Cybersecurity Incident Reporting

for Maryland Public Service Companies

Maryland Department of Information Technology (DoIT) Reporting

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, the Maryland Department of Information Technology has established a Cybersecurity Incident Reporting Requirements for Public Utilities Manual (DoIT Manual). The Cybersecurity Incident Reporting Requirements for Public Utilities Manual is now in effect.

Maryland Public Service Commission (PSC) Reporting

Existing cybersecurity regulations in the Code of Maryland Regulations (COMAR) Title 20, Subtitle 06 Regulation .05, Cybersecurity Breach Reporting[1] also continue to be effective until waived by the Commission or superseded by new regulation proposals currently being drafted. The COMAR definition of a cybersecurity breach[2] is more limiting than the DoIT criteria for cybersecurity incident reporting in the DoIT manual. Public service companies shall verbally report confirmed cybersecurity breaches to one of the following:

Primary - PSC Office of Cybersecurity:

Christopher Perez Nieves, Cybersecurity Specialist
410-767-6390

Alternate - PSC Cybersecurity Reporting Workgroup (CSWRG) Leader:

John Borkoski, Senior Commission Advisor
410-269-9707

[1] Regulation .05, Cybersecurity Breach Reporting requires: All utilities shall report confirmed cybersecurity breaches of a smart grid system, information technology system, or operations technology system to a Commission-designated representative without divulging energy/electric infrastructure information, as defined by 18 CFR §388.113, no later than 1 business day after confirmation, unless prohibited or recommended by law enforcement to avoid compromising an investigation.

[2] "Cybersecurity breach" means any unauthorized act that has been confirmed to result in access to acquisition, control, destruction, disclosure, or modification of a utility's information technology systems, operations technology systems, or smart grid systems.