RECEIVED 2025 AUG 7 1:17 PM

pepco
AN EXELON COMPANY

Dennis P. Jamouneau
Assistant General Counsel

EP9628
701 Ninth Street NW
Washington, DC 20068-0001

Office 202.428.1122
Fax 202.331.6767
pepco.com
djamouneau@pepcoholdings.com

August 7, 2025

Ms. Brinda Westbrook-Sedgwick
Commission Secretary
Public Service Commission
of the District of Columbia
1325 G Street N.W., Suite 800
Washington, DC 20005

Re: Cyber Security Hearing

Dear Ms. Westbrook-Sedgwick:

Enclosed please find Potomac Electric Power Company's response and presentation provided during the District of Columbia Public Service Commission "2025 DC Cyber Security Briefing" on July 16, 2025.

Please feel free to contact me if you have any questions regarding this matter.

Sincerely,

s/ *Dennis P. Jamouneau*
Dennis P. Jamouneau

Enclosure:

cc: All Parties of Record

POTOMAC ELECTRIC POWER COMPANY
DISTRICT OF COLUMBIA INFORMAL
RESPONSE TO CYBER SECURITY HEARING DR NO. 1

QUESTION NO. 1

Commissioner Beverly- Since Exelon is a multi-jurisdiction company and must comply with different regulations, is there something you need from this commission to make your job simpler?

RESPONSE:

Thank you again for the opportunity to participate in this year's Cybersecurity Conference on July 16. During the event, you asked whether Washington Gas Light Company and Potomac Electric Power Company ("Pepco" or the "Company") had any requests for the Public Service Commission of the District of Columbia. At the time, Pepco deferred its response to allow for internal consultation. Now the Company writes to share its thoughts.

First and foremost, Pepco appreciates the Commission's openness to input from the utilities. This proactive engagement fosters a collaborative and transparent regulatory environment, which Pepco values deeply.

The Company views its engagement with the Commission and Commission staff to be frank, forthcoming, and productive for all involved. Thus, the Company does not have any specific issues or requests. More generally, however, Pepco respectfully requests that if ever the Commission considers additional cybersecurity regulations and/or reporting standards, it avoid duplication and mirror federal or state requirements. thereby allowing utilities to efficiently analyze and fulfill their reporting obligations. This is especially important given that when utilities contact the Commission (and other regulators) during a cyber incident, they are also likely to be engaged in active incident response and remediation.

Additionally, if the Commission is evaluating cybersecurity practices or considering new approaches, we would welcome the opportunity to review and provide feedback on any preliminary findings or proposals. In this regard, the Company appreciates the ongoing dialogue with Commission staff as these communications enable the Company to respond quickly and effectively and support the Commission's oversight responsibilities.

We thank the Commission for the opportunity to provide this feedback.

SPONSOR: The Company

exelon[SM]

July 16, 2025

District Utilities Overview:
Cyber security threat landscapes and increased threat focus

Scott Franklin, Director of Security Architecture
Exelon | Cyber & Information Security Services (CISS)

Exelon Cyber & Information Security Services

Scott Franklin

Director of Security Architecture

Responsible for Governance of cybersecurity by providing an enterprise-wide, risk-based, intelligence driven, defense-in-depth approach to securing enterprise assets and information.

- Exelon identifies Cybersecurity as a top Enterprise Risk and defines it as a cybersecurity incident targeting Exelon or a third-party supplier resulting in a significant adverse impact to Exelon data, systems, or customers.
- Key Risk Indicators (KRIs) are used to identify changes in risk exposure, to create actionable intelligence for management, to support evaluations of control and mitigation effectiveness, and to provide the Exelon Board with a visual representation of the monitoring of key cybersecurity risks.

Strategic Imperatives

- Continued Maturity of Cyber Defense Capabilities
- SASE/Zero Trust Implementation
- Reduce Attack Surface
- Sustain Security Governance and Compliance Capabilities
- Measure Response and Recover Capabilities
- Attract, Develop and Retain Top Talent

exelon

Who is Exelon?

6 T&D-only utilities
Operate within seven regulatory jurisdictions

4 major metro areas served
Chicago, Philadelphia, Baltimore, and Washington D.C.

20,000
Employees across our operating companies

10.7 million(1)
Electric and gas customers served across our service territories

25,600
Square miles of combined service territory across our jurisdictions

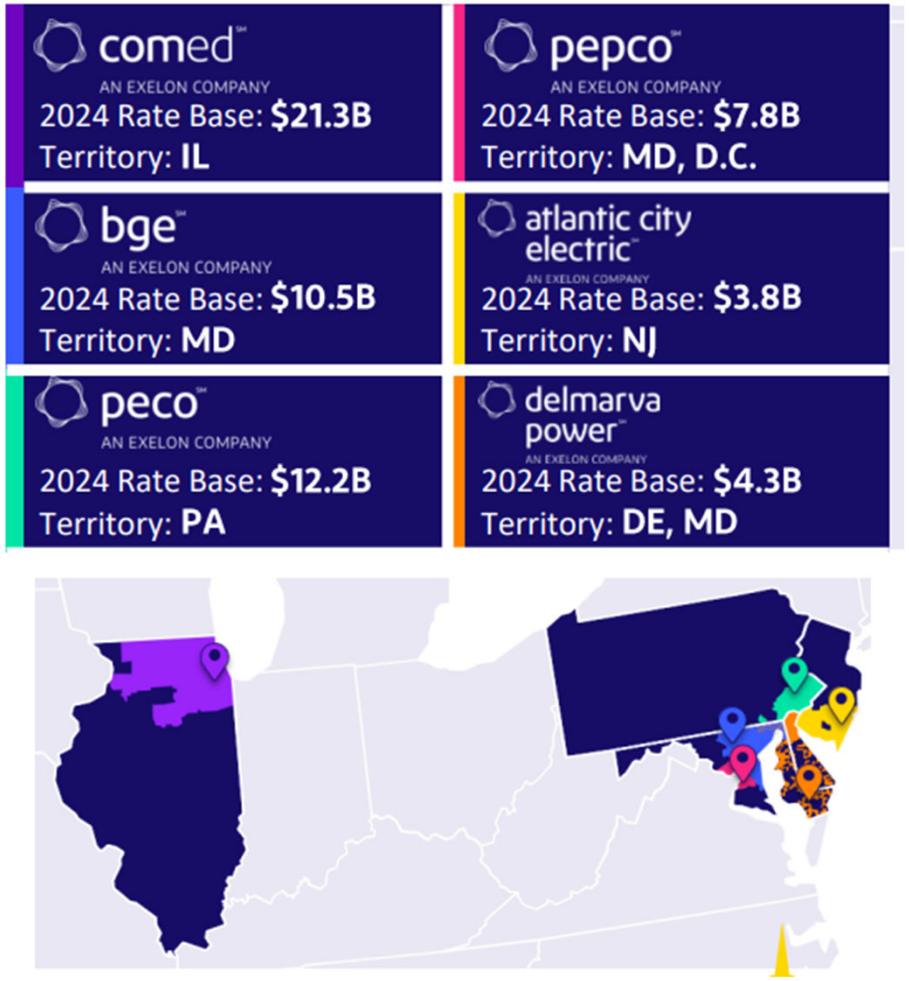
183,540
Circuit miles of electric and gas distribution lines

11,189
Circuit miles of FERC-regulated electric transmission lines

$23.1
Operating revenues recorded at our utilities in 2024

$64.1 billion
Rate base estimate for 2025

$38.0 billion
Projected capital investment through 2028



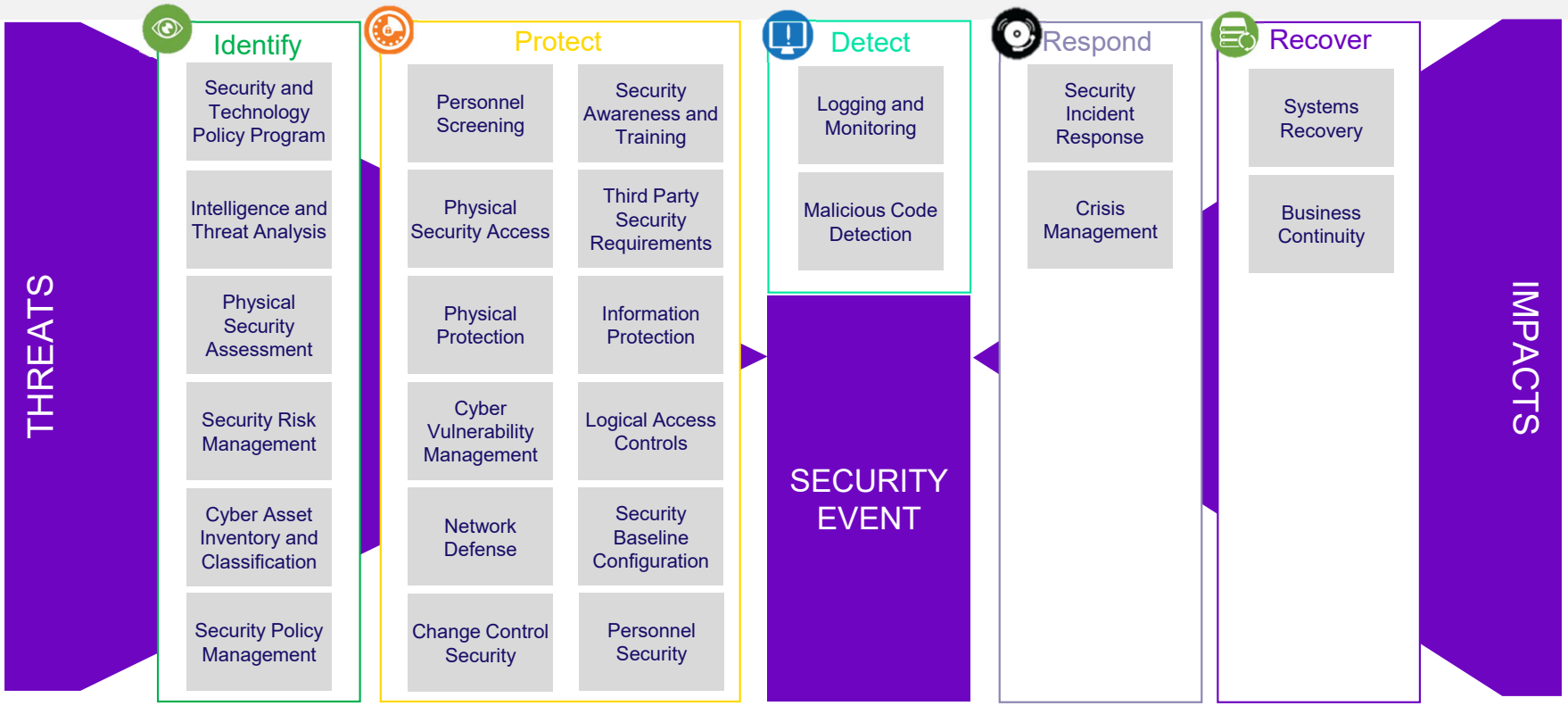
(1) Customer count reflects the sum of Exelon's total gas and electric customer base; Exelon consolidated customer count may not sum due to rounding

exelon

Enterprise Standards Governance at Exelon

What security programs make up Enterprise Standards Governance?

To appropriately address internal and external cybersecurity threats, Exelon has aligned its Security Program to the NIST Cybersecurity Framework (Identify | Protect | Detect | Respond | Recover). The programs below fall within the responsibilities of IT, OT, Physical, and Common Security and play key parts in assessing and preparing for threats, minimizing risk of security events, and preventing negative impacts from those events.



exelon

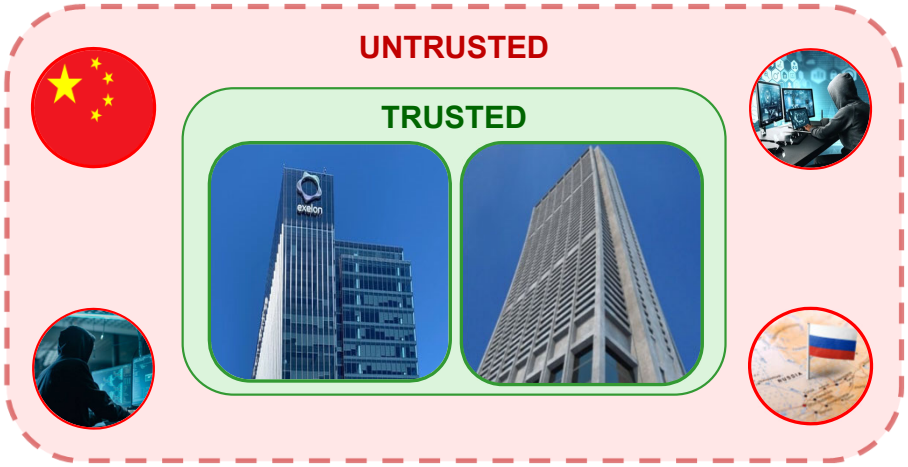
What Is SASE/Zero Trust and Why It Matters

A unified security and networking solution to keep users and data protected wherever and whenever they connect.

Zero Trust Security Model: Trust nothing by default. Verify users, devices, and actions before granting access. Assumes breach and enforces least-privilege access.

Old Model

Once you're inside the network, you're trusted.



A centralized IT environment where employees worked onsite, systems were on-prem, and security focused on the network perimeter.

New Model

Trust nothing without verification, access securely from anywhere.

A flexible, remote-friendly model where users, apps, and data are accessible from any location, requiring identity and device-based security controls.

exelon

exelon[SM]

External Partnerships

Exelon leverages partnerships and direct relationships to facilitate information sharing, but also to establish direct lines of communication. Exelon has established information sharing collaboration efforts with other utilities of similar size and service territory.

Government Agency

- Cybersecurity & Infrastructure Security Agency (DHS CISA)
  - Joint Cyber Defense Collaborative (JCDC)
- Federal Bureau of Investigation (FBI)
  - InfraGard
  - Gryphon Citadel
  - Threat Analytics Collaboration Unit (TACU)
- National Security Agency (NSA)
  - Defense Industrial Base Program
- Department of Energy (DOE)
  - Cybersecurity Risk Information Sharing Platform (CRISP)
  - Energy Threat and Analysis Center (ETAC)
  - Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

| Engagement Participation Initiatives |

- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Electricity Information Sharing and Analysis Center (E-ISAC)
- Downstream Natural Gas Information Sharing and analysis Center (DNG-ISAC)

| ISACS / organizations we work with |

Non-Government Agency

- National Association of Regulatory Utility Commissioners (NARUC)
- North American Electric Reliability Corporation (NERC)

| Collaborative Information Gathering Organizations |

- UNITE
  - Cyber Threat Intelligence Group (CTIG)
  - Cyber Mutual Assistance (CMA) Program

Edison Electric Institute (EEI)

- Electric Subsector Coordinating Council (ESCC)
- American Gas Association (AGA)
- Oil and Natural Gas Subsector Coordination Council (ONG SCC)

| Membership Programs |

CERTIFICATE OF SERVICE

I hereby certify that a copy of Potomac Electric Power Company's response and presentation to Cyber Security Hearing Data Request 1 was served this August 7, 2025 on all parties below via electronic mail.

Ms. Brinda Westbrook-Sedgwick
Commission Secretary
Public Service Commission
of the District of Columbia
1325 G Street N.W. Suite 800
Washington, DC 20005
bwestbrook@psc.dc.gov

/s/ *Dennis P. Jamouneau*
Dennis P. Jamouneau