Tucson Electric Power | UNS Electric, Inc.

88 East Broadway Blvd. | Post Office Box 711 | HQE910 | Tucson, AZ 85702-1702

June 30, 2025

RE: *In the matter of filing of In the matter of the Generic investigation into cyber threats to critical infrastructure and data. (ACC-00000A-20-0008)*

Tucson Electric Power and UNS Electric, Inc. ("TEP" and "UNS Electric," collectively "Companies") are providing this information in response to Vice Chairman Myers' request for information regarding Chinese-manufactured solar inverters and potential cybersecurity vulnerabilities.[1] In general, the questions focus on the prevalence of, and potential threats from, Chinese-manufactured inverters in our generation system. We appreciate Vice Chairman Myers' concern to ensure utility services are adequately protected.

As of the writing of this response, the Companies have identified four solar projects that have Chinese-manufactured inverters. These projects total thirty-four megawatts and represent less than one percent of the Companies' total resources.[2] If such inverters contain a "kill switch", and were individually or simultaneously activated, the Company is confident that it could maintain system reliability.

The Companies share your concerns regarding the potential vulnerability of utility infrastructure. As previously reported to the Commission, the Companies have a comprehensive cyber security program, with policies, plans, and procedures to secure Company systems from cyber threats, including those to critical infrastructure and other systems.[3] The Companies' most critical utility assets are regulated under the North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP"). The Companies continually upgrade and test their systems to ensure the security and reliability of enterprise-wide cyber infrastructure. The Companies also employ safeguards to prevent cyber-attacks that could result from any threat, including Chinese-manufactured inverters.

The Companies have an established cybersecurity incident response plan, backed by mutual assistance agreements and third-party incident response parties, including a crisis management protocol which provides an inter-departmental response capability to major events, which could include a 'kill switch' event. The Companies subscribe to resources such as the Electricity Information Sharing and Analysis Center ("E-ISAC"), Edison Electric Institute ("EEI"), and Cybersecurity and Infrastructure Security Agency ("CISA") notices and other information sharing mechanisms. The Companies also utilize threat intelligence tools beyond those resources in addition to leveraging our Fortis Inc. subsidiary network for additional layers of information sharing.

The Companies appreciate Vice Chair Myers' leadership on this very important topic.

---

[1] https://docket.images.azcc.gov/E000044461.pdf?i=1750704530096

[2] The Companies (combined systems) has identified that only 3% of its renewable resources and storage systems use Chinese-manufactured inverters. This includes owned systems and those under purchased power agreements. The Companies do not source Chinese-manufactured inverters for owned renewable energy systems. For purchased power agreements, we require that project owners abide by all applicable laws which include federal cyber security rules.

[3] https://docket.images.azcc.gov/E000012345.pdf?i=1750704530096, https://docket.images.azcc.gov/E000005065.pdf?i=1750704530096

ACC - Docket Control - Received 6/30/2025 12:01 PM
ACC - Docket Control - Docketed 6/30/2025 1:19 PM