ARIZONA CORPORATION COMMISSION

May 30, 2025

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

Load Serving Entities and Electric Cooperatives:

I am writing to request information regarding your awareness of and response to the issues highlighted in recent news stories involving Chinese-manufactured solar inverters and potential cybersecurity vulnerabilities.[1]

These news stories raise concerns about unauthorized and/or undisclosed communications hardware and potential backdoors or "kill switch" capabilities embedded in solar technology originating from China. Given the critical nature of utility infrastructure and the increasing reliance on inverter-based technologies like solar, wind, and battery power systems, these news stories raise urgent questions about supply chain security and Arizona's grid resilience.

To better understand how Arizona electric utilities are addressing these concerns, I would appreciate your response to the following questions:

1. Are any of the solar inverters or related infrastructure, including wind and battery inverters, in your system sourced from manufacturers referenced in these news stories or any other Chinese companies?
    a. If so, what is the total number of inverters that have been identified?
        i. Do you require supply chain transparency or specific security certifications from your inverter suppliers?
        ii. Has there been any analysis done to determine if any unidentified, undesired, unexpected, extra, or apparently "superfluous" components are present in the inverters?

[1] Sarah Macfarlane, "Rogue communication devices found in Chinese solar power inverters," Reuters, May 14, 2025, https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/; Hugh Tomlinson, "Chinese 'kill switches' found hidden in US solar farms," The Times, May 15, 2025, https://www.thetimes.com/us/news-today/article/china-solar-panels-kill-switch-vptfnbx7v; Robert Freedman, "'Rogue' communication devices found on Chinese-made solar power inverters," Utility Dive, May 15, 2025, https://www.utilitydive.com/news/rogue-communication-devices-found-on-chinese-made-solar-power-inverters/748242/; Oliver Moody, "Denmark finds 'suspicious components in key infrastructure imports," The Times, May 22, 2025, https://www.thetimes.com/world/europe/article/denmark-finds-suspicious-components-in-asian-circuit-boards-v0wzd8k6d.

iii. Do you require manufacturers you purchase from to provide parts lists for inverters?
    1. If so, do you verify those lists?
        a. Are those lists verified by any third-party lab here in the U.S.?
        b. Is there any part of the import process where the government or some other American entity performs a quality control check on the devices with inverters?
        c. Does a review happen before being placed in service or at the end of life of the device during the disposal process?
        d. Are these issues being considered in your future procurement policies?

iv. Is there a potential for those undisclosed components to cause inadvertent or undesired operations?

v. What steps were taken to attempt to identify those components and/or the component functions?

vi. Are the unexpected, extra, or superfluous components identified as being used in potential software upgrades or requiring the purchase of an additional software license to be functional?
    1. What software upgrades/keys are available on the inverters that you have *not* purchased, or you are not using?

vii. Are any of these inverters physically or wirelessly connected to the internet, or are they all "air gapped"?
    1. If the inverters are connected to the internet, either wirelessly, cellularly, or wired, is there monitoring done to continuously check for unintended/undesired communications regardless of firewall or VPN status?
    2. Please note that the existence of a local network to facilitate communications and linking between same make/model inverters is not of concern because this is expected operation when in a "ganged configuration," but it could be a concern if that communication is attached to a wide-area network or the internet.
    3. Also, any inverter that is connected to a LAN/WAN that is "VLAN'd" is not considered "air gapped" for this discussion. Please identify if the inverters are on a VLAN within a network that is otherwise connected to the internet.

b. How many megawatts do those inverters provide to the grid, individually and in the aggregate?
    i. By "aggregate," I mean both in a "ganged configuration" or a total aggregate across the system. Please answer this question in both contexts.

    c. Is there any statistical information on how many of those converters, and megawatts of those inverters, are active on your system at any given time?
    d. Should all of these inverters be shut down simultaneously, what would the impact be to your grid?
2. Have you identified any unauthorized communications or irregularities in your installed equipment?
3. Have you replaced or disabled any affected inverters based on these or prior concerns?
4. What protocols do you follow for evaluating the cybersecurity of imported solar, wind, and battery technologies?
5. How many foreign inverters are on your system, Chinese or otherwise?
6. What steps are you taking to detect and mitigate the risk of remote access or command-and-control functionality within your grid-connected inverters?
    a. Is there a plan in place to "gracefully" recover from an unexpected inverter shutdown?
    b. Is SCADA equipment used to automatically restart an inverter that unexpectedly goes offline?
7. Are the logic and control portions of the inverters primarily powered by the AC or DC side of the circuitry?
    a. If the inverter goes offline, will it be able to be restarted remotely?
    b. Presuming the inverter logic and control circuitry are primarily DC powered, do they have any means of disconnecting themselves from the DC power?
    c. Is a separate piece of hardware used to disconnect DC power?
        i. Is this hardware Chinese made?
        ii. Is the hardware remotely controlled? If so, please answer all these questions for the disconnect equipment as well.
8. Are there documented procedures for responding to a potential "kill switch" or network breach event?
9. What would a recovery scenario look like should there be a catastrophic "kill switch" event?
10. What redundancies are in place to ensure uninterrupted power supply in the case of a "kill switch" event?
11. What are your current protocols for firmware updates or patches to inverter software?
12. Do you monitor for unauthorized wireless signals from solar, wind, and battery inverters?
13. How is your utility collaborating with industry peers to share threat intelligence and best practices?
14. If it is identified that some of these suspicious inverters are on your system, what would be the mitigation plan?
    a. Are (or could) the inverters (be) protected by a faraday cage?
    b. Is there an alternate supplier that can be utilized to replace the inverters?

i. Are there supply chain issues involved with acquiring these replacements? Please describe.

Thank you for your attention to this important matter. Recognizing the potential sensitive nature of this information, you may choose to docket a redacted (or abbreviated) copy of your response to this docket, while providing the unredacted or complete responses to ACC Utility Staff. Please provide your responses by June 30, 2025. I look forward to your responses.

Sincerely,

Vice Chairman Nick Myers