

Original: 2404

(1)

Hawke
 McKeon
 Sniscak &
 Kennard LLP
ATTORNEYS AT LAW

William T. Hawke	Craig R. Burgraff
Kevin J. McKeon	Steven D. Snyder
Thomas J. Sniscak	Janet L. Miller
Norman James Kennard	Steven K. Haas
Lillian Smith Harris	William E. Lehman
Scott T. Wyland	Rikardo J. Hull
Todd S. Stewart	Katherine E. Lovette

2004 JUL 21 PM 2:53

100 North Tenth Street, Harrisburg, PA 17101 Phone: 717.236.1300 Fax: 717.236.4841 www.hmsk-law.com

July 19, 2004

James J. McNulty, Secretary
 Pennsylvania Public Utility Commission
 Commonwealth Keystone Building
 400 North Street – Filing Room (2 North)
 P.O. Box 3265
 Harrisburg, PA 17105-3265

RECEIVED
 2004 JUL 19 PM 4:15
 SECRETARY'S BUREAU

Re: Rulemaking Re Public Utility Security Planning and Readiness; Docket No. L-00040166; **COMMENTS OF THE PENNSYLVANIA TELEPHONE ASSOCIATION**

Dear Secretary McNulty:

The Pennsylvania Telephone Association ("PTA"), on behalf of its members, has reviewed and offers the following comments on the Proposed Rulemaking Order in the above-referenced proceeding.

It is the PTA's understanding that the Proposed Rulemaking Order, once finalized, will not require Pennsylvania utilities to file copies of their physical and cyber security, emergency response, and business continuity plans with, or provide sensitive or proprietary information to, the Commission. It is also the PTA's understanding that the Proposed Rulemaking Order only requires utilities to have physical and cyber security, emergency response, and business continuity plans in place, and does not impose any specific plans nor specific timeframe schedules for testing upon the utilities. Further, the Commission is not attempting to infringe upon a utility's management of its own operations.

Based upon this understanding, the PTA does not have any specific objections to the Proposed Rulemaking Order.

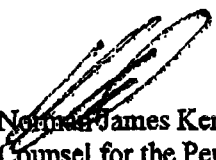
The PTA, however, does seek clarification that the four plans may exist within a single document, and that certification of compliance to that single document attests to compliance with

MAILING ADDRESS: P.O. BOX 1778 HARRISBURG, PA 17105

all four plans. The PTA member companies suggest that the maintenance of all plans within a single document and a single certification to the Commission is efficient and easier to manage.

In closing, the PTA thanks you for this opportunity to file comments in this proceeding.

Sincerely,



**Norman James Kennard
Counsel for the Pennsylvania
Telephone Association**

NJK/rjh

(2)

COPY

Original: 2404

2004 JUL 21 11:01
LEGAL SERVICES



Allegheny Energy

600 Cabin Hill Drive
Greensburg, PA 15601-1689
Phone: (724) 837-3000
FAX: (724) 838-6177

Writer's Direct Dial No. (724) 838-6210

E-mail: jmunsch@alleghenyenergy.com

July 19, 2004

VIA FEDERAL EXPRESS

James J. McNulty, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street
Harrisburg, PA 17120

RECEIVED

JUL 19 2004

PA PUBLIC UTILITY COMMISSION
SECRETARY'S BUREAU

**Re: Public Utility Security Planning and Readiness;
Docket L-00040166**

Dear Mr. McNulty:

Enclosed please find an original and 15 copies of the **Comments of Allegheny Power** in the above-captioned rulemaking. An electronic copy of the Comments has been sent to Kimberly A. Joyce, kjoyce@state.pa.us, at the Commission.

This filing is made by express mail and is deemed filed today under Commission rules.

2004 JUL 21 11:01:53

Very truly yours,

John L. Munsch
John L. Munsch
Attorney

cc: Darren Gill - Fixed Utility Service
Kimberly A. Joyce - Law Bureau
David Epple - Energy Association of Pennsylvania

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

RECEIVED

JUL 19 2004

PA PUBLIC UTILITY COMMISSION
SECRETARY'S BUREAU

Re: Public Utility Security : Docket No. L-00040166
Planning and Readiness :

COMMENTS OF ALLEGHENY POWER

Allegheny Power¹ submits comments in the rulemaking at the above-captioned docket concerning protection of the Commonwealth's infrastructure through implementation by utilities of written physical, cyber security, emergency response and business continuity plans. The proposed regulations were published in the Pennsylvania Bulletin on Saturday, June 19, 2004 (34 Pa. B. 3138). Allegheny Power's comments are specific to items in the proposed self-certification form.

1. The self-certification form asks questions at Item Nos. 3, 7, 10 and 13 about annual testing of the four plans. For example, the question at Item No. 3 states: "Is your cyber security plan tested annually?" Item Nos. 7, 10 and 13 similarly request annual testing of the other three plans. Allegheny Power requests that the term "test" be defined in the regulations. In particular, it is important that the term "test" be defined to recognize that the four plans do not need to be entirely tested within a calendar year, and that testing of a portion of a plan constitutes a test of a plan. Such an understanding of

¹ Allegheny Power is the trade name of West Penn Power Company, a Pennsylvania corporation and public utility providing electric distribution and transmission service to approximately 697,000 customers in Pennsylvania.

the term "test" was conveyed in earlier Commission Orders which recognized that testing should be an ongoing process for the plans, but not necessarily a distinct annual drill where an entire plan is tested from beginning to end. The Commission stated: "We agree with [Energy Association of Pennsylvania] that, in some cases, testing of physical security, cyber security, emergency response and business continuity plans are ongoing and security is achieved through a sum of continuous partial testing rather than one big test undertaken over some specified time table." Order entered December 9, 2003, at Docket No. M-00031717, p. 7.

2. Item No. 7 of the self-certification questionnaire states: "Has your company performed a vulnerability or risk assessment analysis as it relates to physical and/or cyber security?" Allegheny Power submits that the terms "vulnerability or risk assessment," as the terms are used in Item No. 7 of the self-certification questionnaire, should be defined in the regulations. The terms appear to have a particular meaning in the security area, but could be subject to interpretations, and their definition could assist utilities' compliance activities.

3. Finally, Item Nos. 2, 5, 9 and 12 of the self-certification questionnaire ask if the four plans have been "reviewed and updated" in the past year. For example, Item No. 12 in the self-certification asks: "Has your business continuity plan been reviewed and updated in the past year?" A company that has reviewed its business continuity plan, found it to be up to date and not in need of changes, may nevertheless have to answer the question "No." That is, the plan was reviewed but not updated. Because a plan can be reviewed, but purposefully not updated after the review, the question is susceptible to unintentionally misleading answers. The questions should ask if a plan has been "updated or reviewed."

Respectfully submitted,

Date: July 19, 2004

By:



John L. Munsch
800 Cabin Hill Drive
Greensburg, PA 15601
Phone: 724-838-6210

Attorney for
Allegheny Power

Original: 2404

3



COPY

2004 JUL 21 11:30 AM
Robert C. Barber
Senior Attorney
PUC

Room 3D
3033 Chain Bridge Road
Oakton, VA 22185
703 691-6061
FAX 703 691-6093
EMAIL rbarber@att.com

July 16, 2004

BY OVERNIGHT MAIL

James McNulty, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street
Harrisburg, PA 17120

2004 JUL 21 11:25 AM

Re: **Public Utility Security Planning and readiness**
Docket No. L-00040166

Dear Mr. McNulty:

Please find enclosed for filing in the above-captioned matter the original and fifteen (15) copies of the Initial Comments of AT&T Communications of Pennsylvania, LLC.

Please do not hesitate to contact me with any questions regarding this submission.

Very truly yours,

Robert C. Barber
Robert C. Barber

Enclosures

cc: (electronically)
Ms. Kimberly A. Joyce

RECEIVED

JUL 16 2004

PA PUBLIC UTILITY COMMISSION
SECRETARY'S BUREAU



**BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION**

**PUBLIC UTILITY SECURITY
PLANNING AND READINESS**

:
:

Docket No. L- 00040166

**INITIAL COMMENTS OF
AT&T COMMUNICATIONS OF PENNSYLVANIA, LLC.**

While AT&T supports the Commission's proposed rulemaking, it is submitting these comments in an order to clarify the scope of proposed Rule 101.6(d) and its reference to the ability of utilities to utilize "substantially similar cyber security, physical security, emergency response or business continuity plans under the directive of another state or Federal entity". It must be understood that whether or not such plans are "under the directive of another state or Federal entity", utilities providing service nationwide do utilize and maintain such plans on a national level, and that any such plans are national in scope.

Therefore, while these plans may address assets that are located in Pennsylvania, they may not always be specific to Pennsylvania assets, as they may be centralized and/or regionalized in nature. Furthermore, implementation of such plans may be directed by prioritization at a national level through the NCC within the Department of Homeland Security, depending upon the situation, and priority of restoration, in a specific geographical area.

RECEIVED

JUL 16 2004

**PA PUBLIC UTILITY COMMISSION
SECRETARY'S BUREAU**

2004 JUL 21 11 2:53

Respectfully submitted, .

**AT&T COMMUNICATIONS
OF PENNSYLVANIA, LLC.**

By Its Attorneys,



Robert C. Barber
3033 Chain Bridge Road
Oakton, VA 22185
(703) 691-6061

Of Counsel:
Mark Keffer

Dated: July 16, 2004

4

COPY

Original: 2404



Zsuzsanna E. Benedek
Attorney

240 North Third Street, Suite 201
Harrisburg, PA 17101
Voice 717 236 1385
Fax 717 236 1389
sue.e.benedek@mail.sprint.com

2004 JUL 21 PM 3:01

July 20, 2004

VIA HAND DELIVERY

James J. McNulty, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street, 2nd Floor
Harrisburg, PA 17120

RECEIVED
2004 JUL 20 PM 3:42
SECRETARY'S BUREAU

Re: **Public Utility Security Planning and Readiness**
Docket Number: L-00040166

Dear Secretary McNulty:

Per the notice set forth in the June 19, 2004, issue of the *PA Bulletin*, attached please find an original and fifteen (15) copies of Joint Comments of (1) The United Telephone Company of Pennsylvania, operating as an incumbent local exchange company; (2) Sprint Communications Company L.P. (including ASC Telecom), operating as interexchange carriers; and (3) Sprint Communications Company L.P. operating as a competitive local exchange carrier (hereinafter collectively referred to as "Sprint")

If you have any questions, please do not hesitate to contact me or Russell Gutshall at (717) 245-6502.

Sincerely

Sue Benedek

ZEB/jh
enclosures

2004 JUL 21 PM 3:53

**BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION**

**Public Utility Security Planning
And Readiness**

:

Docket No. L-00040166

SECRETARY'S BUREAU

2004 JUN 20 PM 3:42

RECEIVED

**JOINT COMMENTS OF
THE UNITED TELEPHONE COMPANY OF PENNSYLVANIA
AND
SPRINT COMMUNICATIONS COMPANY L.P.**

On March 25, 2004, the Pennsylvania Public Utility Commission ("PUC" or "Commission") entered a Proposed Rulemaking Order in the above-referenced docket. The Commission's Proposed Rulemaking Order was issued following the entry of a Tentative Order, at Docket No. M-00031717, in which the Commission addressed physical and cyber security self certification requirements for public utilities. The Commission's Proposed Rulemaking Order was published in the *Pennsylvania Bulletin* for Comment.¹

These Joint Comments are submitted by the following entities: (1)The United Telephone Company of Pennsylvania, operating as an incumbent local exchange company; (2) Sprint Communications Company L.P. (including ASC Telecom), operating as Interexchange carriers; and (3) Sprint Communications Company L.P. operating as a competitive local exchange carrier. For purposes of these Joint Comments, these entities shall be collectively referred to as "Sprint".

Sprint appreciates the opportunity to provide comment on this important

¹34 Pa.B. 3138.

2004 JUL 21 PM 3:50

issue. Sprint supports the Commission's rulemaking effort to develop physical security, cyber security, emergency response and business continuity planning – along with development of measures “to detect, prevent, respond to and recovery from abnormal operating conditions.”²

In these Joint Comments, Sprint seeks clarification – rather than present objection – as to the intended scope of this Commission's new reporting requirement. The substantive issues for which Sprint seeks clarification are addressed immediately below.

A. Continued business operations cannot be “ensured”.

The proposed definition of a “business continuity plan” in pertinent part states that the written plan will “ensure” the continuity or uninterrupted provision of operations and services. The definition employed for the three (3) other security plans – namely the cyber security plan, the emergency response plan and the physical security plan – do not employ language requiring corporate security planning to “ensure” continuity and uninterrupted operations and services. Sprint is concerned with the reference to “ensure” in the definition of a “business continuity plan” and seeks further clarification of the Commission's intention.

No plan can absolutely “ensure” uninterrupted operations and services 100% of the time, regardless of the nature or gravity of the circumstances. Sprint, as a public utility, is cognizant of its obligations under the Public Utility Code and will endeavor to implement a business plan that reasonably ensures uninterrupted operations and services. Indeed, Section 1501 of the Public Utility

² Proposed Rulemaking Order at 4.

Code does not mandate an absolute assurance of utility service or operations.³

The Pennsylvania Public Utility Code requires “just and reasonable” utility service – not perfect utility service.

The Commission should clarify that the business continuity plan does not require utilities to go beyond the Public Utility Code and “ensure” uninterrupted operations and services. Accordingly, Sprint recommends that the Commission modify the definition of a “business continuity plan” in relevant part as follows: “A written plan that will reasonably ensure the continuity or uninterrupted provision of operations and services....” Alternatively, the definition of a “business continuity plan” should be modified to be consistent with the definitions employed for a cyber security plan, the emergency response plan, and the physical security plan.

B. State security reporting requirements should be flexible enough to allow for the incorporation of nationally-developed, corporate security programs and processes.

Sprint has developed an extensive national, corporate-wide security program aimed at providing safe continuous and reliable service. Sprint has developed programs that consist of multiple components (policies, processes and organizational structure). These programs enable Sprint to respond to an event in such a manner that critical business functions continue without interruption or essential change.

Sprint and the telecommunications industry also continue to meet and continue to foster public/private initiatives with both the Federal Communications

³ 66 Pa. Code §1501.

Commission ("FCC") and the Department of Homeland Security ("DHS"). Before the FCC, the public/private initiative is referred to as the Network Reliability and Interoperability Council ("NRIC"). Before the DHS, the public/private initiatives consist of the National Security Telecommunications Advisory Committee ("NSTAC"), National Coordinating Center ("NCC") for Telecommunications, and the Telecom-Information Sharing and Analysis Center ("ISAC"). Each one of these federal initiatives was designed to address the very issues of concern in this proposed rulemaking.

Sprint interprets its security programs as satisfying the "plans" contemplated in the proposed regulations, albeit the terminology differs. Sprint is concerned that the Commission's proposed regulations may be interpreted or implemented in a manner that would impose the development of "plan" specific to the four identified subject matters – without flexibility or understanding that integrated, multifaceted providers of telecommunications services develop, implement, and monitor security requirements in terms of processes spanning these subjects.

Thus, Sprint's first comment on this issue seeks clarification that security programs which reasonably ensure service and operational continuity are equivalent to a specific "plan" for purposes of these Commission reporting requirements.

Second, Sprint seeks clarification as to whether processes that are part of a corporate-wide, national security program for a reporting entity qualify for the

certification set forth in the proposed regulations. Telecommunications services subject to Commission jurisdiction are provided by diversified carriers.⁴ Effective security measures for diversified operating entities hinge upon the consistent development of a comprehensive and uniform program that encompasses all operating divisions and then the application and monitoring of that comprehensive program by all corporate operations. In this regard, Sprint recognizes that a nationally-developed comprehensive security program for an integrated company should be implemented and monitored at a local level.

Moreover, corporate level programs, once developed, can be updated promptly based on national security input or industry practices. Indeed, the reality is that security planning is continuously updated. As industry practices and technology advance and evolve, corporate level practices can readily incorporate new developments in security protection practices.

National, corporate-wide security programs foster consistent and efficient implementation of security measures. As a result of consistent, corporate-wide planning, "abnormal operating conditions" will be efficiently and readily detected, prevented, and responded to and recovered from.⁵ For telecommunications carriers with more than one Pennsylvania jurisdictional utility, therefore, Sprint seeks clarification that a security program which may be part and parcel of a reporting entity's corporate-wide, national security program can qualify for purposes of the certification set forth in the proposed regulations.

⁴ Proposed Rulemaking Order at 4 ("The intent of this rulemaking is to create a minimum set of requirements that can be consistently implemented with sufficient flexibility to account for differences in the types of utilities under the Commission's jurisdiction.").

⁵ *Id.*

C. Electronic Availability of Security Plans.

In the definitional section of the various security plans as well as in proposed Section 101.3(a), the language qualifies that plans must be "written".⁶ We live in an electronic, data-centric age. Digital storage and retrieval of written documents are standard in most organizations, public or private. Sprint's processes and practices consist of a national, corporate-wide security program that each Sprint site is required to implement. Immediate access to important documents – including any updates to those documents – is promoted by use of electronic means of access to important documents. Electronic documents ensure accuracy. Moreover, given the reality of depleting natural resources such as trees used to make paper, the electronic means of document retention is generally wiser from a policy standpoint.

Accordingly, Sprint suggests that the Commission should clarify that the use of the term "written" includes electronic means of storing and updating security plans required in these regulations.

D. Clarification is needed as to the contemplated "testing schedule".

In the third paragraph of the Executive Summary that accompanied publication of the proposed regulations, the Commission suggests: "In addition, jurisdictional utilities will be required to review and exercise their ability to detect, prevent, present, respond to and recover from abnormal operating conditions on

⁶ See, e.g., proposed 52 Pa. Code §101.1 ("Business continuity plan – A written plan"; "Cyber security plan – A written plan..."; "Emergency Response Plan – A written plan . . ."; "Physical security plan – A written plan"). See also, proposed 52 Pa. Code §101.3(a) ("A jurisdictional utility shall develop and maintain writtenplans.").

an annual basis.⁷ This annual testing requirement is also set forth on the certification form at Appendix A of the proposed regulations.⁸ Meanwhile, proposed Section 101.3(c), requires that utility plans shall maintain “a testing schedule” of the various plans.

To the extent that an annual review or testing requirement is applied, Sprint believes such a requirement would be unnecessary and unwise. Some processes need to be reviewed more than annually, such as cyber infrastructure security practices. An annual review requirement would be unwise relative to these processes. Meanwhile, an annual “review” of other security practices may be unwarranted. The suggestion of an annual review should be rejected.

Finally, Sprint seeks to make clear that proposed Section 101.3(c)'s requirement of a “testing schedule” includes intra-company assessments of security plans undertaken by the reporting entity, or its agent or employees – rather than a third party. Sprint is continually reviewing and modifying its security programs and processes as part of assessing its standard operating procedures. The word “testing” in the proposed regulations, therefore, is too limiting. Accordingly, Sprint recommends that proposed Section 101.3(c) should be modified to include “a testing or assessment schedule of these plans.”

⁷ 34 Pa.B. 3138 (emphasis added).

⁸ See, e.g., Item No. 3 (“Is your physical security plan tested annually?”). See also, App.A Item Nos. 6, 10 and 13.

E. Section 101.6(c)'s reference to a utility's "facility" should be clarified.

The proposed regulations authorize the Commission to "inspect a utility's facility to assess performance of its compliance monitoring..."⁹ Sprint has two concerns with Section 101.6(c).

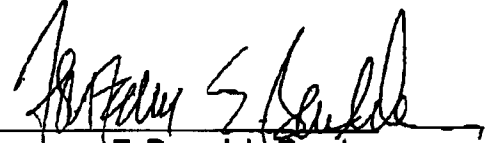
First, Sprint seeks clarification regarding Section 101.6(c)'s reference to "facility". To the extent that a utility's facilities are not utilized, and are not necessary, for the provision of a jurisdictional utility service, Sprint questions the Commission's reach over these facilities. Accordingly, Sprint suggests that Section 101.6(c) should be modified in relevant part as follows: "The Commission may inspect a utility's facility, to the extent utilized for or necessary to the provision of utility service, so as to assess performance of its compliance monitoring under 66 Pa.C.S. §§ 504-506."

Second, while Sprint does not oppose a reasonably conducted Commission inspection, there is no reference made in proposed 101.6(c) regarding the level of confidentiality that will be extended during and following any such Commission inspection. How a company protects its assets and what it does in an emergency, constitutes sensitive information and should not be made available to the public. Public dissemination of information regarding perceived weaknesses could be a windfall for someone with ill intentions, such as a terrorist or even a competitor. Any information or data gathered during a Commission inspection pursuant to Section 101.6(c) must be accorded confidentiality (e.g., Inspector must execute a non-disclosure agreement) and must not be accessible as a public document.

F. Conclusion

Sprint appreciates the opportunity to present these Joint Comments and requests that the Commission consider its request for clarification and its recommendations as to these issues.

Respectfully submitted,



Zsuzsanna E. Benedek, Esquire
Sprint Communications Company, L.P.
240 North Third Street, Suite 201
Harrisburg, PA 17101
Phone: (717) 236-1385
Fax: (717) 236-1389
e-mail: sue.e.benedek@mail.sprint.com

Dated: July 20, 2004

⁹ Proposed Section 101.6(c).