Security Update

Jim Gluck
Sr. Director, Cybersecurity

Operating Committee
November 5, 2026

Disclaimer: While materials are current at the time of publishing, applicable requirements may change. PJM Governing Documents control.

PJM © 2026

Important Security Alerts

- Nation-state threat actors exfiltrate sensitive data globally, including from US critical infrastructure.
- Critical PHP vulnerabilities disclosed require immediate patching.
- CISA CIRCIA incident reporting requirements move closer to publication.

Monitored Threats

- Exploitation of unpatched vulnerabilities
- Phishing and smishing attacks
- Use of deepfake and Adaptive AI technology
- Distributed Denial of Service attacks

Contact PJM

- To report unusual events, notify your normal PJM contacts.
- To report connectivity issues, contact Member Relations.
- To report suspicious email, notify SecurityAlertTm@pjm.com.
- Share this info with your security team.

PJM © 2026

Contact

Presenter:
Jim Gluck,
jim.gluck@pjm.com



Security Update

Member Hotline

(610) 666 – 8980

(866) 400 – 8980

custsvc@pjm.com

PJM © 2026

PROTECT THE POWER GRID

THINK BEFORE YOU CLICK!

pjm





BE ALERT TO MALICIOUS PHISHING EMAILS

Report suspicious email activity to PJM.

Call (610) 666-2244 or email it_ops_ctr_shift@pjm.com

PJM © 2026