



Regulatory Affairs
PAB4TB | P.O. Box 52025
Phoenix, AZ 85072-2025

June 30, 2025

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

Dear Chairman and Commissioners,

Thank you for your inquiry regarding recent news articles highlighting potential unauthorized and undisclosed communications hardware capabilities embedded in inverter-based resources (IBRs). Salt River Project Agricultural Improvement and Power District (SRP) takes threats to critical infrastructure seriously and uses leading cyber security, physical security, and supply chain practices to protect against, as well as prepare appropriate resilience to, potential impacts.

Sourcing and Operating Solar Inverters and Related Infrastructure

SRP has reviewed the articles cited in the above-referenced docket. Nearly all of SRP's current portfolio of IBR's are purchased power agreements from projects that are developed, owned and operated by other parties. SRP is in the process of surveying these project owners to determine if they are using equipment from the vendors in question.

SRP also owns and operates three IBR facilities. One of these facilities is a small pilot facility that is being built by SRP to test equipment from various manufacturers for possible use in future SRP-owned facilities. The overall size of this facility will be about 55 MW. For this particular project, there is equipment on order from one of the vendors in question for an 18 MW portion of this facility. This equipment was ordered over six months ago. When the equipment arrives on site, it will be inspected before being placed into operation to confirm there are no unauthorized communication devices. In addition, SRP has also been in contact with the manufacturer, and the manufacturer has provided certification that no communications devices have been installed. The other two IBR facilities, owned by SRP, do not utilize any equipment from the vendors in question.

IBRs, such as solar generation, inherently produce variable power output. Solar resources, in particular, cycle offline each night and are subject to fluctuations due to weather conditions and seasonal changes. The power system is deliberately planned and engineered with built-in flexibility and redundancy to accommodate these variations. Grid operators account for the intermittent nature of IBRs by integrating a diverse mix of generation sources, reinforcing transmission infrastructure, and employing operational safeguards to ensure consistent reliability. Even during periods of high demand—such as peak summer days—the system is structured to maintain power delivery through advanced forecasting, reserve margins, and dynamic grid management. Consequently, while unexpected reductions in solar output may create localized challenges, the broader grid remains capable of adapting without compromising overall reliability.

Maintaining the Security of the Bulk Electric System

SRP operates a robust cyber security program and works closely with industry and government partners to build a network of information sharing, coordinated incident response, and collaboration on critical infrastructure protection issues. Extensive network segmentation, monitoring, and preventive controls are used to mitigate and protect against evolving cyber threats that target employees, processes, and technologies. Additionally, corporate risk management and emergency management practices are in place to ensure ongoing resilience to the changing threat landscape.

SRP monitors developing policy and adheres to industry regulations, including compliance with all cyber security standards designed to protect critical systems to ensure the reliability and resilience of the power grid. These mandatory security regulations are overseen by the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), and the Western Electric Coordinating Council (WECC).

SRP remains steadfast in its commitment to ensuring the security and resilience of our infrastructure.

Thank you for the opportunity to provide input on this important matter.

Sincerely,

SRP Regulatory Affairs