



STATE OF DELAWARE

**PUBLIC SERVICE COMMISSION**  
861 SILVER LAKE BLVD.  
CANNON BUILDING, SUITE 100  
DOVER, DELAWARE 19904

TELEPHONE: (302) 736-7500  
FAX: (302) 739-4849

September 28, 2016

**MEMORANDUM**

TO: The Chair and Members of the Commission  
FROM: Amy Woodward, Public Utility Analyst III  
SUBJECT:

IN THE MATTER OF THE COMMISSIONS' )  
REVIEW OF THE NECESSITY FOR )  
CYBERSECURITY GUIDELINES OR ) PSC DOCKET NO. 16-0659  
REGULATIONS FOR DELAWARE INVESTOR )  
OWNED ELECTRIC, GAS AND WATER )  
(FILED MAY 23, 2016) )

**STAFF FINDINGS AND RECOMMENDATIONS**

**BACKGROUND**

On May 23, 2016, the Staff of the Public Service Commission (“Staff”) filed a petition requesting that the Delaware Public Service Commission (the “Commission” or “PSC”) open a docket to review whether cybersecurity guidelines or regulations are needed to ensure and maintain safe and reliable public utility services for customers in the State of Delaware. The Commission has the exclusive jurisdiction and authority over such matters pursuant to 26 *Del. C.* §§201(a) and 209(a)(2).

There remains a potential for a cybersecurity breach of utility customer information and/or their system control systems. No matter how well the utilities monitor

and secure these systems. As noted in the petition, Staff recommended a discussion of the cybersecurity risks that Delaware's regulated utilities may have to ensure that they are prepared for any such system breach or cyber-attack.

Cybersecurity has become a hot topic in all levels of government in the last few years. Many states, including Delaware, are having open discussions with utilities to determine whether to enact guidelines or regulations. A few surrounding states, Pennsylvania, Maryland, D.C. and New Jersey, have initiated working groups, passed guidelines and regulations to help ensure that their utilities are taking actions to help better manage the risk of cyber-attacks.

The utility industry as a whole is facing an ever-changing cyber threat landscape. Whether these cybersecurity attacks are accidental or malicious it is important that utilities protect both their operational and information technology environments. Staff was ordered by the Commission to hold a public workshop to initiate high-level discussions on the need for cybersecurity guidelines or regulations Delaware's regulated public utilities.

### **STAFF'S REVIEW PROCESS**

Staff held a public workshop (see minutes included as Attachment B) in the Commission Hearing Room in accordance with Commission Order No. 8898 dated May 23, 2016. It was held August 18, 2016, at 10 a.m. with representatives from all of the regulated water, gas and electric utilities along with PJM, the Division of the Public Advocate, and Staff. There were no attendees from the public.

Staff initiated the discussions by stating that the PSC wants to be certain that the utilities are making significant efforts and proper investments to ensure they are prepared for a cybersecurity attack of either their physical critical infrastructure or digitally for their networks and supervisory control and data acquisition ("SCADA") systems. Staff also noted it wanted to avoid any duplication or conflicting regulatory standards that other agencies are requiring from the utilities. Staff indicated that it completely understands the need for confidentiality and information sharing and expressed desire to keep the lines of communication open between Staff and the utilities.

Staff requested that each utility present a brief statement and summary of their cybersecurity guidelines that they have in-house and are currently operating under. Each Class A utility discussed what they currently have in place and their future plans to

be sure they stay current with the ever-changing technologies.<sup>1</sup> They indicated they are creating and hiring new positions to assist them in cybersecurity activities within their organization. They are providing on-going training to employees to ensure they know what to look for and are aware of the potential cyber areas of exposure within the companies. They are working with reputable firms to help develop and assess where they are in terms of cybersecurity. They are currently adjusting their programs as needed and sharing information on emerging threats in industry cybersecurity groups. The utilities appear to be following the National Institute of Standards and Technology (“NIST”) cybersecurity framework. Additionally, the utilities have partnered with both federal and state agencies like the Department of Homeland Security, the Federal Bureau of Investigation and the Federal Energy Regulatory Commission. After an extensive workshop, Staff feels that the utilities are taking cybersecurity risks seriously and are providing the necessary training, while assessing and taking the necessary precautions within their organization to minimize the risk of a cybersecurity breach.

Lastly, Staff also asked for opinions regarding posting a list of cyber related questions and responses from each utility on the PSC’s website to let the public know that cybersecurity is an issue Staff and the utilities takes seriously and that the utilities are striving to ensure they are in fact keeping up with the risk of potential cyber-attacks. The utilities appeared to be receptive to this idea and had no issues with filing such questions on an annual basis and thereafter if the responses required updating as processes change.

## **STAFF CONCLUSIONS & RECOMMENDATIONS**

Staff has confirmed that all utilities in Delaware are aware of the cybersecurity risks and are diligently monitoring facilities and training workforce to ensure that they are prepared for any potential security breach. The utilities are taking the actions that they need to take in order to continue ensuring safe, adequate and reliable utility service to its customers.

During the workshop, Staff presented a series of questions for response by the utilities. Staff received a few edits and took those edits under consideration and has revised the questions to meet the current needs of the utilities and the PSC. To ensure that customers and the general public are aware of how serious the PSC and the utilities take cybersecurity issues, Staff recommends the an individual PSC website

---

<sup>1</sup> Class A utilities are defined in 26 *Del. Admin. C.* §§1002 as a utility or division with annual gross intra-State revenues of \$1 million or more.

page with the list of questions and responses posted and updated as new information is received from the utilities.

Therefore, after thorough review and discussion with the Class A regulated utilities Staff recommends that the Commission does not need to promulgate a regulation or guidelines pertaining to cybersecurity at this time. Staff recommends that an order be put forth from the Commission requiring Staff to conduct an annual review of the cybersecurity questions (see questions included as Attachment A) and requiring all Class A utilities to file an annual report in DelaFile that includes both the questions, as may be revised, and the utilities responses to the cybersecurity questions. Staff has also attached a draft order (see order included as Attachment C) which formalizes Staff's recommendations and requests the Commission's consideration of the order.

## **Attachment A**

### **Annual Cybersecurity Questions - Docket No. 16-0659 - Final**

#### **Planning/Risk Management**

- Is your cybersecurity plan regularly reviewed and audited? Internally or externally?
- Has your plan been reviewed recently? If not how often is it reviewed?
- Do you assess vulnerabilities to your system and assets?
- Do you assess threats to your system and assets?
- Do you prioritize risks and what processes do you use?

#### **Personnel and Policies**

- Are background checks being conducted upon hire?
- Do you provide internal cyber security training for all employees?
- Do you provide enhanced internal cyber security training for those that are actually in the utilities operating network?
- Are there structural and/or organizational policies and procedures in place that allows the utility to be able to address or think through these things (cybersecurity issues)?
- Are there managerial and operational controls in place?
- How quickly is access to those personnel who quit/fired eliminated?
- Do you have certain employees that are assigned as cybersecurity personnel? Or outsourced?
- Do you have specific practices and policies in place about how your private customer data should be handled? Contingency plans for breach of data?
- Are recovery activities communicated to internal stakeholders and executive and management teams?
- Do you screen vendors and third parties that have access to cyber control systems?

#### **Standards and Guidelines for Reporting**

- Do you have a disaster recovery plan? (The plan itself should not be made public.)
- Do you have separate plans for separate business units in the company?
- Are you reporting to the necessary agencies in regards to your plan?
- Are response and recovery plans regularly tested?
- Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed?
- Do you have a list of contacts for cybersecurity information sharing? (i.e. Federal and state emergency management, law enforcement, National Security, or Any others?)
- Should the Commission create guidelines or regulations to ensure utilities are properly managing cyber security issues?

## Attachment B



STATE OF DELAWARE

**PUBLIC SERVICE COMMISSION**  
861 SILVER LAKE BLVD.  
CANNON BUILDING, SUITE 100  
DOVER, DELAWARE 19904

TELEPHONE:  
FAX:

(302) 736-7500  
(302) 739-4849

### MINUTES

Date: August 31, 2016

From: Amy Woodward, Public Utility Analyst

Re: In the Matter of the petition of the Delaware Public Service Commission Staff for a Review of the Necessity for Cybersecurity Guidelines or Regulations for Delaware Public Utilities - PSC Docket No. 16-0659

---

Pursuant to Order No. 8898 signed on June 28, 2016 there was a public workshop held in the Commission Hearing Room on Thursday August 18, 2016 at 10am. There were representatives from all the Class A utilities along with a representative from PJM, DPA, and Staff. (See attached Attendee List). An agenda was presented to the parties and the floor also remained open for any issues the parties wished to discuss related to the docket (See agenda attached). The sole purpose of the workshop was to initiate a high-level discussion on the need for cybersecurity guidelines or regulations for Delaware Public Utilities.

All Class A utilities gave a short high level presentation on their efforts in putting cybersecurity at the forefront of their Company's operations. They discussed new positions in their companies that have been created for cybersecurity and the reporting that they currently do to other agencies and in other states with cybersecurity regulations.

Staff proposed that Class A utilities would complete a cybersecurity questionnaire (see attached list of questions) and it would be posted with answers on the PSC website. Staff also suggested that this be reviewed yearly and updated for the PSC to certify that utilities are in fact taking cybersecurity serious.

There appeared to be a consensus among those in attendance that the Commission does not at this time need to promulgate a regulation or guidelines for Cybersecurity practices. The group also agreed to complete the questionnaire but wanted to review and comment on the questions by August 31, 2016. An order will be put forth to the Commission along with Staff's findings and recommendations for further approval.

## ***Cybersecurity Guidelines or Regulations Docket No. 16-0659***

***Public Workshop August 18, 2016 10AM***

### ***Agenda***

#### **Introductions**

- Utility/Public/Staff introductions

#### **Staff Introduction to Docket 16-0659**

- PSC efforts to ensure that utilities in Delaware make proper investments
- PSC Review reporting requirements to other cyber security agencies
- Cost Recovery of physical critical infrastructure and digitally for networks and SCADA
- Avoid duplication and conflicting regulatory standards
- Confidentiality issues
- Information sharing
- PSC maintain open lines of communication between Staff and utilities

#### **Utility statements and thoughts**

#### **Conclusion**

- Any need of regulations/guidelines
- Answer cybersecurity questionnaire and post publicly on PSC's website with yearly updates
- Public Comments

## **Cybersecurity Docket No. 16-0659**

### **Planning/Risk Management**

- Is your cybersecurity plan regularly reviewed and audited? Internally or externally?
- Has your plan been reviewed recently? If not how often is it reviewed?
- How do you assess vulnerabilities to your system and assets?
- How do you assess threats to your system and assets?
- How do you prioritize risks and what processes do you use?
- How prepared is the utility to operate critical electronic control systems (SCADA) manually?
- How prepared is the utility to operate electronic processing systems (accounting, billing, customer information) manually?

### **Personnel and Policies**

- What types of background checks are being conducted upon hire?
- Do you provide internal cyber security training for all employees?
- Do you provide enhanced internal cyber security training for those that are actually in the utilities operating network?
- Are there structural and/or organizational policies and procedures in place that allows the utility to be able to address or think through these things (cybersecurity issues)?
- Are there managerial and operational controls in place?
- How quickly is access to those personnel who quit/fired eliminated?
- Do you have certain employees that are assigned as cybersecurity personnel? Or outsourced?
- Do you have specific practices and policies in place about how your private customer data should be handled? Contingency plans for breach of data?
- Are recovery activities communicated to internal stakeholders and executive and management teams?
- Do you screen vendors and third parties that have access to cyber control systems?

### **Standards and Guidelines for Reporting**

- Do you have a disaster recovery plan? (The plan itself should not be made public.)
- Do you have separate plans for separate business units in the company?
- Who do you report to and how often in regards to your plan? (i.e. Homeland Security, NAWC, FERC)
- Are response and recovery plans regularly tested?
- Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed?
- Do you have a list of contacts for cybersecurity information sharing? (i.e. Federal and state emergency management, law enforcement, National Security, or Any others?)
- Should the Commission create guidelines or regulations to ensure utilities are properly managing cyber security issues?

August 18, 2016 - PSC Docket No. 16-0659 Cyber Security Public Comment Session

Name	Company	E-mail Address
Dave Valcarenghi	Artesian	dvalcarenghi@artesianwater.com
Scott Stephan	Artesian DPL	SStephan@artesianwater.com
Karl Randall	Artesian	Piscette@artesianwater.com
Kirsten Higgins	Tidewater Utilities, Inc.	khiggins@tidewater.com
Georgia Simpson	SUEZ Delaware	Gsimpson@middlesexwater.com
Larry Finnerum	SUEZ Delaware	Larry.Finnerum@Suez.com
Paul Ackerman	Exelon Corp	Paul.Ackerman@exeloncorp.com
Bob Harvett	PSE	rbharvett@state.de.us
Lori Murphy Lee	PJM Interconnect	lemurphy.lee@pjm.com
Stu Wilson	Culpeper Corp	Stu.Wilson@culpeper.com
Greg Robinson	Chesapeake	grobison@chpk.com
Bill Gibney	"	
Vik Gadyal	"	
Andrea Macher	DPA	andrea.macher@state.de.us
Amy Woodward	PSC	
Connie McDowell	PSC	
Bob Willard	PSC - Attorney DOJ	
Robert Harvett	PSC	

## Attachment C

BEFORE THE PUBLIC SERVICE COMMISSION

OF THE STATE OF DELAWARE

IN THE MATTER OF THE COMMISSIONS'	)	
REVIEW OF THE NECESSITY FOR	)	
CYBERSECURITY GUIDELINES OR	)	PSC DOCKET NO. 16-0659
REGULATIONS FOR DELAWARE INVESTOR	)	
OWNED ELECTRIC, GAS AND WATER	)	
(FILED MAY 23, 2016)	)	

ORDER NO. XXXX

**AND NOW**, this 18<sup>th</sup> day of October, 2016, the Delaware Public Service Commission ("Commission") determines and orders the following:

**WHEREAS**, on May 23, 2016, the Commission Staff ("Staff") filed a petition that requested this Commission to authorize it to review whether cybersecurity guidelines or regulations are needed to ensure and maintain safe and reliable public utility services for consumers in the State of Delaware; and

**WHEREAS**, the Commission has exclusive jurisdiction and authority over such matters pursuant to 26 *Del. C.* §§ 201(a) and 209(a)(2); and

**WHEREAS**, there remains a potential for a cybersecurity breach of utility customer information in this day of technologies; and

**WHEREAS**, as noted in the petition, Staff recommended a discussion of the cybersecurity risks that Delaware utilities may have to ensure that they are prepared for any such system breach or cyber-attack; and

**WHEREAS**, a few states surrounding Delaware have initiated working groups or adopted guidelines to help ensure that their utilities are taking actions to help manage a risk of cyberattacks; and

**WHEREAS**, Staff was ordered by the Commission to hold a public workshop to initiate high level discussions on the need for cybersecurity guidelines or regulations for Delaware public utilities (see Order No. 8898); and

**WHEREAS**, Staff held a public workshop on August 18, 2016, with representatives from all of the regulated water, gas and electric utilities, along with PJM and DPA; and

**WHEREAS**, Staff requested that each utility present a statement and summary of their cybersecurity guidelines that they have in-house and under which they are currently operating; and

**WHEREAS**, each Class A utility discussed what they currently have in place and their future plans to be sure they stay current with ever changing technologies; and

**WHEREAS**, the utilities indicated that they have created and are creating new positions to assist them in cybersecurity operations; and

**WHEREAS**, the utilities are providing training to employees to ensure that such employees are aware of potential areas of exposure to cyber risk within their companies; and

**WHEREAS**, the utilities are working with reputable firms to help develop ways of dealing with cyber risks; and

**WHEREAS**, the utilities are adjusting their programs as needed and sharing information on emerging threats in industry cybersecurity groups; and

**WHEREAS**, the utilities appear to be following the National Institute of Standards and Technology ("NIST") cybersecurity framework

and are partnering with federal agencies such as the Department of Homeland Security, the FBI, and the FERC; and

**WHEREAS**, after an extensive workshop Staff feels the utilities are taking cybersecurity risks seriously and are providing the necessary training, while assessing and taking the necessary precautions within their organizations to minimize the risk of a cybersecurity breach; and

**WHEREAS**, Staff discussed posting a list of cyber security related questions and responses from each utility on the PSC website so the public will know that cybersecurity is taken as a serious issue by Staff and the utilities and the utilities have agreed to file responses to such questions on an annual basis; and

**WHEREAS**, Staff has concluded that all utilities in Delaware are aware of cybersecurity risks and are diligently monitoring facilities and training workforces to ensure that they are prepared for any potential security breach and are taking all necessary actions to continue ensuring safe, adequate and reliable utility service to their customers; and

**WHEREAS**, after discussions with the utilities and after making certain revisions, Staff has created a series of questions for utilities to respond to annually on cybersecurity issues; and

**WHEREAS**, Staff recommends that an individual PSC website page be maintained with the questions and responses posted and that the website be updated as new information is received from the utilities; and

**WHEREAS**, Staff therefore recommends that the Commission not order the promulgation of regulations or guidelines on cybersecurity at this time; and

**WHEREAS**, Staff recommends that an order be issued by the Commission requiring Staff to conduct an annual review of cybersecurity questions (see Exhibit A) and requiring all Class A utilities to file an annual report in DelaFile that includes both the cybersecurity questions, as may be revised, and the utilities' responses to the questions.

**NOW, THEREFORE, IT IS ORDERED BY THE  
AFFIRMATIVE VOTE OF NOT FEWER THAN THREE COMMISSIONERS:**

1. The Commission orders that no new guidelines or regulations on cybersecurity be promulgated.

2. Staff shall conduct an annual review of cybersecurity questions contained on Exhibit A.

3. All Class A utilities shall respond to these questions on annually.

4. Staff shall review and when appropriate make changes to the questions.

5. An individual website shall be maintained showing the questions and responses which website shall be updated as new information is received.

**BY ORDER OF THE COMMISSION:**

---

Chair

---

Commissioner

---

Commissioner

---

Commissioner

---

Commissioner

ATTEST:

---

Secretary

Exhibit A

Annual Cybersecurity Questions

PSC Docket No. 16-0659

Planning/Risk Management

- Is your cybersecurity plan regularly reviewed and audited? Internally or externally?
- Has your plan been reviewed recently? If not how often is it reviewed?
- Do you assess vulnerabilities to your system and assets?
- Do you assess threats to your system and assets?
- Do you prioritize risks and what processes do you use?

Personnel and Policies

- Are background checks being conducted upon hire?
- Do you provide internal cyber security training for all employees?
- Do you provide enhanced internal cyber security training for those that are actually in the utilities operating network?
- Are there structural and/or organizational policies and procedures in place that allows the utility to able to address or think through these things (cybersecurity issues)?
- Are there managerial and operational controls in place?
- How quickly is access to those personnel who quit/fired eliminated?
- Do you have certain employees that are assigned as cybersecurity personnel? Or outsourced?
- Do you have specific practices and policies in place about how your private customer data should be handled? Contingency plans for breach of data?
- Are recovery activities communicated to internal stakeholders and executive and management teams?
- Do you screen vendors and third parties that have access to cyber control systems?

Standards and Guidelines for Reporting

- Do you have a disaster recovery plan? (The plan itself should not be made public.)
- Do you have separate plans for separate business units in the company?
- Are you reporting to the necessary agencies in regards to your plan?
- Are response and recovery plans regularly tested?

- Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed?
- Do you have a list of contacts for cybersecurity information sharing? (i.e. Federal and state emergency management, law enforcement, National Security, or Any others?)
- Should the Commission create guidelines or regulations to ensure utilities are properly managing cyber security issues?