill when an entire plan is tested from beginning to end.

§ 101.3. Plan requirements.

(a) A jurisdictional utility shall develop and maintain written physical and cyber security, emergency response and business continuity plans.

(1) A physical security plan must, at a minimum, include specific features of a mission critical equipment or facility protection program and company procedures to follow based upon changing threat conditions or situations.

(2) A cyber security plan must, at a minimum, include:

(i) Critical functions requiring automated processing.

(ii) Appropriate backup for application software and data. Appropriate backup may include having a separate distinct storage media for data or a different physical location for application software.

(iii) Alternative methods for meeting critical functional responsibilities in the absence of information technology capabilities.

(iv) A recognition of the critical time period for each information system before the utility could no longer continue to operate.

(3) A business continuity plan must, at a minimum, include:

(i) Guidance on the system restoration for emergencies, disasters and mobilization.

(ii) Establishment of a comprehensive process addressing business recovery, business resumption and contingency planning.

(4) An emergency response plan must, at a minimum, include:

(i) Identification and assessment of the problem.

(ii) Mitigation of the problem in a coordinated, timely and effective manner.

(iii) Notification of the appropriate emergency services and emergency preparedness support agencies and organizations.

(b) A jurisdictional utility shall review and update these plans annually.

(c) A jurisdictional utility shall maintain and implement an annual testing schedule of these plans.

(d) A jurisdictional utility shall demonstrate compliance with subsections (a)—(c), through submittal of a Self Certification Form which is available at the Secretary's Bureau and on the Commission's website.

(e) A plan shall define roles and responsibilities by individual or job function.

(f) The responsible entity shall maintain a document defining the action plans and procedures used in subsection (a).

Cross Reference

This section cited in 52 Pa. Code § 101.6 (relating to compliance).

§ 101.4. Reporting requirements.

(a) A utility under the reporting requirements of § 27.10, § 57.47, § 59.48, § 61.28, § 63.36 or § 65.19 shall file the Self Certification Form at the time each Annual Financial Report is filed, under separate cover at Docket No. M-00031717.

(b) A utility not subject to the financial reporting requirements in subsection (a), but subject to the reporting requirements of § 29.43, § 31.10 or § 33.103 (relating to assessment reports; assessment reports; and reports) shall file the Self Certification Form at the time each Annual Assessment Report is filed, under separate cover at Docket No. M-00031717.

Cross References

This section cited in 52 Pa. Code § 101.6 (relating to compliance).

§ 101.5. Confidentiality of self certification form.

A Self Certification Form filed at the Commission is not a public document or record and is deemed confidential and proprietary.

§ 101.6. Compliance.

(a) The Commission will review a Self Certification Form filed under § 101.4 (relating to reporting requirements).

(b) The Commission may review a utility's cyber security plan, physical security plan, emergency response plan and business continuity plan under 66 Pa.C.S. §§ 504—506 (relating to reports by public utility; duty to furnish information to commission; and inspection of facilities and records).

(c) The Commission may inspect a utility's facility, to the extent utilized for or necessary to the provision of utility service, to assess performance of its compliance monitoring under 66 Pa.C.S. §§ 504—506.

(d) A utility that has developed and maintained a cyber security, physical security, emergency response or business continuity plan under the directive of another state or Federal entity that meets the requirements of § 101.3 (relating to plan requirements) may utilize that plan for compliance with this subpart, upon the condition that a Commission representative be permitted to review the cyber security, physical security, emergency response or business continuity plan. A company that is utilizing another entity's plan shall briefly describe the alternative plan and identify the authority that requires the alternative plan along with the Self Certification Form filed with the Commission.

§ 101.7. Applicability.

This chapter does not apply to an entity regulated by the Federal Railroad Safety Act (FRSA) (49 U.S.C.A. §§ 20101—20153) and the Hazardous Materials Transportation Act (HMTA) (49 U.S.C.A. §§ 5101—5127), if by August 10, 2005, it submits a certification to the Commission indicating that it has its own written physical and cyber security, emergency response and business continuity plans in place and is in compliance with the FRSA and HMTA.

[Next page is 102-1.]