ORIGINAL

E000045048

TRICO
AN ENERGY COOPERATIVE

June 30, 2025

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

Arizona Corporation Commission:

Trico Electric Cooperative, Inc. provides the following response to the questions posed in Vice Chair Myers' letter dated May 30, 2025 ("Letter"). Trico has attempted to provide as much information as practical given security considerations. Trico places a significant amount of focus on site and system security at every stage from planning to construction, to operation. Trico has engaged in a variety of operational and strategic projects to ensure and enhance security on its system and continues to focus on this issue.

Trico has identified eight (8) inverters at its solar and battery facilities which include Chinese components or are produced by one of the companies named in the articles referenced in the Letter. These inverters support 21MW of solar generation capacity.

As part of its planning and security process, Trico works with its development, engineering, procurement, and construction partners to identify the supply chain and source country of equipment including inverters. Trico's Solar/BESS Technicians have been certified to work on the installed inverters and visited the United States based assembly plant for training. They work on-site with the systems regularly.

After receiving the Letter, Trico has again reviewed its parts lists, as-built drawings, and records. In addition, Trico's Manager of Electrical and Generation Services, two Solar/BESS Technicians, and Electrician visited each of Trico's solar and battery facilities and inspected the inverters (and related components). This review took into consideration the details described in the articles referenced and the issues listed in the Letter. Trico's staff is satisfied there are no unexpected components.

In addition to the on-site review and analysis processes Trico has in place, Trico also enforces other system protections. Trico views its solar generation inverter systems as "air gapped" and there are several protection methods, tools, and pieces of equipment in place. For security reasons, we are not setting out these measures in detail.

Trico is not aware of any government agency or third-party lab that performs a pre-delivery review of parts or equipment for cybersecurity purposes. Trico performs its own internal review along with the assistance of its development, engineering, procurement, and construction partners before systems are placed into service.

Trico is always working to improve its cybersecurity and is currently enhancing its processes for supply chain risk management for software. Trico does have a plan in place for recovery in the event of the loss of one of its solar and battery sites. As an example, Trico maintains an Emergency Response/Restoration Plan ("ERP") as required by the RUS and exercises this plan regularly. An update and enhancement of the ERP was just completed by a Trico Strategic Project Team. There are also protections in place to mitigate risk to Trico's wider system.

Trico projects that its ability to ensure uninterrupted power would not be significantly impacted by an "attack" on its solar and battery facilities. Still, these systems do provide value to Trico's Members and Trico focuses substantial effort to ensure the facilities are secured and protected.