**via posting**

**TO:** Interested Industry Parties

**FROM:** Elizabeth Mallett, Director, Wholesale Gas Quadrant and Retail Markets Quadrant

**RE:** Final Minutes from October 23, 2023 WEQ Business Practices Subcommittee (BPS), RMQ BPS, and WEQ Cybersecurity Subcommittee (CSS) Meeting

**DATE:** November 14, 2023

**WHOLESALE ELECTRIC QUADRANT**

**RETAIL MARKETS QUADRANT**

**Business Practices Subcommittees and Cybersecurity Subcommittee**

**Conference Call**

**October 23, 2023 – 1:00 PM to 3:00 PM Central**

**FINAL MINUTES**

1. **Welcome**

Mr. Phillips welcomed the participants to the meeting. Ms. Trum provided the antitrust and meeting policies reminder. The participants introduced themselves. Mr. Phillips reviewed the agenda. Mr. Brooks moved, seconded by Mr. Galloway, to adopt the agenda as final. The motion passed a simple majority vote without opposition.

The participants reviewed the draft minutes from the October 5, 2023 meeting. A minor change was made to correct the attendance list. Mr. Brooks moved, seconded by Ms. Kee, to adopt the revised minutes as final. The motion passed a simple majority vote without opposition. The final minutes for the October 5, 2023 meeting can be viewed at the following link: <https://naesb.org/pdf4/weq_bps_css_rmqbps100523fm.docx>.

1. **Continue to Discuss** **2023 WEQ Annual Plan Item 3.d 2023 RMQ Annual Plan Item 4.a – Review cybersecurity protections, such as Public Key Infrastructure (PKI), that may be necessary to secure electronic communications for distributed energy resources (DERs), and develop business practices as needed**

Mr. Phillips asked Ms. Kee to review her presentation, Cybersecurity for EV Fast Charging Networks. Ms. Kee stated that NIST, in conjunction with the National Cybersecurity Center of Excellence, developed a cybersecurity framework profile for electric vehicle extreme fast charging infrastructure based on the NIST Cybersecurity Framework. She explained that while the profile is specific to fast charging infrastructure, the security objectives are likely applicable to any DER: (1) deliver reliable performance through secure communications; (2) maintain resilience of infrastructure; (3) build and maintain trustworthy relationships between parties; and (4) maintain continuity of operations. Ms. Kee noted that the NIST Cybersecurity Framework specifically calls for multifactor authentication and identifies a need issue, manage, verify, revoke, and audit identities and credentials for authorized devices, users and processes. She stated that the NAESB PKI Framework would meet these requirements and could be a viable, scalable, and affordable method to protect DER transactions.

The participants reviewed the U.S. DoE White Paper – Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid. Mr. Brooks observed that there are likely to be multiple layers of interactions, including communications between a utility and DER aggregator and then the DER aggregator and individual DERs. Mr. Galloway asked if there are existing standards addressing DER aggregator communication protocols. Mr. Brooks responded that there is not an industry consensus for standards in this area. He noted that there are some industry standards regarding interconnection by inverter-based resources but that most of the available guidance addresses operational and performance considerations or cybersecurity in the design of a DER.

Ms. Trum stated that during the previous meeting, the participants had noted that there may be industry white papers developed by NERC that could be useful for subcommittee discussions. She noted that NAESB and reached out to NERC staff who provided the NERC Privacy and Security Impacts of DERs and DER Aggregators and identified the NIST SP1800-32 Security DER Resources as one of the documents referenced in the creation of the NERC white paper.

The participants reviewed the NERC Privacy and Security Impacts of DERs and DER Aggregators white paper. Mr. Brooks stated that in considering cybersecurity protections, there is a differentiation between requirements that establish access control and those that relate to authorization. He explained that access control requirements ensure that a party possesses the proper credentials to gain access to a tool or system while authorization requirements address what types of actions a party can perform once access is gained. Mr. Brooks suggested that the development of business practices by NAESB should focus on access control and creating a standardized process or method for party identification and verification.

Mr. Phillips asked how such a process could be structured. Mr. Brooks suggested that one method to consider is modeling requirements based on a use case similar to how NAESB PKI digital certificates are used to control access software platforms such as OASIS nodes. Mr. Galloway stated that any standardized protocol to protect DER-related communications would need to be scalable and supportive of identity verification being shared or transitive. He noted that ISO-New England uses NAESB PKI digital certificates to control access to an internal software platform but that only a few thousand clients require access. Mr. Galloway stated that PKI could be leveraged as a foundational element for some cybersecurity protections that may be needed but that use of digital certificates to protect communications with individual DERs may be difficult as it would be challenging to have a single central authority verify all DER identities. Mr. Brooks agreed that installing a digital certificate on every DER may not be feasible at this time and suggested that this is an area participants discuss in greater detail. Ms. Kee stated that there is widespread use of PKI digital certificates for authentication purposes and that the scalability of issuing a digital certificate is separate from certificate management. Mr. Brooks noted that the U.S. DoE White Paper – Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid is supportive of the use of PKI.

Mr. Galloway stated that while FERC has issued directives to NERC regarding cybersecurity for inverter-based resources, these efforts will likely not address access control considerations and that NAESB standards in this area could be beneficial. Ms. Kee stated that in discussing possible requirements, it will be important to consider the continuity, availability, and scalability of a solution. Mr. Galloway suggested that the development and evaluation of use cases will be important to identify the potential concepts and solutions to address as part of the standards.

1. **Other Business**

Mr. Phillips suggested that for the next meeting, as an initial step in the development of use cases, the participants focus on identifying the different communication paths between parties that are interacting with DERs and the types of data that would need to be exchanged.

1. **Adjourn**

The meeting adjourned at 2:32 PM Central on a motion by Mr. Galloway.

1. **Attendance**

| **First Name** | **Last Name** | **Organization** |
| --- | --- | --- |
| Rebecca | Berdahl | BPA |
| Dick | Brooks | Reliable Energy Analytics |
| Michelle | Coon | OATI |
| Keith | Dalia | Bonneville Power Administration |
| Kate | Davis | BPA |
| John | Galloway | ISO-New England |
| Lila | Kee | GlobalSign |
| Annabelle | Lee | Nevermore Security |
| Elizabeth | Mallett | North American Energy Standards Board |
| Catherine | Meiners | ERCOT |
| Joshua | Phillips | Southwest Power Pool |
| Lisa | Sieg | LG&E and KU |
| Scott | Stewart | Bonneville Power Administration |
| Caroline | Trum | North American Energy Standards Board |
| Sam | Watson | North Carolina Utilities Commission |
| Jason | Williams | Southern Company |