Public Utility Security Planning and Readiness Self Certification Form
Frequently Asked Questions

1. Why did my company receive this form?
You received the Public Utility Security Planning and Readiness Self Certification Form because our records indicate that all or a portion of your business operations fall under the jurisdiction of the PA Public Utility Commission. **If you are unsure about what plans are being referenced for self-certification, please see the answers to questions 8, 9, 11 and 12, below.**

2. Does my company need to fill out this form?
If all or a portion of your business operations have been granted operating rights under the jurisdiction of the PA Public Utility Commission, then yes, your company should complete and return this form.

3. If I am a single vehicle truck/taxi/limousine owner and operator, do I still need to fill out this form?
Yes, if all or a portion of your business operations have been granted operating rights under the jurisdiction of the PA Public Utility Commission, you must complete this form. Most operators already have the elements of these four plans in place, but they may not have written them down to formalize them. For examples, please see the answers to questions 8, 9, 11 and 12, below.

4. My company completed and returned this form last year. Does my company have to complete and return another form this year?
Yes, the Public Utility Security Planning and Readiness Self Certification Form should be submitted annually, even if there are no changes in your answers from last year's submission.

5. What do I write in the "Utility/Industry Type" space on the top of the form?
This line should describe the type of business operations that your company performs that are jurisdictional to the PA Public Utility Commission (e.g., electric distribution company, natural gas distribution company, trucking, taxi, limousine, etc.).

6. What do I write in the "Year Ended" space on the top of the form?
For this year's submission, the "Year Ended" is 2019. The Public Utility Security Planning and Readiness Self-Certification Form is used to certify compliance during the previous calendar year.

7. Should my company submit its plans or provide a description of its plans with this form?
No. Security plans should not be submitted with the Public Utility Security Planning and Readiness Self Certification Form.

8. What is a Physical Security Plan?
A Physical Security Plan is designed to safeguard personnel, property, and information. A Physical Security Plan should be a document that characterizes the company's response to security concerns at mission critical facilities or on equipment. The Physical Security Plan may include the specific features of mission critical equipment or a facility protection program (e.g., fences, surveillance cameras, etc.), and company procedures to follow based upon changing threat conditions or situations.

For a small motor carrier company, a Physical Security Plan could be a plan that ensures the security of the business office and vehicles, such as locking the vehicles and keeping them in a locked garage, or behind locked gates. Also to be considered are any alarm systems installed on vehicles or in the garage or office.

9. What is a Cyber Security Plan?
A Cyber Security Plan addresses the measures designed to protect computers, software and communications networks that support, operate or otherwise interact with the company's operations. A Cyber Security Plan involves maintaining and testing an information technology disaster recovery plan, which includes: (1) critical functions requiring automated processing, (2) appropriate backup for application software and data, (3) alternative methods for meeting critical functional responsibilities in the absence of information technology capabilities, and

(4) a recognition of the critical time period, for each information system, before the company could no longer operate.

For a small company with only a few computers, a Cyber Security Plan may include an updated virus protection program and alternative media or location storage of critical data. Routinely backing up key data might also be included. Many businesses that use computers in their regular operations are likely following these procedures.

10. How should my company answer the cyber security portion of the form if the company does not have any computers or does not utilize computers to perform critical business operations or store critical data?
If you believe your company falls into this category, please enter an "N/A" response to question numbers 4, 5 and 6 related to cyber security planning and provide an explanation as to why the cyber security planning questions are not applicable.

11. What is an Emergency Response Plan?
An Emergency Response Plan describes the actions a company will take if a problem exists at a facility, whether due to a natural causes or sabotage. Actions typically include identifying and assessing the problem, mitigating the problem if possible, and notifying the emergency management system to protect human life and property.

For a small motor carrier company, an Emergency Response Plan could include keeping a list of emergency numbers stored in drivers' cell phones with a hard-copy backup in the glove compartment. Also, any fire extinguishers or first aid kits stored on the trucks as well as an evacuation plan for a garage or office in case of fire or other event requiring evacuation could be part of an Emergency Response Plan.

12. What is a Business Continuity Plan?
A Business Continuity Plan should ensure the continuity or uninterrupted provision of operations and services. As part of its business continuity planning process, a company may review the continuity or recovery of any facilities or operations that are critical to the company's survival. Business continuity planning is an on-going, comprehensive process with several different but complementary elements. It includes business succession, business recovery, business resumption, and contingency planning.

For a small motor carrier company, a Business Continuity Plan would include a plan ensuring the continuing operation of the business that overcomes the potential loss of the business office, personnel and/or vehicles due to pandemic, accident, fire, terrorism, etc. For most, this is done through insurance on the vehicles or office/garage and with the ability to dispatch from alternate sites, other than the businesses' main location.

13. What does it mean to test my Physical Security, Cyber Security, Emergency Response and Business Continuity Plans annually?
The PA Public Utility Commission requires all our jurisdictional utilities to test their security plans annually; however, we understand that it may not be feasible to test an entire plan each year. In such cases, we request that companies maintain a schedule of testing for each portion of their plans, such that the entire plan is fully tested over some definitive period of time.

14. Does the form need to be notarized?
No. The Public Utility Security Planning and Readiness Self Certification Form does not need to be notarized.

15. The bottom of the form requests a name, signature, phone number and e-mail of Officer. Who in my company should fill out this portion of the form?
The individual responsible for ensuring the secure operations of the business should be the person that signs the bottom of the form.

Pennsylvania Public Utility Code Chapter 101 – Public Utility Preparedness Through Self-Certification

Subpart E. PUBLIC UTILITY SECURITY PLANNING AND READINESS

CHAPTER 101. PUBLIC UTILITY PREPAREDNESS THROUGH SELF CERTIFICATION

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 sup-port, 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.]

Information on the Pennsylvania State Police Criminal Intelligence Center

In 2011, the Pennsylvania State Police (PSP), Pennsylvania Criminal Intelligence Center, began a new initiative designed to increase the information exchange between criminal justice agencies and critical infrastructure owners and operators who share the fundamental responsibility of safeguarding our communities. The PSP created the Critical Infrastructure and Key Resource (CI/KR) unit to monitor and track threats to the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. Their primary mission is to educate and share information by preparing and disseminating timely and relevant updates on known risks and potential threats to businesses and entities.

Since 2011, the PSP CI/KR unit has established over 4,000 partnerships and continues to seek out new relationships to maximize the benefit of this initiative. Information sharing will continue to enhance statewide situational awareness and potentially aid in the prevention of future terrorist or criminal acts through early identification and intervention. By creating an open dialog with the public/private sector, the unit has assisted in the facilitation of proactive suspicious activity reporting, discussion of emerging threats, and the sharing of concerns.

Any agency, business, or entity interested in receiving CI/KR products and participating in information sharing, should e-mail sp-protectpa@pa.gov for a registration form. If you would like a CI/KR presentation at your next business function or meeting, please send a request via email to sp-protectpa@pa.gov or call (855) 772-7768. By actively communicating and working together, we can continue to improve our preparation for and response to future incidents. The CI/KR unit looks forward to working with you to protect Pennsylvania.