

**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. 8955

AND NOW, this 18th 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 learning the extensive measures already being undertaken by the utility companies to address cybersecurity risks, Staff has concluded that 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, Staff has created a list of questions pertaining to cybersecurity issues for the utility companies to respond to annually; and

WHEREAS, Staff recommends that an individual PSC website page be maintained pertaining to cybersecurity which would include the

list of PSC generated questions along the responses provided by the utility companies on an annual basis, with such information being Updated as new information is received from the utilities; and

WHEREAS, Staff therefore recommends to the Commission that based upon its review and analysis of the measures currently being undertaken by Class A utility companies pertaining to cybersecurity, along with those requirements already in place through Federal agencies including but not limited to FERC, NERC and Homeland Security, it is not necessary for the Commission to adopt regulations or guidelines on cybersecurity at this time; and

WHEREAS, in lieu of any regulations or guidelines, Staff recommends that an order be issued by the Commission requiring Staff to conduct an annual review of the proposed list of cybersecurity questions (see attached Exhibit A) and requiring all Class A utilities to file in DelaFile the list of cybersecurity questions, as may be revised, and the utilities' responses to those questions.

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

1. The Commission orders that the list of cybersecurity questions set forth on the attached Exhibit A be adopted.

2. The Commission further orders that a separate page be created on the PSC website that would contain the list of adopted cybersecurity questions.

3. The Commission further orders that the Class A utility companies be required to file with the PSC their responses to the list of adopted questions within thirty (30) days from the date that

the separate website page is created and the list of adopted questions is posted thereon.

4. Staff shall conduct an annual review of the adopted cybersecurity questions contained in Exhibit A and shall make changes to such questions as deemed appropriate.

5. All Class A utilities shall be required to file responses to the cybersecurity questions on an annual basis within thirty (30) days following Staff's posting of the annual questions on the PSC website.

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?