

# **Engineering Division Cyber Security Breach Reporting Procedure for Maryland Electric, Gas, or Water Companies**

## **Scope**

New cybersecurity regulations in the Code of Maryland Regulations (COMAR) Title 20, Subtitle 06 are effective as of July 25, 2022. 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.

## **Definitions**

“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.

“Information technology system” means hardware and software related to electronic processing, and storage, retrieval, transmittal, and manipulation of data.

“Operations technology system” means a system or network that monitors or controls electric, gas, or water system infrastructure used for utility operations.

“Smart grid system” means a system or network that enables a utility to gather and store personally identifiable customer information from customer devices or allows for the control of customer devices.

“Utility” means any electric company, gas company, or water company regulated by the Commission.

## **Reporting**

Utilities will verbally report security breaches to:

Primary Contact:

John Borkoski, P.E.  
Chief Engineer

Designated Alternates:

John Clementson  
Deputy Chief Engineer

Craig Taborsky  
Assistant Chief Engineer