STATE OF MARYLAND

PUBLIC SERVICE COMMISSION

April 10, 2024

In the Matter of Cyber-Security Reporting of Maryland Utilities	* * * * * * * *	Case No. 9492

NOTICE OF STATUTORY REQUIREMENT TO CONDUCT ASSESSMENTS AND SUBMIT CERTIFICATIONS TO COMMISSION

During the 2023 Session, the Maryland General Assembly enacted House Bill 969, entitled the Critical Infrastructure Cybersecurity Act of 2023 ("The Act"). The Act was codified in the Annotated Code of Maryland, Public Utilities Article ("PUA") § 2-108 and § 5-306, with an effective date of July 1, 2023. The Act imposes several requirements on public service companies,[1] including the following:

- Adopt and implement cybersecurity standards;
- Adopt a zero–trust cybersecurity approach for on–premises services and cloud–based services;
- Establish minimum security standards for each operational technology and information technology device based on the level of security risk for each device;
- On or before July 1, 2024 and on or before July 1 every other year thereafter (e.g., July 1, 2026), engage a third party to conduct an assessment of operational technology and information technology devices;
- Submit to the Commission certification of the public service company's compliance with standards used in the assessments; and
- Report any cybersecurity incident to the State Security Operations Center in the Department of Information Technology.

[1] "Public service company" has the meaning provided in PUA § 1-101 including investor-owned electric companies, electric cooperatives, municipal electric companies, gas companies and water companies, but excluding public service companies that are a common carrier or a telephone company per PUA §5-306(b).

In more depth, PUA § 5-306(c) provides the following language that relates to public service companies' assessment and certification responsibilities:

> (4)(i) on or before July 1, 2024, and on or before July 1 every other year thereafter, engage a third party to conduct an assessment of operational technology and information technology devices based on:
>
> 1. the Cybersecurity and Infrastructure Security Agency's Cross-Sector Cybersecurity Performance Goals; or
>
> 2. a more stringent standard that is based on the National Institute of Standards and Technology security frameworks; and
>
> (ii) submit to the Commission certification of the public service company's compliance with standards used in the assessments under item (i) of this item.

Pursuant to the Act, multiple third-party assessments may be required by a public service company to cover all operational technology[2] and information technology[3] devices. For example, North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") or Transportation Security Administration ("TSA") audits may only cover a portion of public service company operational technology and information technology devices. In accordance with PUA § 5-306(c)(4), certification of the public service company's compliance with standards shall be submitted to the Commission by July 1, 2024.[4] These certifications shall include the date each assessment was completed, the name of each third party that performed an assessment, and their qualifications to conduct NIST or CPG cybersecurity framework-based assessments. If consistent with the requirements of PUA § 5-306(c), audits performed as required by the NERC

[2] Pursuant to Code of Maryland Regulations ("COMAR") 20.06.01.02(3) an "Information technology system" means hardware and software related to electronic processing, and storage, retrieval, transmittal, and manipulation of data.

[3] In accordance with COMAR 20.06.01.02(4), an "operations technology system" means a system or network that monitors or controls electric, gas, or water system infrastructure used for utility operations.

[4] Documents that are uploaded in the "public" section of the e-file dropbox are made publicly available on the Commission's website. Therefore, a public service company should consider a confidential filing of certifications through e-file, or alternatively make arrangements for providing certifications directly with the Commission's Office of Cybersecurity at psc.cyberoffice@maryland.gov.

CIP standards or TSA schedules may be used as a third-party assessment for purposes of PUA § 5-306(c).

Any questions related to the Act's filing requirements should be directed to the Commission's Office of Cybersecurity at psc.cyberoffice@maryland.gov.

By Direction of the Commission,

/s/ Andrew S. Johnston

Andrew S. Johnston
Executive Secretary