delmarva power®
An Exelon Company

Pamela J. Scott
Assistant General Counsel

U S Mail
92DC42
PO Box 6066
Newark, DE 19714-6066

All other deliveries
92DC42
500 N. Wakefield Drive
Newark, DE 19702

302.429.3143 – Telephone
302.429.3801 – Facsimile

pjscott@pepcoholdings.com

September 25, 2017

SENT VIA ELECTRONIC MAIL
AND FILED IN DELAFILE
Amy Woodward
Public Utility Analyst III
Delaware Public Service Commission
Cannon Building, Suite 100
861 Silver Lake Boulevard
Dover, DE 19904

Re: PSC Docket Nos. 16-0659 – Delmarva Power & Light Company
Responses to Cybersecurity Questions - 2017

Dear Ms. Woodward:

Please accept this letter and the attachments as compliance with Delaware Public Service Commission Order No. 8955 in the above referenced docket, and as Delmarva Power & Light Company's (Delmarva) response to your email dated August 17, 2017. Delmarva has reviewed the list of questions pertaining to cybersecurity which are currently posted on the Commission's website and has no suggested changes to those questions. In addition, Delmarva has no changes to the responses that it filed to the listed questions on December 22, 2016 (see attached).

Should you have any questions or require any additional information, please do not hesitate to contact me.

Very truly yours,

Pamela J. Scott

Attachments
cc: Spencer Wilcox (w/attachments)
Jill Vito (w/attachments)
Thomas F. Minton, III (w/attachments)
Laura Ritter (w/attachments)
Paul Ackerman, Esquire (w/attachments)
Pierce Bassett (w/attachments)
Heather Hall (w/attachments)

Pamela J. Scott
Assistant General Counsel

U.S. Mail
92DC42
PO Box 6066
Newark, DE 19714-6066

All other deliveries:
92DC42
500 N. Wakefield Drive
Newark, DE 19702

302.429.3143 – Telephone
302.429.3801 – Facsimile

pjscott@pepcoholdings.com

December 22, 2016

VIA ELECTRONIC MAIL
Amy Woodward
Public Utility Analyst III
Delaware Public Service Commission
Cannon Building, Suite 100
861 Silver Lake Boulevard
Dover, DE 19904

Re: PSC Docket Nos. 16-0659 – Delmarva Power & Light Company
Responses to Cybersecurity Questions for 2016

Dear Amy:

In compliance with Delaware Public Service Commission Order No. 8955 in the above referenced docket, enclosed please find the responses of Delmarva Power & Light Company to the list of questions attached as Exhibit "A" to the referenced Order. Per the requirements of the Order, these responses are being submitted to you within thirty (30) days of notice of the posting of the questions on the Commission's website.

Thank you for your assistance. Should you have any questions or require any additional information, please do not hesitate to contact me.

Very truly yours,

Pamela J. Scott

Enclosures
cc: Spencer Wilcox (w/enclosures)
Thomas F. Minton, III (w/enclosures)

Paul Ackerman, Esquire (w/enclosures)
Heather Hall (w/enclosures)

BEFORE THE PUBLIC SERVICE COMMISSION

OF THE STATE OF DELAWARE

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

RESPONSES OF DELMARVA POWER & LIGHT COMPANY

TO QUESTIONS PRESENTED BY DELAWARE PUBLIC SERVICE COMMISSION STAFF

Comes now, Delmarva Power & Light Company ("Delmarva") and its parent company, Exelon (Delmarva and Exelon are collectively referred to herein as "Exelon") by and through its authorized counsel, and offers the following responses to the list of questions posed by Delaware Public Service Commission Staff ("Staff") in this docket, as approved in Order No. 8955, dated October 18, 2016. Exelon views cybersecurity as an enterprise-wide endeavor; therefore, the responses being provided herein are provided relevant to the security of Delmarva, an Exelon utility.

Planning/Risk Management

1. **Question: Is your cybersecurity plan regularly reviewed and audited? Internally or externally?**

   Response: Yes. Exelon's cybersecurity plans and other governance are regularly reviewed and subject to audits by both internal and external parties.

2. **Question: Has your plan been reviewed recently? If not, how often is it reviewed?**

   Response: Yes. Exelon's crisis management plans are reviewed and exercised at least annually, to include an annual exercise at the Executive Committee level. Business continuity exercises are executed on a set frequency for each business continuity plan. Cybersecurity tabletops and scenarios are exercised as a regular component of our Cybersecurity Operations Center. Exelon also conducts reviews and exercises to ensure

compliance with North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requirements.

3. **Question: Do you assess vulnerabilities to your system and assets?**

   Response: Yes. Exelon uses a risk based model to assess the threats to its enterprise, to identify any vulnerability and to determine the impact that an adverse event could have on our customers and our business.

4. **Question: Do you assess threats to your system and assets?**

   Response: Yes. Exelon Corporate Information Security Services' (CISS) end-to-end Threat Intelligence process actively monitors threat information across the country and around the world.

5. **Question: Do you prioritize risks and what processes do you use?**

   Response: Yes, we use a risk based approach. Findings are rated, and the impacts assessed.

Personnel and Policies

6. **Question: Are background checks being conducted upon hire?**

   Response: Yes. Exelon has a formalized background check standard for all employees, as well as for all contractors, consultants, temporary workers, and other personnel, including those affiliated with third parties performing work on behalf of Exelon.

7. **Question: Do you provide internal cyber security training for all employees?**

   Response: Yes. Our security awareness programs include computer-based training, a web portal, phishing susceptibility testing, high visibility posters, articles and regular threat based communications to our employee base. All employees must complete the annual corporate ethics training, which includes a module on Acceptable Use of information assets, and information protection. Exelon training covers cybersecurity training relevant to remote

access, using personal devices in company facilities, and precautions to take during international travel.

8. **Question: Do you provide enhanced internal cyber security training for those that are actually in the utilities operating network?**

   Response: Yes. While all employees receive internal cybersecurity training, those employees with access and responsibilities related to the Bulk Electric System who are governed by NERC receive enhanced cybersecurity training, certifications and continuing education requirements and opportunities.

9. **Question: 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)?**

   Response: Yes. Exelon has policies and procedures in place documenting how Exelon utilities address cybersecurity matters. These policies and procedures establish organizational roles, responsibilities and processes for addressing cybersecurity issues.

10. **Question: Are there managerial and operational controls in place?**

    Response: Yes. Our security governance is modeled after industry best practices, particularly those contained in the National Institute of Standards and Technology's (NIST) Cyber Security Framework (CSF), key components of which call for a range of appropriate security controls.

11. **Question: How quickly is access to those personnel who quit/fired eliminated?**

    Response: Exelon adheres to the NERC standards for removing access of employees who are terminated and for employees who resign or retire.

12. **Question: Do you have certain employees that are assigned as Cybersecurity personnel? Or outsourced?**

    Response: Yes, Exelon maintains a full cybersecurity team which reports to the Chief Security Officer.

13. **Question: Do you have specific practices and policies in place about how your private customer data should be handled? Contingency plans for breach of data?**

    Response: Yes and Yes.

14. **Question: Are recovery activities communicated to internal stakeholders and executive management teams?**

    Response: Yes

15. **Question: Do you screen vendors and third parties that have access to cyber control systems?**

    Response: Yes. Exelon's vendor security program has been recognized by NIST as an industry best practice.

Standards and Guidelines for Reporting

16. **Question: Do you have a disaster recovery plan? (The plan itself should not be made public).**

    Response: Yes. Exelon has IT Disaster Recovery Programs which prioritize the recovery of applications to ensure that critical business processes such as delivering energy safely and maintaining Exelon's business presence are restored in a timely manner.

17. **Question: Do you have separate plans for separate business units in the company?**

    Response: Yes. All Exelon facilities and businesses have disaster recovery and business continuity plans.

18. **Question: Are you reporting to the necessary agencies in regards to your plan?**

    Response: Yes.

19. **Question: Are response and recovery plans regularly tested?**

Response: Yes. Our crisis management function is exercised at least annually, to include an annual exercise at the Executive Committee level. Business continuity exercises are executed on a set frequency for each business continuity plan.

20. **Question: Are legal and regulatory requirements regarding Cybersecurity, including privacy and civil liberties obligations, understood and managed?**

    Response: Yes. The Exelon business units have processes in place to meet response and reporting obligations at the federal and state level in the event of a cybersecurity incident. Among other things, these processes are intended to protect customer privacy.

21. **Question: 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?)**

    Response: Yes. As discussed above, Exelon communicates with a variety of federal and state emergency management, law enforcement and national security and intelligence agencies, as appropriate, on cybersecurity matters.

22. **Question: Should the Commission create guidelines or regulations to ensure utilities are properly managing cyber security issues?**

    Response: Exelon concurs with the Delaware Public Service Commission's decision in this docket, per Order No. 8955, adopted on October 18, 2016, in which the Commission supported the findings of Commission Staff that all Delaware utilities are aware of cybersecurity risks, 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 to provide safe, adequate and reliable utility service to their customers. As a result, the Commission determined that it was not necessary to implement guidelines or regulations in this area. For the reasons set forth in this docket, Exelon does not believe that state regulations pertaining to cybersecurity are necessary.

Respectfully submitted,

Pamela J. Scott
Pepco Holdings
PO box 6066
Newark, De 19714-6066
302-429-3143
pjscott@pepcoholdings.com
Counsel for Delmarva Power & Light Company

Dated: December 22, 2016

BEFORE THE PUBLIC SERVICE COMMISSION

OF THE STATE OF DELAWARE

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

CERTIFICATE OF SERVICE

I, Pamela J. Scott, hereby certify that on December 22, 2016, I caused a copy of the attached RESPONSES OF DELMARVA POWER & LIGHT COMPANY TO QUESTIONS PRESENTED BY DELAWARE PUBLIC SERVICE COMMISSION STAFF to be served upon Amy Woodward of Delaware Public Service Commission Staff.

Pamela J. Scott
Pepco Holdings
PO Box 6066
Newark, De 19714-6066
302-429-3143
pjscott@pepcoholdings.com