Cybersecurity Incident Reporting

for Maryland Public Service Companies

Background

During the 2023 Session, the Maryland General Assembly enacted House Bill 969 entitled, "Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023). House Bill 969 was codified in Public Utilities Article § 2-108 and §5-306, Annotated Code of Maryland, which was enacted July 1, 2023. In accordance with the Critical Infrastructure Cybersecurity Act of 2023, public service company cybersecurity incidents[1] shall be reported to the Maryland Department of Information Technology (DoIT). DoIT's preferred methods to report cybersecurity incidents are described in the Cybersecurity Incident Reporting Requirements for Public Utilities Manual (DoIT Manual).

Maryland Public Service Commission (MD PSC) Reporting

DoIT will contact the MD PSC's Office of Cybersecurity once a cybersecurity incident is confirmed. Public service companies do not need to contact the MD PSC's Office of Cybersecurity unless there is an unusual situation or an impact that the utility wants to discuss with the PSC or make the PSC aware of directly.

MD PSC Office of Cybersecurity Contacts:

Christopher Perez-Nieves, Cybersecurity Specialist
443-965-6268 (Cell)
Email: psc.cyberoffice@maryland.gov

Damilare Olakunle (Daré), Cybersecurity Specialist
443-965-6269 (Cell)
Email: psc.cyberoffice@maryland.gov

[1] "Cybersecurity Incident" means a malicious act or suspicious event that compromises, or was an attempt to compromise, a public service company's cybersecurity device. "Cybersecurity device" means any combination of hardware, software, and related services, including informational technology systems, operational technology systems, and smart grid systems used for delivery of electricity, gas, or water, or systems that store customer information.