##### August 20, 2025

**TO:** All Interested Parties

**FROM:** Amrit Nagi, Staff Attorney

**RE: WEQ/RMQ/WGQ Cybersecurity Activities**

The WGQ Electronic Delivery Mechanism (EDM) Subcommittee and RMQ Information Requirements and Technical Electronic Implementation Subcommittee (IR/TEIS) voted out a recommendation as part of their coordinated annual review of the cybersecurity and technical standards. This work included validating and updating technical references, correcting outdated or obsolete citations, and revising HTML references to reflect its current “living standard” status. The subcommittees confirmed that current encryption methods remain adequate, addressed minor corrections to timing examples, and added cross-references between cybersecurity and the Quadrant Electronic Delivery Mechanisms (QEDM) manuals to provide more complete guidance. As part of this process, participants reaffirmed that future annual reviews will cover the entirety of each manual to ensure all data fields, minimum technical characteristics, and supporting references remain accurate and up to date. A formal comment period began on August 13, 2025 and will end on September 12, 2025.

The WEQ Cybersecurity Subcommittee is continuing its annual review of the WEQ Business Practice Standards and the Accreditation Requirements for Authorized Certification Authorities (ACAs). As part of this review, the subcommittee examined recent and proposed NERC Critical Infrastructure Protection (CIP) Reliability Standards, as well as recent FERC actions related to cybersecurity, and determined that no changes to the WEQ Standards are needed at this time. The subcommittee agreed to continue to monitor these activities, including upcoming work on supply chain risk management and other CIP initiatives, to assess any potential impact in the future. The subcommittee also advanced proposed updates to the ACA requirements to clarify applicability, align with guidance from the National Institute of Standards and Technology (NIST) on algorithm key size and strength, and set an effective date for phasing out the Digital Signature Algorithm (DSA). These revisions are intended to improve clarity, ensure consistency across the document, and reflect evolving security practices. In addition, the group reviewed NIST’s recent recommendations on post-quantum encryption and discussed how the current requirement for RSA and ECDSA related to one another. A vote on the ACA revisions, along with a no action recommendation for other assigned items, is planned for the next meeting on August 27, 2025.