

Dear County Auditor and Candidates,

This is an industry notification regarding undue wear on county infrastructure resulting from computational malware operating at scale under the legal cover of blockchain technologies.

The Threat

Malicious software is mimicking legitimate cryptocurrency activity in order to exploit the protections afforded by [Utah HB230 \(2025\)](#), including exemptions from local zoning oversight, noise regulation, and money transmitter licensing audits. The statute was written to protect individual rights in legitimate blockchain participation. It is now functioning as a legal shield for computational malware that consumes public energy infrastructure at scale.

Because blockchain is premised on transparency, it is the obfuscation of physical infrastructure costs that signals something worth examining. These operations cannot hide their physical footprint in county utility data, capital asset depreciation schedules, and grid stress patterns.

The malware exploits Landauer's limit, the thermodynamic principle governing energy dissipation in computation, with the practical effect of overloading energy grids, accelerating infrastructure wear, and displacing costs onto public utilities and taxpayers. There is also regional impacts on water ecosystems such as rivers, lakes, and streams.

Based on blockchain cycle threat modeling and thermodynamic load projections, the next peak stress event on regional energy infrastructure is projected for spring 2028. County infrastructure must be evaluated for exposure now and immediate mitigative actions taken. Market-driven hash rate acceleration, in which cryptocurrency price volatility triggers coordinated mining surges, creates unpredictable and compounding spikes in regional energy demand. At sufficient scale these surges can destabilize the power infrastructure that election systems depend on, making this not only a financial audit concern but a direct threat to election integrity and continuity of county government operations.

[Dr. Rob Davies of Utah State University](#) quantified the data technology attacks and more details on the exploitation method can be read [here](#).

What HB230 Did Not Close

HB230 did not touch county financial governance. County auditors retain full authority over:

1. Public infrastructure costs: utility infrastructure, power hubs, water resources, and cooling systems remain county property and fully auditable.
2. Capital asset depreciation: auditors can examine whether counties are receiving what data center incentive agreements promised versus what public infrastructure is absorbing.
3. Incentive compliance: HB507 (2026) prohibits incentives to large data centers outside a Regionally Significant Development Zone. Auditors can verify compliance.
4. Energy excise tax revenue: counties levying up to 6% on high-impact consumer energy use can audit whether that revenue is being collected and applied correctly.
5. Utility variance as ICFR signal: HB230 never touched Internal Controls Over Financial Reporting. Unexpected utility spikes remain auditable financial anomalies regardless of what caused them.

Questions for County Auditors

As learned during my tenure as Information Security Officer over Digital Assets at a major financial institution, the deepest, most complex cyber risks overlap directly with physical energy architectures and financial line items. To combat the cyber-attacks, county auditors can ask the following. Additionally, requests to NIST—specifically the team over NIST SP 800-239 and local state cybersecurity offices can be engaged for help obtaining thermodynamic analysis at Landauer methodology. Notifications went out to industry beginning in February 2025.

1. Within your ICFR testing, have you established a baseline protocol where unexpected spikes in power grid utility expenditures are flagged as potential cybersecurity indicators? How will your audit team reconcile physical utility data with your county's digital risk posture?
2. Before new data center proposals are financially approved, how will your audit evaluate the risk of accelerated degradation on county-owned infrastructure such as regional power hubs and cooling water resources?

3. Will your audit protocols examine hardware depreciation anomalies as a forensic tool to detect unauthorized or compromised high-entropy workloads running inside county architecture?

Taxpayer Disclosure

Current law does not require counties to notify taxpayers of energy infrastructure attacks. County auditors can fill that gap by supporting a public information campaign alerting residents to nation state social engineering operations recruiting ordinary Utahns into installing parasitic ASIC mining hardware on home and business electrical systems, unknowingly transferring energy costs to themselves and degrading the county grid at public expense.

While phishing training is aimed at prevention, there is very little in the market to undo social engineering once a population has been captured. [Cybersecurity Mindfulness](#) fills that gap.

Closing

County energy infrastructure is absorbing undue and unaccounted tax burden today. Left unaudited, these financial liabilities shift onto unsuspecting taxpayers instead of the technologists and financial firms where they belong. The situation is much like Amazon switching to electric vehicles to bypass the gas tax while continuing to use public roads.

Happy Monday,

January N. Walker

Executive, Planetary Information Security Officer

ORCID: [0009-0000-6843-2051](#)