November 4, 2019

**Quadrant:** Wholesale Electric Quadrant

**Subcommittee:** Executive Committee

**Recommendation:** 2019 API 6.a, 6.b.ii, and 6.c.ii

**Submitted By:** PJM Interconnection, LLC

PJM appreciates the opportunity to offer comments in response to NAESB’s October 4, 2019 request for Formal Comments pertaining to the 2019 WEQ Annual Plan Items 6.a, 6.b.ii, and 6.c.ii.

After careful review, PJM would like to raise the following points for consideration.

## 002-5 IMPLEMENTATION AND PERFORMANCE REQUIREMENTS

The recommendation contains several “best practices” regarding the implementation and operation of both an OASIS Node and the related supporting infrastructure. These best practices appear to be derived from the surety assessment performed by Sandia National Laboratories which posits that the lack of OASIS Node implementation details in the Business Practice Standards creates a risk that “there are insecure system configurations that may provide an attack vector to an adversary.”

PJM can easily support the majority of these recommended best practices; however, we offer the following commentary on a select few:

* **Timely application of latest software patches and updates, ideally within seven days after the patch or update becomes available.**
	+ We note that although this best practice is meant to decrease the likelihood of security vulnerabilities, the phrasing does not specify that security-related patches and updates should be the focus; rather, the recommendation calls for the implementation of *every* software patch and update that could potentially apply to the infrastructure supporting an OASIS Node, regardless of functional impact. We feel this requirement is too broad in its scope.
	The surety assessment explains that updates and patches can have detrimental impacts on functionality, and our own experience has shown this to be a real concern. As such, we feel that the operator of an OASIS Node should have the latitude to choose whether to apply software updates that are potentially disruptive but do nothing to improve the node’s security posture. We recommend this change to the phrasing: “Timely application of latest security-related software patches and updates . . .”
* **Performing vulnerability scans and penetration testing of OASIS applications at least quarterly.**
	+ We believe the best practice, as found in the surety assessment, was unintentionally altered when incorporated into WEQ-002. The surety assessment states: “. . . the team recommends conducting internal and external scans of the nodes on a quarterly basis, and a security assessment or penetration test.” We note that it is the internal and external scans that are recommended on a quarterly basis, not the security assessment or penetration test; however the proposed language indicates that penetration tests must also be conducted quarterly.
	In PJM’s view, the mandate for a quarterly penetration test ignores that the operator of the OASIS Node will be in the best position to judge when the supporting software or infrastructure has changed in a manner that merits a new penetration test. Absent a material change to the OASIS node, and given that vulnerability scans occur on a regular basis, additional penetration testing provides questionable value. The authors of the surety assessment seemed to appreciate the complexities involved with this process as they state: “Since each node can be unique in its software, environment, and supporting security systems, the assessment team recommends that the node owner perform these assessments on their own systems.”
	With respect to our comments above, we recommend the following change: “Performing vulnerability scans of OASIS applications at least quarterly and penetration testing of OASIS applications at least annually. Additional penetration tests should be conducted when the OASIS Node is impacted by significant software, infrastructure, or network changes.”