Brian T.N. Jordan
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

302.429.3786 – Telephone
302.429.3801 – Facsimile

Brian.Jordan@ExelonCorp.com

October 28, 2021

VIA ELECTRONIC MAIL and DELAFILE
Matthew R. Hartigan
Executive Director
Delaware Public Service Commission
Cannon Building, Suite 100
861 Silver Lake Boulevard
Dover, DE 19904

RE: PSC Docket No. 16-0659 – Delmarva Power & Light Company
Responses to Cybersecurity Questions - 2021

Dear Mr. Hartigan:

On behalf of Delmarva Power & Light Company ("Delmarva"), please accept this letter and the attachments as compliance with Delaware Public Service Commission Order No. 8955 in the above-referenced docket. Delmarva has reviewed the list of questions pertaining to cybersecurity which are currently posted on the Commission's website and has provided updated responses to those questions. Lastly, we have answers in our response to the three new questions that were added by the April 12, 2021 memo. We agree that the list of questions is correct and that no additional revisions to the list of cybersecurity questions are necessary at this time.

Please contact me at brian.jordan@exeloncorp.com or Diane Goff at diane.goff@pepcoholdings.com with any questions related to this matter.

Respectfully submitted,

/s/ Brian T.N. Jordan

Brian T.N. Jordan

Attachment
cc: Andrew Slater, Public Advocate (via email)
Regina A. Iorii, Esq. (via email)
Andrea Maucher (via email)
Thomas Walsh, Esq. (via email)
Malika Davis (via email)

BEFORE THE PUBLIC SERVICE COMMISSION OF THE STATE OF DELAWARE

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

DELMARVA POWER & LIGHT COMPANY'S RESPONSES TO THE PUBLIC SERVICE COMMISSION'S CYBERSECURITY QUESTIONS

Delmarva Power & Light Company ("Delmarva") and its parent company, Exelon Corporation (Delmarva and Exelon Corporation are collectively referred to herein as "Exelon") provides the following responses to 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, and, therefore, the responses 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 security policies and security controls programs, aligned with the National Institute of Standards and Technology's ("NIST") Cyber Security Framework ("CSF"), are reviewed, and certified on an annual basis. These documents are reviewed during the same week period each year as a way to ensure consistency across our documentation. incident response,

business continuity, and information technology ("IT") disaster recovery plans are reviewed annually and updated as appropriate.

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, supported by a team of cyber and physical intelligence analysts, actively monitors, and collects information from government, industry, and open sources; assesses for threats and vulnerabilities relevant to company operations, assets, and personnel; and distributes intelligence to key stakeholders for appropriate action.

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

Response: Risks, both internal and external, are assessed on a continuous basis. If an immediate risk is identified, such as a phishing attack, immediate measures are taken to protect the company. In addition, once a year, a large-scale risk workshop is conducted to identify risk trends. Findings are rated, and the impacts are 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 and instructor-led training, interactive games, a web portal, phishing susceptibility testing, articles, and regular threat-based communications to our employee base. All employees and contractors must complete the annual corporate security awareness, phishing, and ethics training. Exelon training covers physical and cyber threats, acceptable use of corporate assets, protecting information, identifying, and reporting suspicious activity, international travel precautions, etc.

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 and contractors receive internal cybersecurity training on an annual basis, those employees with access and responsibilities related to the Bulk Electric System, which are governed by North American Electric Reliability Corporation ("NERC"), receive enhanced cybersecurity training, certifications and continuing education requirements and opportunities. Additional security training on Operational technology ("OT") security is offered to operational personnel.

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 NIST CSF, key components of which call for a range of appropriate security controls. The maturity of the programs and controls are assessed on an annual basis using the Department of Energy's Cybersecurity Capability Maturity Model ("C2M2").

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. As an enterprise standard, core network, remote and physical access are removed within 24 hours after offboarding.

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. Additionally, Exelon uses third party services to bolster our monitoring and identification of security threats across the industry and uses this information to inform tactical operations.

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. All critical business functions have a business continuity/recovery plan which is updated, approved by a senior leader, and exercised on a regular basis. Leaders review the plans with their teams every year. IT system disaster recovery plans are also updated annually and tested periodically in accordance with the criticality of the system. Executive leadership participates in annual reviews and exercises of crisis management procedures.

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. In addition, Exelon also successfully implemented the NERC CIP-013 standard which provides mandatory controls on the vendor security program for bulk electric system vendors.

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 maintains business continuity plans for essential functions, IT disaster recovery plans for the prioritized recovery of applications and infrastructure, crisis management plans for coordinated response to emerging events and potential business disruptions and a cybersecurity incident response plan.

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

Response: Yes. All essential business functions have a business continuity plan. Our business continuity team facilitates standardization and sharing of best practices across similar business functions. IT system recovery details are integrated with the business continuity plans. Each business unit also maintains crisis management/emergency response procedures.

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

Response: Yes. Incident response procedures outline state and federal reporting requirements.

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

Response: Yes. Our executive crisis management team is exercised at least annually. Business function continuity plans and IT system recovery plans are regularly tested on a frequency commensurate with the function/system criticality.

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. Exelon maintains a list of key local, state, and national contacts for information sharing and incident reporting, and regularly collaborates with these agencies and forums to improve intelligence sharing, emergency preparedness and cyber defense.

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 additional 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.

23. Does your utility use multi-factor identification for system sign-on purposes?

Response: Yes. We use multi-factor authentication for any user who needs to access to company network remotely. In addition, for access to our most critical systems, we also require multi-factor authentication. Both controls are documented in the applicable Exelon procedures.

24. Do you keep audit logs for all remote connection protocols?

Response: Yes. Exelon maintains logs for all remote connection protocols for all Exelon assets whether used by employee or contractor.

25. Do you have the capability to identify and suspend access of users exhibiting unusual computer activity?

Response: Yes. Exelon monitors for unusual computer activity and maintains the ability suspend access for users or machines that exhibit unusual behavior. We have internal standards that govern acceptable use of company provided equipment. In addition, all employees and contractors must complete an annual training to review the standards.

Respectfully Submitted,

/s/ ***Brian Jordan***
Brian Jordan (DE Bar ID. No.: 5501)
Assistant General Counsel
Delmarva Power & Light Company
PO Box 6066
Newark, Delaware 19714
(302) 429-3143
(302) 429-3801 (fax)
brian.jordan@exeloncorp.com

Dated: October 28, 2020

BEFORE THE PUBLIC SERVICE COMMISSION OF THE STATE OF DELAWARE

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

CERTIFICATE OF SERVICE

I, BRIAN T.N. JORDAN, hereby certify that on October 28, 2021, I caused a copy of the attached DELMARVA POWER & LIGHT COMPANY'S RESPONSES TO THE PUBLIC SERVICE COMMISSION'S CYBERSECURITY QUESTIONS to be served via electronic mail upon Matthew R. Hartigan, Executive Director of the Delaware Public Service Commission, and via DelaFile in the above-captioned docket.

Respectfully Submitted,

/s/ ***Brian Jordan***
Brian Jordan (DE Bar ID. No.: 5501)
Assistant General Counsel
Delmarva Power & Light Company
PO Box 6066
Newark, Delaware 19714
(302) 429-3143
(302) 429-3801 (fax)
brian.jordan@exeloncorp.com