Brian T.N. Jordan
Assistant General Counsel

302.429.3786 – Telephone
302.429.3801 – Facsimile

Brian.Jordan@exeloncorp.com

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

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

September 29, 2023

Via Delafile

Malika Davis
Deputy 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 - 2023

Dear Deputy Director Davis:

On behalf of Delmarva Power & Light Company, please accept the attached answers to the Delaware Public Service Commission's cybersecurity questions as compliance with Delaware Public Service Commission Order No. 8955 (October 18, 2016) in the above-referenced docket.

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

Enc.
cc: Ruth Ann Price, Public Advocate (via email)
Regina A. Iorii, Esq. (via email)
Andrea Maucher (via email)
Sommer Poppe, Esq

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.

2023 Update

1. **Is your cybersecurity plan regularly reviewed and audited? If yes, is it audited internally or externally?**

Response: Yes. Exelon's Cybersecurity Incident Response Plan ("CSIRP") is regularly reviewed. The plan provides guidance before, during, and after a confirmed or suspected cybersecurity incident. The CSIRP clarifies roles and responsibilities, provides guidance on key activities and details a response strategy that aligns with the National Institution of Standards and Technology ("NIST") Cybersecurity Framework ("CSF"). Exelon regularly reviews the plan and briefs external auditors on any relevant updates.

2. How often is the cybersecurity plan reviewed?

Response: Exelon's CSIRP is continuously updated to address changes in operational and technological response capabilities, new reporting requirements, lessons learned from tabletop exercises, and personnel changes that affect rosters. Exelon conducts an annual tabletop exercise to review and test incident response capabilities.

3. Do you assess vulnerabilities and threats to your system and assets?

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

4. Do you have a documented risks assessment and management program?

Response: Yes. Exelon's cybersecurity risk management program aligns with the NIST CSF and integrates Cyber Asset Identification, Continuous Threat Assessment, Risk assessment, Risk Management, and Risk Monitoring elements. Exelon's security programs have mandatory awareness and role-based training, enterprise-level common controls and policy and procedural documents which guide the establishment and implementation of governance over Exelon's enterprise-wide cyber and physical security programs. Exelon subject matter experts annually review and update all policies and procedures.

5. **Are background checks being conducted upon hire for those with access to critical systems and assets?**

Response: Yes. Exelon performs background investigations for all employees, as well as for all contractors, consultants, temporary workers, and other personnel. Exelon requires vendors to conduct background investigations for those affiliated with third parties performing work on behalf of Exelon with access to restricted/confidential information/systems.

6. **Do you provide internal cyber security training for all employees?**

Response. Yes. Our security awareness programs include computer-based and instructor-led training, a web portal, phishing susceptibility testing and education, 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, and international travel precautions.

7. **Do you provide enhanced internal cyber security training for those that are actually in the utility's information technology (IT) and operations technology (OT) networks?**

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.

8. Are there structural and/or organizational policies and procedures in place that allow the utility to be able to address cybersecurity issues?

Response: Yes. Exelon's has a cybersecurity governance structure, which includes published policies and procedures, and oversees and implements its coordinated security programs for all utilities. These policies and procedures establish organizational roles, responsibilities, and processes for addressing cybersecurity issues.

9. Are there managerial and operational controls in place to ensure compliance with the company's cybersecurity policies and procedures?

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. Within Exelon's security programs, owners/custodians of the security controls are identified, and are required to certify compliance with those controls on a set frequency.

10. How quickly is access terminated for personnel who leave the company?

Response: Exelon adheres to the NERC Critical Infrastructure Protection ("CIP") standard (NERC CIP-004) for removing access for 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 from offboarding.

11. Do you have certain employees who are assigned as cybersecurity personnel? Or is the function outsourced?

Response: Exelon's Chief Information Security Officer manages the cybersecurity teams which includes full time Exelon personnel in Cyber Defensive Operations, Cybersecurity Architecture and Engineering, Business Information Security Office, Cybersecurity Services, and Security Policy.

12. 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: Exelon has robust policies and procedures to safeguard customer data. Exelon's Information Protection Program includes security control requirements to protect the confidentiality, integrity and availability of information, including customer data. Personally Identifiable Information ("PII") and Personal Information ("PI") are defined terms that are part of Exelon's classification schema. Each are subject to certain handling requirements, sharing restrictions, and security controls. IT applications that store or process PII and/or PI are identified. Exelon also performs privacy impact assessments for processing activities that handle PII or PI.

13. Are recovery activities communicated to internal stakeholders and executive management teams?

Response: Yes. Exelon's CSIRP includes communication procedures for coordinating internal stakeholders and notifying executive management teams. 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 annually. 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. Additionally, our Business Continuity team is responsible for the activation of our Corporate

Emergency Response Organization ("ERO"). The Corporate ERO is tasked with performing actions as they relate to the strategic management of events that adversely impact the organization's ability to operate or reputation.

14. Do you screen vendors and third parties that have access to cyber control systems?

Response: Yes. Exelon's third-party security program evaluates security risk assessments ("SRA") from vendors that provide materials and/or services that are regulated, are in receipt of Exelon's most sensitive data, include IT solutions being introduced to the Exelon network, or categorized as Exelon's most critical suppliers. In addition, Exelon also successfully implemented the NERC CIP standard (NERC CIP-013) which provides mandatory controls on the third-party security program for bulk electric system vendors.

15. Do you have a disaster recovery plan?

Response: Yes. We have a robust incident response program to manage and respond to cyber and physical incidents to drive system recovery and business continuity. Exelon maintains business continuity plans for essential functions, IT disaster recovery plans for the prioritized recovery of applications and infrastructure, and crisis management plans for coordinated response to emerging events and potential business disruptions. We have a single, centralized cyber incident response program and plan.

16. 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. In the cyber arena, we have crafted a single, centralized cyber incident response program and plan.

17. Are you reporting to the necessary state and/or federal agencies in regard to your plan?

Response: Yes. Exelon's Security Policy function supports reporting and communications with state, federal, and stakeholder engagement alongside other relevant performance. We have a robust incident response program to manage and respond to cyber incidents. Our centralized cyber incident response plan identifies state and federal incident reporting requirements and roles and responsibilities for reporting.

18. 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. Likewise, Exelon's cyber incident response plan is regularly tested and updated.

19. Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed?

Response: Yes. Exelon's Security Policy and Legal and Compliance functions provide support and oversight for cybersecurity and privacy legal and regulatory obligations.

20. 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's Corporate Security, Security Policy and Government Regulatory and External Affairs teams maintain strong, bi-directional relationships with a variety of industry and governmental entities, including a contact list for key local, state, and federal agencies. Exelon engages in information sharing and regularly collaborates with state and federal agencies and forums to improve intelligence sharing, emergency preparedness and cyber defense.

21. 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.

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

Response: Yes. Exelon applies multi-factor authentication for remote user access the company network and critical systems. Access controls are documented in the applicable Exelon procedures.

23. 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.

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

Response: Yes. Exelon monitors for unusual computer activity and maintains the ability to 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.

25. Is cybersecurity addressed differently for IT and OT systems?

Response: Yes. Exelon's IT and OT systems have different security requirements and require specialized security controls to ensure that each system is protected against cyber threats.

26. Does your company include in its procurement contract language cybersecurity requirements for IT and OT assets?

Response: Exelon utilizes specialized cybersecurity terms and conditions in its procurement contracts; the terms address various cybersecurity risks based on the products and services that a vendor is providing. Exelon utilizes NIST and NERC, among other industry-accepted cybersecurity standards, as the basis for our vendor cybersecurity requirements.

27. Do you have a documented records retention policy?

Response: Yes. Exelon's corporate procedure for Records and Information Management, Retention and Disposal sets forth requirements to ensure compliance with all applicable laws and regulations concerning the creation, handling, protection, retention, maintenance and disposition of records.

28. Have you implemented processes and procedures for identifying and tracking suspicious cyber activity?

Response: Yes. Exelon has processes and procedures for identifying and tracking suspicious cyber activity. Exelon maintains a 24/7 internal security operations center which monitors for suspicious cyber activity. The company also has a threat intelligence team that tracks threat actors and campaigns that are targeting our industry. Exelon engages a wide variety of federal, state, and local intelligence and law enforcement agencies, third-party intelligence services, and internal data and telemetry analysis.

29. Have you worked with, or used resources provided by, a federal agency (e.g., ICS-CERT/CSET, DHS C3 Program, FERC Architectural Reviews) to conduct a cybersecurity assessment?

Response: Exelon applies the Department of Energy's Cybersecurity Capability Maturity Model ("C2M2") to assess the maturity of Exelon's programs and controls. The C2M2 was developed by the DOE and the U.S. energy sector to address emerging technologies and the evolving cyber landscape. The evaluation tool covers both IT and OT. In addition to DOE, Exelon is accountable to several federal agencies for cybersecurity, including the Department of Homeland Security ("DHS"), the Federal Energy Regulatory Commission ("FERC") and must comply with regulations set forth by the NERC CIP standards. Exelon's cybersecurity standards align with the NIST CSF.

Respectfully Submitted,

Steven J. Foley
Vice President & CISO
Cyber & Information Security Services

Dated: September 29, 2023

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 September 29, 2023, 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 Malika Davis, Deputy 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