



Circular Solar LLC
Cherise Petker
CircularSolar@outlook.com

October 7th, 2026

Subject: Industry Response / Public Comment to DOE CESER Request for Information (RFI) – Securing the United States Bulk-Power System (Executive Order 14421)

To: U.S. Department of Energy (DOE)

Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

Executive Summary: Field-Tested Edge Architecture and the Reality of Foreign-Manufactured Vulnerabilities

This public comment submits empirical research, field-tested hardware configurations, and microgrid architecture data accumulated since 2014 to support the Department of Energy's implementation of Executive Order 14421 ("Declaring a National Emergency to Secure the United States Bulk-Power System").

True protection of the bulk-power system requires addressing the physical and communication vulnerabilities embedded in mass-market, foreign-manufactured inverters, modems, and cloud-dependent components. Independent research, full-time development, and rigorous field validation demonstrate that secure distributed energy resource (DER) management must rely on hardened edge architecture rather than vulnerable cellular or foreign-backed cloud infrastructure.

Led by my research, which began in 2010 after going through an event where I learned of failed equipment causing a disaster. In 2014 after learning of the 2014 SolarWorld Breach, this became a pet project of mine to try to solve potential problems/solutions associated with certain U.S. foreign adversary made equipment. In the whitepaper below I address/respond to the RFI category A: A-1, A-2, A-3 and Category B-6, B-7 and D-3.

In 2022 I realized (possibly proved) one reason why the Biden-Harris-Granholm administration's 2021 suspension of President Trump's executive order restricting foreign bulk-power components was a mistake that possibly prioritized low-cost market deployment over national security. I tried very hard to have the opportunity to address and possibly fix it but these efforts were all essentially blocked; as multiple grant contest submissions were denied, while possibly addressing edge-security and microgrid challenges to increasing recycling of clean energy to

lower its cost of energy with innovative lifecycle innovations, circularity back into clean energy. The research, testing I was doing, based on my surveying some in the industry in 2021-2023 - it was kind of “out there”; EMIs and the connectivity issues from interference. Our initiatives received zero OEM, institutional capital or structural backing but knowing the potential greater danger, I never gave up on it. The research and field test results were somewhat independently supported by the 2025 study *ReThink* about power inverter electromagnetic vulnerabilities with foreign hardware which may also have backdoors and physical-layer sensor vulnerabilities (when made in China, their software, their telemetry etc). Leaving the grid edge exposed to foreign supply chains and vulnerable public communication links invites remote coercion, communication blackouts, and I think possibly electrical fires. Reversing course under Executive Order 14421 by enforcing strict bans on adversarial hardware and mandating localized, foreign-free edge isolation is therefore an urgent, non-negotiable imperative to secure the U.S. bulk-power system.

At this point, I would like to thank the Trump administration for prioritizing safety and national security, again in 2026.

Hardening the Grid Edge: Eliminating Foreign Supply Chain Vulnerabilities, Communication Single Points of Failure, and Cyber-Physical Risks in Distributed Energy and Wind Infrastructure

Author: Cherise Petker, Founder/CEO, CircularSolar.net

Date: October 7th, 2026

Abstract

As the United States and NATO allies accelerate the deployment of Distributed Energy Resources (DERs), solar-BESS farms, and offshore wind powerplants, the attack surface of the bulk-power system has expanded exponentially. Decades of prioritizing low-cost, mass-market foreign hardware—specifically unvetted inverters, chargers, and modems with cloud-tethered dependencies—have left critical energy infrastructure vulnerable to foreign-adversary manipulation, remote cyberattacks, and systemic communication blackouts.

This whitepaper outlines an empirical, field-tested counter-architecture. Drawing from over a decade of continuous research following the 2014 SolarWorld AG cyber espionage event (and then others over the years), our research and findings confirmed in 2022-2023, confirmed at a PG&E Innovation Summit in 2024 and reinforced by independent third-party security validation in 2025 (such as the *ReThink* study on power inverter electromagnetic vulnerabilities), this paper establishes why cloud-first enterprise software and public cellular/satellite backhails fail in real-world grid environments. Furthermore, it presents a ruggedized, localized edge hardware suite (utilizing vetted controllers and uninterruptible, EMI-tolerant local wireless architectures) as the mandatory standard for securing domestic microgrids and offshore wind assets against geopolitical and physical threats.

1. Introduction and Threat Landscape

The transition toward a decentralized energy grid introduces unprecedented orchestration challenges while creating severe national security vulnerabilities. Modern grid management platforms—such as utility Distributed Energy Resource Management Systems (DERMS) deployed on cloud infrastructures—focus heavily on top-down forecasting, market optimization, and capacity management. However, these systems routinely treat the physical grid edge as a black box, assuming that field devices will securely and reliably execute commands. Our website addresses and cites one 2022 DOE report we recommend to be reviewed along with our findings, found at the bottom of this page: <https://circularsolar.net/more-details>

Real-world threat intelligence and peer-reviewed technical findings prove this assumption is fundamentally flawed:

- **2014 SolarWorld AG Breach:** Initiated state-sponsored recognition that renewable energy hardware and intellectual property represent primary targets for foreign economic and cyber espionage.
<https://www.nbclosangeles.com/news/local/west-coast-solar-companys-clash-with-china-pre-date-s-cyber-espionage-indictment/1976130/>
- **The *AcidRain* Cyber Attack on European Wind Fleets:** Russian-backed wiper malware targeted ground-based management systems and Viasat's KA-SAT satellite modems, cutting remote wireless telemetry and connection links for thousands of wind turbines across Europe (including Enercon's fleet in Germany). This incident demonstrated that relying on satellite and cloud-tethered remote links leaves critical generation assets entirely blind and vulnerable to remote coercion.
- **Foreign Supply Chain Infiltration:** Mass-market smart inverters, chargers, and industrial modems imported from adversarial nations frequently contain undocumented communication channels, hidden firmware backdoors, and direct-to-cloud telemetry leaks, bypassing local administrative oversight.

2. The Intentional Threat Model: Software Backdoors vs. Inherent Hardware Vulnerabilities (RFI Category A: A-1, A-2, A-3)

A foundational pillar for restricting foreign-manufactured inverters and modems—particularly those originating from adversarial states like China—involves differentiating between intentional software backdoors and inherent physical vulnerabilities:

A. The Intentional Threat Model (The "Trojan Horse" Concern)

- **The Suspicion:** Policymakers and national security experts who advocate for strict supply-chain restrictions note that connected inverters and smart energy components rely on complex microchips and proprietary firmware that are exceedingly difficult to fully audit.

- **The Risk:** If a foreign manufacturer or state-sponsored actor intended to compromise domestic infrastructure, they could theoretically embed hidden instructions—such as a remote kill-switch or an encrypted backdoor triggered by a specific network packet—directly into the device's code. Because modern smart inverters maintain continuous cloud connectivity for routine monitoring and firmware updates, a malicious update could theoretically be pushed globally or regionally. This would allow an adversary to shut down thousands of distributed energy resources simultaneously, causing rapid frequency collapse and widespread grid destabilization.

B. Inherent Hardware and Sensor Vulnerabilities

In tandem with intentional software backdoors, physical components present inherent design risks. As independently validated by recent security research (e.g., the *ReThink* analysis on power inverter electromagnetic susceptibilities published at NDSS 2025), even mass-market inverters that comply with baseline electromagnetic compatibility standards contain severe physical-layer vulnerabilities. External electromagnetic interference (EMI) or targeted signal injection can manipulate internal voltage and current sensors, tricking internal control algorithms into uncoordinated shutdowns, performance damping, or hardware burnout. Relying on foreign hardware compounds these risks, as supply chains lacking rigorous transparency leave utilities exposed to both malicious code injection and structural hardware vulnerabilities.

3. Empirical Research, Independent Third-Party Validation, and Field-Testing (2014–2025)

To counter these systemic vulnerabilities, our research shifted from theoretical risk analysis to empirical, hardware-level engineering—a trajectory directly backed by parallel real-world developments and academic testing.

A. Threat Prioritization & Elimination of Cloud Dependencies

Recognizing that foreign-manufactured hardware and unvetted cloud servers act as persistent backdoors, our architecture rejects all open internet exposure and foreign supply-chain components. Telemetry is restricted to report-by-exception monitoring, preventing unauthorized inbound remote command-and-control access from the public internet.

B. High-EMI Microgrid Validation (2020) and 2024–2025 Third-Party Inverter Testing

Starting in 2020, a ruggedized microgrid architecture was in research and began to be purpose-built and deployed in severe electromagnetic interference (EMI) environments to test signal integrity and physical resilience. The impact on connectivity and impact on some hardware. Testing explicitly accounted for very heavy rail and train traction interference—forces that generate intense electrical noise capable of jamming standard consumer Wi-Fi bands and dropping public cellular signals. The train track to the test vessel is up to 1,800 feet away but

since the EMIs are severe, are barely blocked by any obstructions so the water preserves the wave's strength that are normally weakened over land.

Over a land environment, that 1,700-foot distance would include natural attenuators:

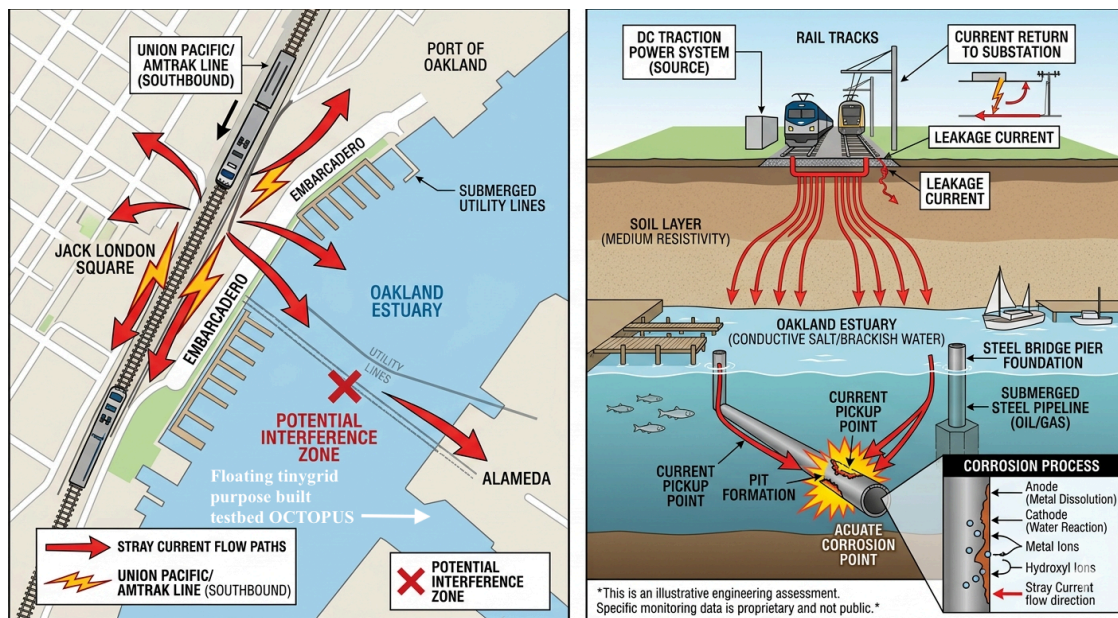
- **Scattering and Absorption:** Trees, brush, terrain variations, and buildings act as physical barriers that scatter and absorb high-frequency RF energy, causing the signal to drop off much faster.
- **Urban/Terrestrial Clutter:** Ground conductivity over soil is often lower, and structural interference breaks up wave fronts. Over open water, several unique factors work together to keep the EMI potent over that distance:
 1. **Zero Obstruction & Low Attenuation:** There are no physical objects to block or absorb the wave front. High-frequency transients travel with minimal loss.
 2. **Water:** acts as a highly reflective, conductive surface. Radio frequency waves bounce off the water and can combine with direct waves (constructive interference), maintaining surprisingly high field strengths at a distance rather than dissipating uniformly.
 3. **Enhanced Coupling to the Microgrid:** Because the microgrid is floating on that same conductive water plane, its long DC and AC cables form an efficient "image antenna" system. The water actually helps couple the electromagnetic energy right into the wiring, making the unshielded inverter more vulnerable than it would be if placed on dry, rocky soil.

Crucially, independent third-party research published across 2024–2025—specifically the comprehensive security analysis on power inverter EMI susceptibility (*ReThink: Reveal the Threat of Electromagnetic Interference on Power Inverters*, accepted at NDSS 2025: <https://arxiv.org/pdf/2409.17873>)—serves as support for our 2022–2023 field findings. The *ReThink* study demonstrated similar problems to our testbed/real-life study that commercial solar and power inverters contain critical physical-layer vulnerabilities where external electromagnetic interference can manipulate internal voltage and current sensors. Even when devices conform to standard baseline compliance, targeted EMI injection tricks internal control loops into uncoordinated shutdowns, power fluctuations, or operational instability.

Our field testing established the real-world operational baseline addressing these exact physical vectors, proving that:

1. **The Failure of Cellular Backhaul:** Public cell tower internet is entirely unreliable for grid-critical operations. During grid disturbances, local emergencies, or network congestion, cellular links drop or experience catastrophic latency.
2. **The Threat of Satellite Vulnerabilities:** As demonstrated in European wind asset attacks, satellite links are acutely vulnerable to cyber-wiping, jamming, and signal disruption.
3. **The Necessity of Localized, EMI-Tolerant Wi-Fi:** Uninterruptible microgrid control requires purpose-built, isolated local wireless frameworks capable of maintaining clean

data transmission through heavy electrical noise without relying on public carrier infrastructure. Rail track to vessel distance is < 1,800 feet but mainly all water.



4. Intersection with Utility Scale: August 2023 Pitchfest, PG&E, Schneider Electric, Microsoft DERMS Integration, and confirmed correct equipment at the 2024 PG&E Innovation Summit (RFI A-2, B-6, B-7)

Our foundational work and field-tested hardware architecture intersected directly with major utility modernization trajectories through formal submissions and high-level industry milestones:

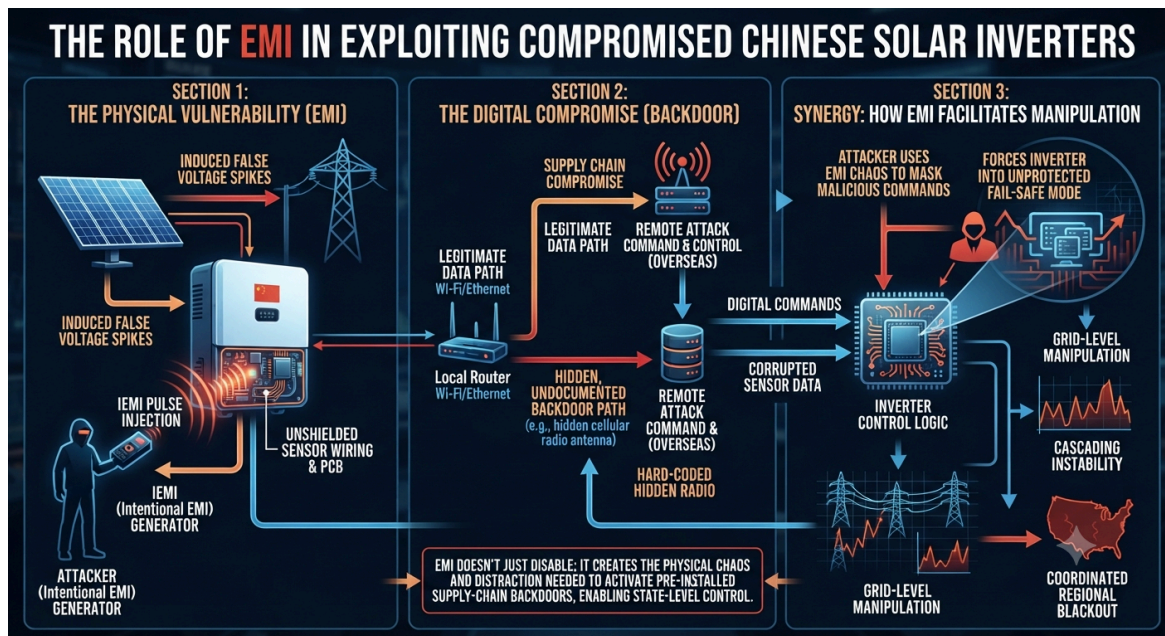
- The August 2023 PG&E Pitchfest Submission & AI Data Center Resilience:** I formally submitted the complete microgrid hardware architecture, solar-BESS designs, and edge control suite to Pacific Gas and Electric Company (PG&E) during their R&D pitch process. This submission detailed specific equipment recommendations engineered to scale into commercial Distributed Energy Resource Management Systems (DERMS) while ensuring strict physical edge resilience for mission-critical loads, including AI data center integration by verifying the problem/solution by EMIs in June 2023.
- Industry Convergence (also in 2023):** Concurrently, major enterprise partnerships were unveiled—such as the announcement between Schneider Electric and Microsoft Azure to deploy a cloud-based DERMS platform designed to maximize EV, solar, and BESS value while accelerating interconnections. While enterprise platforms focus on top-down cloud optimization, our submission exposed the core operational blind spot: *software orchestration is entirely ineffective if the physical edge hardware is unvetted, backdoored, or susceptible to environmental interference.*

- Participation and Solution Validation at the PG&E 2024 Innovation Summit:**
 Cherise directly attended the **PG&E 2024 Innovation Summit** (including the afternoon breakout session titled *"Revealing Grid Flexibility from DERs"*, which featured industry leaders including Schneider Electric). During the session's interactive problem-solving modules, Cherise successfully identified and solved the complex technical hurdles presented in the event's third challenge scenario. Having spent many years in research, already engineered, tested, and submitted these exact equipment solutions to PG&E in August 2023 to the 2023 PG&E Pitchfest. In September they announced the "Schneider Electric and Microsoft Azure to deploy a cloud-based DERMS platform designed to maximize EV, solar, and BESS value while accelerating interconnections" — which I had hope to supply my designs/tests/partnership. We were not chosen in 2023 but I knew the data supported possibly helped solve their problems. So in 2024 I attended the Innovation summit to stand out as uniquely equipped, one of the few or only participants in the audience who had chosen the equipment, as already operationally resolved the exact edge-reliability dilemma utilities were struggling to address. Transcript of the attended event, where we used our phones to blindly insert the answers (to question 3) "realving Grid Flexibility from DERs"

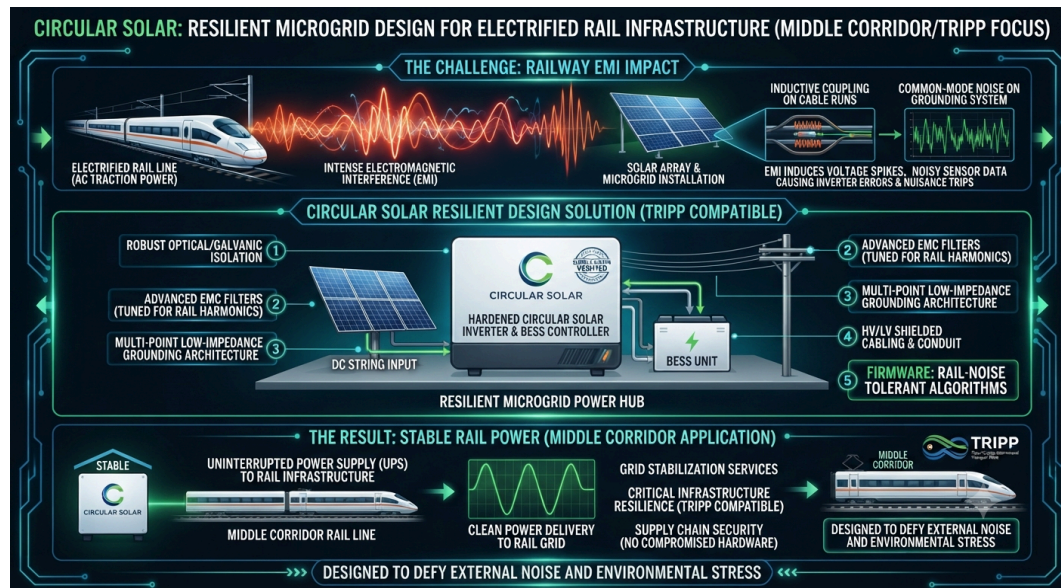
<https://www.pge.com/assets/pge/transcripts/revealing-grid-flexibility.pdf> also transcript from the other event I attended and was called on, "Fast-tracking the EV Future":

<https://www.pge.com/assets/pge/transcripts/fast-tracking-the-ev-future.pdf>

By 2022-2023 I realized, based on research, disruption issues and others installing equipment I specifically did not suggest (Renogy), but they did due to its lower cost, they had problems, then it resolved once they installed the equipment I suggested, pointing to Chinese equipment being the failure point! Rail track to vessel distance is 1,800 feet.



Remote testing: In June 2023, all equipment was installed and verified resilience of the Circular Solar tinygrid on OCTOPUS by severe EMIs/Rail. Later in Türkiye I verified uninterruptible remote monitoring (control). I designed the microgrid and other innovations/products to be resilient, possibly forscale to NATO grids or future microgrids for TRIPP, Central Asia; as we had been years into working on our mining business overseas which would ship, supply-chain via this route, thus our testbed, tests, and CS light for rail safety were to scale into Circular Solar supplying this rail shipping route for our products and of course to be secure and resilient for many other businesses.



5. Securing Offshore and Nearshore Wind Powerplants

The lessons learned from ground-based high-EMI microgrids apply directly to offshore and nearshore wind powerplants. Offshore wind installations face extreme physical isolation, severe maritime weather corridors, and heightened exposure to foreign-adversary interference.

If an offshore wind facility utilizes Chinese or unvetted foreign inverters, chargers, or satellite modems:

- The Remote Interception Risk: Hostile nation-states can exploit hidden firmware backdoors or sensor-level EMI vulnerabilities to manipulate turbine frequency, initiate uncoordinated emergency shutdowns, or inject grid-destabilizing commands.
- The Connectivity Blind Spot: Reliance on cellular links leaves onshore and offshore assets defenseless against localized jamming or wiper malware campaigns.

The Solution: Securing offshore wind requires mandating domestically vetted, edge controllers, such as xxxxxxxxxx paired with isolated, hardened xxxxxxx (equipment list can be made available

to DOE). This ensures operational autonomy, allowing turbines and local BESS arrays to safely manage themselves even if external communication links are completely severed.

Options for decommissioning aging Wind Energy sooner due to the high cost of tear-outs or new concerns associated to foreign made component in Wind farms (or other farms):

Recognizing in 2020 that recycling of EoL Wind turbine blades, nacelles was a demand in need then and would become a major industry in the near future, after making this possible breakthrough in failure points, I ensured to focus on scaling these innovations to the problems associated to the RFI. We already pitched part of our Circular Solar Wind project to mine sites in 2009 - 2012 (to capture the e-waste, copper and REEs, process at the mine site and power the mine site with solar-bess using the composite waste into additional solar energy and Battery storage). These solutions were presented at Wind Europe's annual recycling conference in Portugal last year, EOLis2025. Circular Solar Wind is ready to deploy the in the U.S. or fair trade partner countries: <https://circularsolar.net/cs-wind%2C-recycling%2C-ai>

6. Policy Implications and Recommendations for DOE CESER (Executive Order 14421) (RFI Category B: B-6, B-7)

Despite the proven technical superiority and national security imperatives of this edge-hardened hardware design, independent innovators faced a severe institutional disconnect between 2022 and 2024. Proposals submitted to DOE/NREL-backed HeroX grant contests—including designs for Circular Solar farms integrating recycled and virgin ground-cover materials for increased yields and fireproof barriers—received no capital or structural backing. This oversight stemmed from an over-reliance on top-down cloud models and a failure to enforce strict bans on non-vetted foreign inverters, chargers, and modems—reversing the original protective intent of Executive Order 13920.

To secure the U.S. Bulk-Power System under Executive Order 14421, the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) must implement the following regulatory mandates:

- 1. Ban Adversarial Hardware at the Edge:** Formally prohibit the use of foreign-manufactured inverters, industrial modems, and communication modules from adversarial supply chains in all critical domestic energy assets, land-based microgrids, and offshore wind powerplants.
- 2. Mandate Localized Edge Isolation:** Require that all DER installations utilize hardware-level perimeter isolation, report-by-exception monitoring, and local control logic that cannot be remotely overridden via vulnerable cloud backdoors or sensor-level EMI injection.

3. **Reject Public Cellular and Satellite Dependency for Grid-Critical Control:** Establish strict communication standards ensuring that primary grid control and microgrid telemetry rely on resilient, localized, EMI-tolerant private networks rather than vulnerable public cellular or satellite backhauls.

7. Emerging Safety Risks: High-EMI Environments, Connectivity Drops, and Catastrophic Fire Hazards (RFI Category D-3)

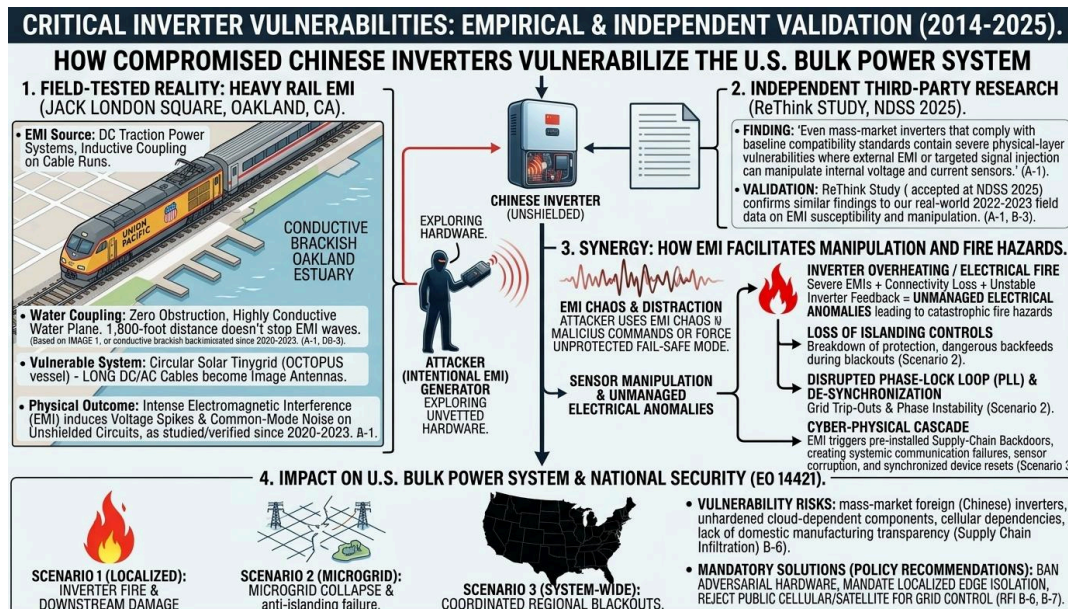
A critical and alarming finding emerging from our decade-long research and field-testing is the intersection of high electromagnetic interference (EMI), sudden drops in remote connectivity, and unmanaged inverter telemetry. When unhardened, cloud-dependent wind, solar and BESS sites that experience severe EMI spikes (such as those studied in high-density infrastructure corridors) combined with cellular or network backhaul dropouts, local inverters may frequently lose closed-loop synchronization with remote management dashboards.

Without autonomous local edge controllers to safely manage state-of-charge, voltage regulation, and thermal thresholds during communication blackouts, these systems face cascading control failures. We hold serious concern that this exact triad—unmitigated high EMIs, sudden loss of remote monitoring/control, and unstable inverter sensor feedback—creates unmanaged electrical anomalies that have directly contributed to catastrophic fire outbreaks across utility-scale and distributed energy sites.

Furthermore, these catastrophic thermal failures and subsequent fires carry compounding environmental hazards: if the deployed wind (PFAS/ fluoropolymer-based paints and final finish coats on towers and blades) or monofacial solar arrays that utilize backsheets containing high concentrations of per- and polyfluoroalkyl substances (PFAS), thermal degradation or combustion can release persistent fluoropolymer toxins, resulting in severe, long-term airborne, soil, and groundwater contamination across surrounding ecosystems.

To address this compounding safety and environmental crisis, we formally submit this whitepaper—alongside our complete microgrid recommendations and a specialized technical version containing non-public intellectual property (IP)—for immediate review and consideration by federal oversight bodies beyond the DOE, including the Department of the Interior (DOI) and land-management agencies tasked with safeguarding public lands, infrastructure corridors, and environmental safety against catastrophic grid-induced fires.

Possible pathway to electrical inverter fire:



Conclusion

True grid reliability and cybersecurity cannot be achieved through software abstractions or paper compliance. Backed by both our empirical field research completed in 2023 and independent 2025 testing (the *ReThink* inverter vulnerability analyses), it is clear that anchoring energy architecture in field-tested, locally controlled, Chinese-free hardware (we did use both American Made and some foreign hardware which is the best on the market; made in a NATO country) is the only path forward to eliminate single points of failure, prevent catastrophic fire risks, and secure the bulk-power system.

Thank you to all parties who read my findings - this is many years of research, trial and error, in hopes of supporting resilience, national security in our grids, be it micro to bulk power.

Cherise Petker

Founder/CEO, CircularSolar.net