COMMONWEALTH OF PENNSYLVANIA
PENNSYLVANIA PUBLIC UTILITY COMMISSION
COMMONWEALTH KEYSTONE BUILDING
400 NORTH STREET
HARRISBURG, PENNSYLVANIA 17120

February 25, 2022

To All Jurisdictional Pennsylvania Public Utilities:

As geopolitical tensions rise, the Public Utility Commission (PUC) and its federal and state stakeholders remind utilities to remain vigilant for cybersecurity threats that could impact their critical infrastructure. During this heightened state of cybersecurity awareness, the PUC recommends that utilities utilize the cybersecurity tips and information provided by the Cybersecurity and Infrastructure Security Agency (CISA) located on their National Cyber Awareness System (NCAS). The NCAS offers a variety of information for users with varied technical expertise.

In addition to reviewing the information on the NCAS website, the PUC strongly urges utilities to review CISA's Alert AA22-011A, Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure. The alert will provide you with an overview of Russian state-sponsored cyber operations; commonly observed tactics, techniques, and procedures (TTPs); detection actions; incident response guidance; and mitigations. The PUC also recommends utilities adopt a heightened state of awareness and conduct proactive threat hunting. We strongly recommend utilities implement CISA's recommendations and mitigations, which will help you improve your functional resilience by reducing the risk of compromise or severe business degradation.

The PUC recommends that utilities take the following actions:

- **Be prepared**. Confirm reporting processes and minimize personnel gaps in IT/OT security coverage. Create, maintain, and exercise a cyber incident response plan, resilience plan, and continuity of operations plan so that critical functions and operations can be kept running if technology systems are disrupted or need to be taken offline.
- **Enhance your organization's cyber posture**. Follow best practices for identity and access management, protective controls and architecture, and vulnerability and configuration management.
- **Increase organizational vigilance**. Stay current on cybersecurity threats. Subscribe to CISA's mailing list and feeds to receive notifications about cybersecurity topics or threats.

The PUC encourages utility executives and senior leaders to review CISA's document entitled "Preparing for and Mitigating Potential Cyber Threats." This document provides executives and senior management with information they can use to proactively take steps to prepare their organizations should an incident occur.

In addition to this information, CISA has created a cyber-threat website entitled Shields Up. This website provides steps organizations can take to ensure that:

- The likelihood of a damaging cyber intrusion is reduced.
- A potential intrusion is quickly detected.
- An organization is prepared to respond if an intrusion does occur.
- An organization has maximized their resilience in the face of a destructive cyber incident.

Finally, if your company has been the victim of a cybercrime, notify the appropriate regional FBI office. The FBI may be able to assist critical infrastructure owner/operators when there is a cyberattack or suspected cyber incident. The FBI regional offices are in Pittsburgh and Philadelphia. The Pittsburgh Office number is 412-432-4000 and the Philadelphia Office number is 215-418-4000.

Pennsylvania utilities can also report incidents to the Pennsylvania Criminal Intelligence Center (PaCIC). PaCIC is the primary All-Hazards Fusion Center for the Commonwealth of Pennsylvania. PaCIC coordinates the intake, processing and dissemination of intelligence and analysis concerning all threats and hazards to the Commonwealth. You can contact PaCIC at:

- 1-888-292-1919
- Email: tips@pa.gov

Cyber incidents identified in the Commission's cyber incident reporting regulations (52 Pa. Code §§ 57.11 (electric), 59.11 (gas), 61.11 (steam heating) and 65.2 (water)) need to be reported to the PUC's Lead Emergency Agency Representative (AREP). The PUC's Lead AREP can be reached at 717-941-0003.

Please let me know if you have any questions regarding this notification. I can be reached at 717- 425-5327 or via email at miholko@pa.gov.

Respectfully,

Michael Holko, Director, Office of Cybersecurity Compliance and Oversight
Pennsylvania Public Utility Commission
400 North Street, 3rd Floor North
Commonwealth Keystone Building, Harrisburg, PA 17120
717-425-5327 | miholko@pa.gov
www.puc.pa.gov |Consumer Hotline 1-800-692-7380
Follow us on: