Post Quantum Cryptography Rollout to External Stakeholders

Nicole Mejia, Sr. Analyst I
Garrett Laman, Sr. Security Architect I

Tech Change Forum
June 15, 2026

Quantum Computing Risk on Encryption

Quantum Computing Risk

- Traditional asymmetric encryption (e.g. RSA 4096) is strong today against classical computing threats.
- Rapid advancements in quantum computing could enable the breaking of widely used traditional asymmetric cryptographic algorithms as early as 2029.

The “Harvest Now, Decrypt Later” Risk

- Adversaries are currently collecting encrypted data, intending to decrypt it once they have powerful quantum computers.
- Data encrypted today that needs to remain secret for 5-20 years is already at risk from future quantum-enabled attacks.

PQC Deployment for PJM External Applications

PJM Approach

- Transition external facing web applications and APIs to **TLS 1.3** to simplify protocol negotiation, remove obsolete cryptography and improve performance.
- Leverage TLS 1.3 to deploy a **hybrid key exchange** that maintains strong security while transitioning to **post-quantum cryptography**.
- Establish TLS 1.3 as the preferred protocol, while continuing to support TLS 1.2 to ensure **backward compatibility**, with gradual TLS 1.2 retirement aligned to industry guidance and stakeholder readiness.
- External stakeholders may need to update client software to gain the benefits of the transition.
- *Monitor public PKI and browser support for **hybrid certificates** and when broadly supported, will transition to hybrid certificates through the existing certificate renewal process.*

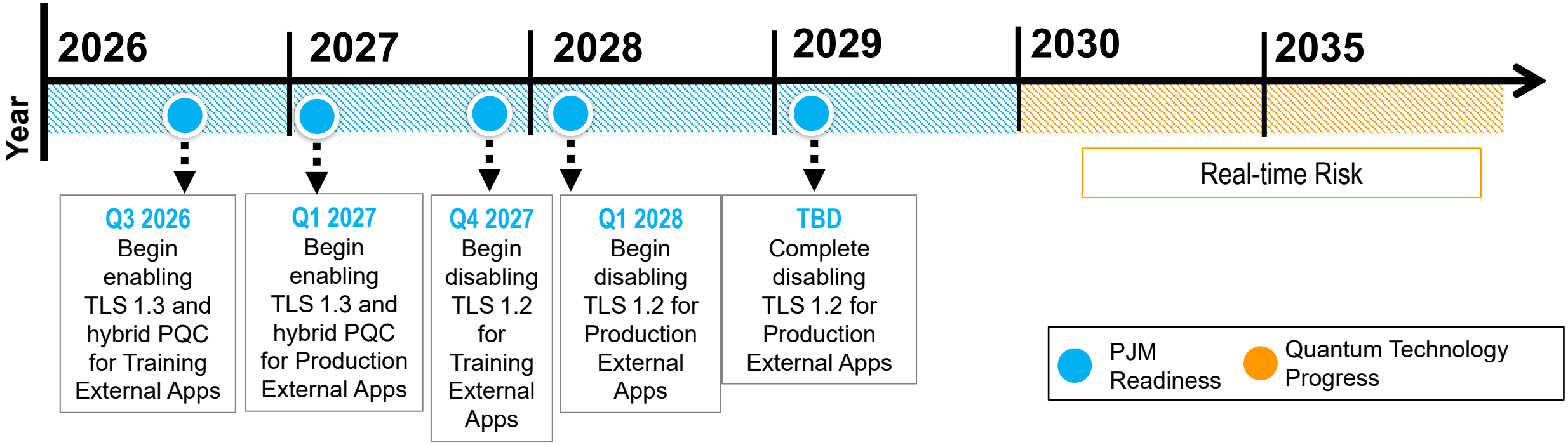
Member Action

Action Required	Deadline	Who May Be Affected
Update clients to support Post-Quantum Cryptography (PQC) as applicable. https://www.pjm.com/-/media/DotCom/etools/security/tls-1-3-transition-guide.pdf	**TBD, PJM will enable PQC with backward compatibility initially**	Participants who use PJM's internet facing applications and use standard encryption on their clients.

Timeline

Harvest Now, Decrypt Later Threat
Encrypted data captured today may be decrypted in the future using capable quantum computers

Quantum Threat Realization
Capable quantum computers become available



Key Takeaways

1	2	3
• Quantum computers present a current and future threat to the unintended disclosure of member data	• To protect member data, PJM will roll out support for PQC on external facing applications	• Participants may need to update clients to gain the benefits of quantum resistant security

Contact

Presenter:
Nicole Mejia, Nicole.Mejia@pjm.com
Garrett Laman,
Garett.Laman@pjm.com

SME:
Quantum Safe Readiness Program – Core Team,
QuantumProgram_CoreTm@pjm.com

Post Quantum Cryptography

Member Hotline

(610) 666 – 8980

(866) 400 – 8980

custsvc@pjm.com