Problem/Opportunity Statement

CYBERSECURITY INCIDENT DISCLOSURE~~DISCLOSURE TO PJM OF CYBER INCIDENT~~

PROBLEM / OPPORTUNITY STATEMENT

- The occurrence of a cyber-issue affecting a Member could have a serious impact on the PJM IT infrastructure as the PJM systems are connected to Member systems.
- PJM needs the ability to ascertain whether a cyber incident affecting a member could have the potential to impact PJM or other members.
- This is an opportunity to obtain valuable information and time to mitigate potential threats to the PJM infrastructure markets, grid, and ability to operate.
- Cyber threats and threat actors are becoming more sophisticated and all critical infrastructure is at an increased risk for such attacks.
- Risks can be identified and mitigated through this opportunity to have notice of such occurrences
- This task is intended to address potential cyber risks and not larger policy issues.
- The Securities and Exchange Commission has promulgated rules requiring publicly traded companies to make cyber disclosures. Not all PJM Members are SEC traded companies.
- Lack of notification to PJM of cyber incidents could ~~delay mitigation of a cascading threat.~~ : (1) delay preventive defensive action by PJM, (2) delay actual threat identification to PJM, and (3) expose other members to cyber or financial risk.
- Cyber incident could constitute a material adverse event or present a risk of default that in turn could present a risk of default to the other members.
-