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

March 3, 2026

To All Jurisdictional Pennsylvania Public Utilities and Licensed Electric Generations Suppliers, and Natural Gas Suppliers:

In response to the current geopolitical situation and the potential for increased cyber activity targeting domestic critical infrastructure, the Pennsylvania Public Utility Commission (PUC) is sharing the following recommendations. While these are not mandates, they represent high-priority security practices designed to help Pennsylvania's regulated utilities strengthen their defenses against potential retaliatory cyber operations.

Recommended Security Measures

1. **Network and Asset Isolation**: Identify Industrial Control Systems (ICS) or Operational Technology (OT) assets currently connected to the public-facing internet. Consider disconnecting or further isolating these systems from the public web whenever possible to minimize the risk of unauthorized remote access.
2. **Credential and Access Management**: Review all default passwords on Programmable Logic Controllers (PLCs) and human-machine interfaces (HMIs), ensuring they have been updated to unique, complex credentials. Implement Phishing-Resistant Multi-Factor Authentication (MFA) for all remote access points, including VPNs, administrative portals, and third-party vendor connections.
3. **Vulnerability Mitigation Prioritize**: Patch "Known Exploited Vulnerabilities" (KEVs) on all edge devices, such as firewalls and remote management tools. Review and audit all remote monitoring and management (RMM) software; disable tools or services that are not strictly necessary for current operations.
4. **Monitoring and Incident Response:** Review your current Business Continuity and Disaster Recovery (BCDR) Plans. Ensure your plans are up to date for the current threat landscape. Increase the frequency of log reviews, specifically looking for unusual remote desktop protocol (RDP) or virtual network computing (VNC) connections that may indicate unauthorized lateral movement.

Identifying "Living off the Land" (LOTL) Activity

Threat actors are increasingly avoiding custom malware in favor of legitimate system tools to evade detection. The PUC recommends monitoring your IT/OT environments for:

1. **Native Tool Abnormalities**: Investigate unusual execution of PowerShell, WMI, or Net.exe by non-administrative accounts.
2. **Persistence Checks**: Audit scheduled tasks and registry "run" keys for unauthorized entries using system binaries to establish persistence.

3. **Host-Based Telemetry**: Monitor for the use of legitimate tools (e.g., NTDSutil.exe) to dump credentials or directory databases.

CISA Resources and Supporting Documentation

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 this, the following resources provide technical details and recent alerts that are associated with the current threat landscape:

- CISA: Iran Threat Overview and Advisories – Provides historical context and specific TTPs used by Iranian actors against US infrastructure.
- CISA: Shields Up – Provides a high-level defensive posture and specific hardening checklists to protect critical infrastructure from imminent cyberattacks.
- CISA: Identifying and Mitigating LOTL Techniques – A comprehensive guide on detecting stealthy activity that uses built-in system tools.
- CISA: Known Exploited Vulnerabilities (KEV) Catalog – A recommended baseline for utilities to prioritize patching.
- CISA Cross-Sector Cybersecurity Performance Goals (CPGs): A prioritized subset of IT/OT cybersecurity practices to reduce risk.

Reporting

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,

PAPUC

www.puc.pa.gov

Michael Holko, Director
Office of Cybersecurity Compliance and Oversight
400 North Street, 3rd Floor North
Commonwealth Keystone Building
Harrisburg, PA 17120
Phone: 717-425-5327
Email: miholko@pa.gov
Consumer Hotline:1-800-692-7380