Zi-Xiang Shen
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

667.313.2775 - Telephone
302.429.3801 – Facsimile
Zi-Xiang.Shen@exeloncorp.com

delmarva power℠
AN EXELON COMPANY

October 20, 2025

FILED VIA DELAFILE
Samantha Hajek
Ombudsman
Delaware Public Service Commission
861 Silver Lake Boulevard
Cannon Building, Suite 100
Dover, DE 19904

RE: PSC Docket No. 16-0659 – Delmarva Power & Light Company
Responses to Cybersecurity Questions - 2025

Dear Ms. Hajek:

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 zi-xiang.shen@exeloncorp.com or Mary Anne Phillips at Mary.Phillips@delmarva.com with any questions related to this matter.

Respectfully submitted,

/s/ Zi-Xiang Shen

Zi-Xiang Shen (#6072)

Enclosure

cc: Jameson Tweedie
Matthew Hartigan

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	))))))	PSC DOCKET NO.: 16-0659

(FILED MAY 23, 2016)

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") provide 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.

2025 Update

Planning/Risk Management

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) v2.0. Exelon reviews the plan and briefs external auditors on any relevant updates. Most recently, Exelon's CSIRP was subject to a Transportation Security Administration (TSA) Targeted

Inspection; TSA had no findings of non-compliance and commended Exelon's Plan as an example for the industry.

2. **How often is the cybersecurity plan reviewed?**

   Response: Exelon's Cybersecurity Incident Response Plan (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. CSIRP underwent a substantive revision in 2024, published in January of 2025, to enhance response velocity and manage the introduction of additional regulatory frameworks. Exelon conducts an annual tabletop exercise and multiple operational exercises 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 business. Exelon's Cyber and Information Security Services ("CISS") maintains distinct Vulnerability Management and Threat Intelligence programs and processes. The Threat Intelligence processes include a team of analysts whose responsibilities include continuous collection, analysis, and dissemination of cyber threat information. The intelligence produced comes through information provided by federal and state governments, industry partners, and open sources. Additionally, Exelon conducts regular vulnerability assessments on our IT and OT systems and assets. A combination of automated scanning, threat intelligence, and manual testing help identify potential weaknesses and emerging risks which are evaluated based on its severity and potential business impact. These assessments are provided to key stakeholders and decision makers for appropriate action and mitigation.

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

   Response: Yes. Exelon's cybersecurity risk management program aligns with the NIST CSF 2.0 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 that are governed by 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, and senior leadership reviews and approves updates.

5. **Is cybersecurity addressed differently for IT and OT systems?**

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

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

   Response: Yes. 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. To the extent that OT assets contain elements that can electronically send, receive or store company electronic information, the vendor providing the same must agree to and comply with similar cybersecurity provisions utilized for IT systems and commensurate with the sensitivity of the information to which they have access. The company's cybersecurity provisions in their vendor agreements are based on the NIST CSF 2.0, NERC requirements, and other industry-accepted

cybersecurity standards. The terms are updated annually to capture changes in the cybersecurity landscape.

7. **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.

Personnel and Policies

8. **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, prior to being hired. Exelon also performs backgrounds investigations for all contractors who will have physical and/or electronic access to identified NERC CIP assets. Exelon further requires vendors to conduct background investigations and provide an attestation for those affiliated with third-parties performing work on behalf of Exelon with physical and/or electronic access.

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

   Response: Yes. Our security awareness program includes computer-based and instructor-led training, a web portal, phishing susceptibility testing and education, and regular threat-based communications to our employee base. All employees and contractors with logical network access 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, third-party security, security controls and international travel precautions.

10. **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 (BES), which are governed by North American Electric Reliability Corporation (NERC), receive enhanced cybersecurity training, certifications and continued education opportunities.

11. **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 has a cybersecurity governance structure, which includes company-wide policies, programs, processes, and procedures which are implemented across the entire enterprise that establishes organizational roles, responsibilities, and processes for addressing cybersecurity issues.

12. **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 the industry's best practices, particularly those contained in the NIST CSF 2.0, 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.

13. **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 separation.

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

Response: Yes. Exelon's Chief Information Security Officer (CISO) manages cybersecurity teams staffed by full-time Exelon personnel in five distinct towers: Cyber Defense Operations, Cybersecurity Technical Services, Business Information Security Office (BISO), Cyber Support Services and Critical Infrastructure Compliance.

15. **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. Exelon has robust policies and procedures to safeguard customer data. Exelon's Information Protection Program includes both physical and information security control requirements to protect confidentiality, integrity and availability of information, including private customer data. Private customer data is classified as either Personally Identifiable Information ("PII") or Personal Information ("PI"), which are defined terms that are part of Exelon's classification schema, with PII considered one of Exelon's most sensitive data classifications. The classifications determine certain handling requirements, sharing restrictions, and security controls based on data classification. IT applications that store or process PII and/or PI are identified and monitored. Exelon also performs privacy impact assessments for processing activities that handle PII and/or PI, both internally and with third-party vendors. In the unlikely event of unauthorized access to confidential data

in the Exelon environment or through a trusted vendor, Exelon activates the appropriate security response team and associated procedures to assess the threat, extent of condition, and mitigate potential impacts to customers, personnel, and/or business operations.

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

    Response: Yes. Exelon's Cyber Security Incident Response Plan (CSIRP) includes communication procedures for coordinating internal stakeholders and notifying executive management teams. All critical business functions have business continuity plans, which are updated, receive approval by a senior leader, and shared with the applicable team annually. These plans are exercised on a scheduled cadence based on their measured impact to the organization's ability to meet safety, customer service, financial, regulatory, and legal or other operational requirements. Leaders review the plans with their teams annually. In addition, 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 its reputation.

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

Response: Yes. Exelon's Third-Party Security organization evaluates security risk assessments ("SRA") of vendors that are in-scope of our program. This includes vendors who provide materials and/or services that are regulated, are in receipt of Exelon's most sensitive data, provide IT solutions being introduced to the Exelon network, or vendors that are categorized as Exelon's most critical suppliers. In addition, Exelon also successfully implemented the NERC CIP standard (NERC CIP-013-2) which requires processes for assessing cyber security risks from bulk electric system (BES) vendors.

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

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

Standards and Guidelines for Reporting

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

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.

20. **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.

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

    Response: Yes. Exelon's Cybersecurity Policy function supports reporting and communications with state, federal, and industry stakeholder engagements. 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 with the appropriate roles and responsibilities for reporting.

22. **Are response and recovery plans regularly tested?**

    Response: Yes. Our executive crisis management team is tested 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 tested and updated annually at a minimum.

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

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

obligations. Exelon employs and retains specific legal resources dedicated to cybersecurity risk, mitigation, and compliance.

24. **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, Cybersecurity 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.

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

    Response: No. Exelon does not believe that guidelines and state regulations pertaining to cybersecurity are necessary.

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

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

27. **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.

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

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

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 alternates between an internal self-assessment and an external cybersecurity assessment every year. Exelon applies the Department of Energy's Cybersecurity Capability Maturity Model ("C2M2") to self-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. Exelon engages a third-party for an external cybersecurity assessment, which is conducted using the NIST Cybersecurity Framework (CSF) 2.0. Exelon conducted a C2M2 assessment in 2025 and will conduct a third-party assessment in 2026.

    In addition to these alternating assessments, 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 2.0.

Respectfully Submitted,

Steven J. Foley

Vice President & Chief Information Security Officer

Exelon Cyber & Information Security Services