

DOCKETED	
Docket Number:	24-OPT-05
Project Title:	Corby Battery Energy Storage System Project
TN #:	272643
Document Title:	Olivia Ramirez Comments - FORMAL OPPOSITION TO CORBY BESS UNMITIGATED CYBERSECURITY, CYBER-PHYSICAL, AND PUBLIC SAFETY RISKS UNDER EXECUTIVE ORDER 14420
Description:	N/A
Filer:	System
Organization:	Olivia Ramirez
Submitter Role:	Public
Submission Date:	9/13/2026 2:23:40 PM
Docketed Date:	9/14/2026

Comment Received From: Olivia Ramirez
Submitted On: 9/13/2026
Docket Number: 24-OPT-05

**FORMAL OPPOSITION TO CORBY BESS UNMITIGATED
CYBERSECURITY, CYBER-PHYSICAL, AND PUBLIC SAFETY
RISKS UNDER EXECUTIVE ORDER 14420**

Additional submitted attachment is included below.

Public Comment on Corby BESS– Severe Unmitigated Cybersecurity and Public Safety Hazards under Executive Order 14420

To: California Energy Commission

From: Olivia Ramirez

I'm writing to express strong opposition to the proposed Corby Battery Energy Storage System (BESS) project. The current project proposal and environmental review fail to evaluate or mitigate critical cyber-vulnerabilities and national security threats explicitly identified in **Executive Order 14420 (*Declaring a National Emergency to Secure the United States Bulk-Power System*, August 26, 2026)**.

Because the Bulk-Power System relies on real-time balance and automated remote management, a compromised Battery Management System (BMS) or power conversion system poses an immediate, unmitigated threat to local public safety, emergency services, and grid stability. I urge the Lead Agency to reject the application or require a revised, recirculated EIR based on the following unaddressed hazards:

1. Inadequate Analysis of Foreign Equipment & Remote Control Risks

EO 14420 prohibits the installation and operation of foreign-produced bulk-power system equipment—specifically software, firmware, and digital remote-access capabilities, supplied by Covered Foreign Entities.

- The environmental documentation fails to provide verification that the project's digital controls are free from backdoors, unauthorized remote access capabilities, or malicious remote action vectors. The EIR must identify all equipment hardware and software vendors and demonstrate full compliance with DOE pre-qualification standards under EO 14420 before any permit is issued.

2. Public Safety Hazards from Cyber-Induced Thermal Runaway or Sabotage

A cyber-breach on a 300 megawatt facility is not merely an IT issue, it is a physical safety hazard. Disabling thermal management software, overriding safety cutoffs, or manipulating cell balance controls remotely can trigger catastrophic thermal runaway, fire, and toxic gas release.

- The EIR's hazard and fire analysis assumes normal operating conditions or localized mechanical failure. It fails to model the impact of a coordinated software-induced shutdown or thermal runaway event caused by remote manipulation of the BMS. The CEC must require a dedicated **Cyber-Physical Hazard Risk Assessment which analyzes** how remote software exploitation could bypass physical fire suppression and safety protocols.
- The EIR must analyze a plume model in which all battery containers were intentionally overheated and put into thermal runaway and analyze risks to adjacent sensitive receptors.

- Can the CEC guarantee that the Corby BESS won't be hacked using cyber hacking or ai infrastructure?
- What prevention measures are included in the EIR to prevent cyber threats and intentional attacks on the Corby BESS?
- If these attacks were to occur how would this impact the nearest neighbors.

Conclusion & Requested Action

Until the developer provides an auditable, federally compliant supply chain and a certified, isolated cyber-architecture, approval of this project places our community's infrastructure and public safety at unacceptable risk. I respectfully request that the Commission deny the project permits or require a comprehensive supplemental EIR addressing these national emergency risks.

Thank you,

Olivia Ramirez
Solano County