

To: expartecommunications@hq.doe.gov
From: Finite State
Date: October 14, 2026
Subject: Ex Parte Meeting on Securing the United States Bulk-Power System (Docket No. DOE-HQ-2026-1123; RIN 1901-AB79)

Finite State is providing this memorandum pursuant to the Department of Energy's guidance on ex parte communications (74 Fed. Reg. 52795, Oct. 14, 2009).

On October 8, 2026, at 2:30 p.m. EDT, Finite State met remotely with the Department of Energy (DOE) regarding Executive Order 14421, Declaring a National Emergency to Secure the United States Bulk-Power System, and DOE's related request for information, Securing the United States Bulk-Power System (91 Fed. Reg. 57322, Sept. 9, 2026).

Participants for Finite State were:

Matt Wyckhouse, Founder and Chief Executive Officer
Doc McConnell, Head of Policy and Compliance

Participants for DOE were:

Emily Burdick, Principal Deputy Director, Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
Leslie Pezzullo, Chief Operating Officer, CESER
Hayden Hemphill, CESER
Miriam Karumbo, DOE Contractor

The issues discussed during the meeting are summarized below. Finite State shared a slide presentation during the meeting, a copy of which is attached as Attachment A.

Finite State experience and assessment capabilities

Matt Wyckhouse described Finite State's work with electric utilities on connected-device supply-chain security and with energy and industrial equipment manufacturers on product security during development and after deployment. He described approximately a decade of binary firmware analysis, automated evaluation of vulnerabilities to distinguish meaningful risks from findings that are non-exploitable in context, and services involving device teardowns and deeper testing. He explained that manual analysis and automated findings can inform one another. He also cited Finite State's 2019 analysis of Huawei equipment and prior work developing a software bill of materials for a substation.

Firmware analysis and graduated testing

Doc McConnell recommended grounding grid-security assessments in deep supply-chain and product-security analysis, including firmware actually shipped on equipment. Mr. Wyckhouse explained that obtaining firmware from fielded devices or manufacturers can be difficult, but analysis can reveal embedded communications capabilities, software components, and hardware or suppliers indicated by drivers and other signals embedded in the firmware. Separate supplier information can help evaluate potential exposure to foreign adversary suppliers. He cautioned that scanning cannot, by itself, determine that otherwise unattributed code is from a particular foreign adversary country.

Mr. Wyckhouse stated that useful analysis is possible without source code, while vendor attestations and development-time scans can add evidence. He recommended applying the approach to both installed equipment and new procurement, with broad, scalable screening followed by deeper hardware or destructive testing where warranted. Because the same products may be used at multiple facilities and utilities, he proposed reusing applicable product findings to reduce duplicative assessment.

Protection of deployed equipment

Mr. McConnell recommended translating assessment findings into specific, verified protections for equipment. He said firmware findings should be evaluated alongside the network, surrounding systems, and local controls as part of a multilayer approach. Communications, encryption, and cryptographic protocols are relevant to that assessment. He noted that cellular communications can serve legitimate functions; controls should establish authorized communications and constrain data and destinations appropriately. He also recommended anticipating some compromise and limiting its operational effects and consequences for electricity recipients.

Mr. Wyckhouse said isolated operational-technology networks and existing utility protections can be effective, but embedded device capabilities may bypass them. He used an embedded cellular modem as an illustrative off-network communications path. He said the response should depend on the identified risk and could include additional mitigation, further isolation, or removal and replacement where residual risk exceeds tolerance.

Independent verification under common standards

Mr. McConnell recommended common DOE standards implemented by qualified, certified, independent assessment providers. He said this would give DOE independently developed results in addition to utilities' representations. Mr. Wyckhouse cited Finite State's experience with DOE's Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program and suggested using knowledge from that and similar programs to establish standards for suppliers and independent verification bodies.

Mr. Wyckhouse characterized the assessment challenge as involving tens of thousands of products and millions of devices and recommended private-sector execution with government oversight to expand capacity beyond spot checks. He cited Federal Communications Commission wireless-product testing laboratories and European Union Cyber Resilience Act testing and certification arrangements as possible analogies. He said grid-equipment criticality may require more rigorous supply-chain and security analysis.

Evidence and support throughout the equipment lifecycle

Mr. McConnell recommended maintaining a meaningful chain of security evidence throughout the product lifecycle, beyond procurement-time assurances and paperwork. He said evidence should help utilities make risk-informed decisions and be updated as vulnerabilities emerge, deployment or use changes, and risks evolve. He recommended continuing manufacturer security support, product updates, and communication to customers about changes. Recognizing that operational-technology downtime can interrupt production and service, he emphasized providing enough information for utilities to minimize disruption and maintain electricity delivery.

Phased implementation

Mr. McConnell described four practical implementation steps:

1. Prioritize the most consequential equipment. DOE should define priority equipment in light of the Executive Order's policy objectives and communicate that prioritization to stakeholders.
2. Standardize assessment profiles and testing scope around relevant risks and security concerns.
3. Reuse applicable product findings across facilities and utilities to conserve assessment resources, support a shared understanding, and disseminate changing risk information.
4. Implement protection through appropriate manufacturer configuration, implementation at utilities and power stations, local controls that constrain inappropriate capabilities while preserving intended functions, and recovery after incidents or unexpected events. The approach should meet DOE standards regardless of utility size.

Mr. McConnell also emphasized the needs of smaller utilities that may lack immediate capital to implement changes.

Product and version level whitelisting

Mr. Wyckhouse supported product-level whitelisting and cited the Department of Commerce's connected-vehicle approach as a comparison. He said a single vendor may offer products with different risk characteristics, so qualification should operate at the product level and potentially the product-version level, rather than approve an entire vendor. He described standards, certification, and whitelisting as ways to make implementation more workable and anticipated utility interest in efficient approaches.

DOE remarks and planned written submissions

Emily Burdick explained that DOE was leading implementation of the Executive Order and the related RFI and that the meeting was principally an opportunity to listen to industry feedback. She reminded participants that DOE's ex parte guidance applied and limited DOE's specific responses. She noted that DOE had recently released frequently asked questions and said a link would be shared in the meeting chat.

Ms. Burdick described DOE's ongoing consideration of industry feedback, internal analysis, and risk-based assessment in developing a supply-chain-risk recommendation to the Secretary. She encouraged specificity in Finite State's written comments to help DOE focus potential forthcoming rules. Finite State confirmed its intention to submit a separate detailed RFI response by the October 9, 2026 deadline. Mr. McConnell said Finite State would elaborate its assessment-scope ideas in that response. DOE expressed appreciation for the input and interest in continued engagement.

Attachment A

Presentation from Finite State to the Department of Energy
Re: Executive Order 14421 and Securing the United States Bulk-Power System
October 8, 2026

FINITE STATE

EXECUTIVE ORDER 14421 • DOCKET DOE-HQ-2026-1123

National grid equipment assurance

Finite State recommendations in response to the Department of Energy request for information

Matt Wyckhouse

Founder and CEO

Doc McConnell

Head of Policy and Compliance

October 8, 2026

Product-level **evidence** for grid decisions

We provide product and software supply-chain security software and expert services, including threat modeling and risk management.



Binary analysis

Reconstructs what shipped
firmware contains: components,
services, privileges, and update
paths.



Validated findings

Connects analysis to product
behavior, confirmed weaknesses,
and candidate mitigations.



Ongoing risk management

Supports laboratories,
manufacturers, utilities, and
engineering partners as products
change.

OVERVIEW

Five recommendations for grid assurance

- | | | |
|----|--|---|
| 01 | Require deep supply-chain and product security assessment | Use firmware assessment as the common baseline, with real security findings across supplier tiers and targeted hardware escalation. |
| 02 | Turn findings into verified protections for installed equipment | Assess fielded equipment, verify the local controls operators rely on, and plan for bounded compromise. |
| 03 | Scale verification through standards and qualified providers | Extend CyTRICS with supplier evidence and certified independent testing bodies applying DOE standards. |
| 04 | Make manufacturer evidence support trusted procurement | Maintained evidence, authorized access, timely security fixes, and safe deployment across the product lifecycle. |
| 05 | Phase implementation and support utilities | Prioritize consequential equipment, reuse applicable findings, and help smaller utilities implement protections. |

Firmware assessment as the common baseline

Deep supply-chain analysis

Analyze delivered firmware across supplier tiers, including proprietary code and module firmware. Validate functionality, access paths, and weaknesses.

Targeted deeper testing

Escalate to hands-on hardware, dynamic, or destructive testing when the equipment profile, findings, or unresolved questions require it.

Risk-based decision criteria

Tie findings to the critical function, adversary capability, exposure, deployment concentration, recovery difficulty, and remaining uncertainty.

REQUESTED DOE ACTION

Require substantive software and firmware assessment across supplier tiers, with validated findings, explicit gaps, and defined triggers for deeper hardware testing.

Turn findings into **verified** protections

Assess what is installed

Reuse product and firmware findings across applicable installations, then assess local networks and configurations without removing every unit.

Verify the local controls

Cellular support found in BESS
firmware should prompt a check for an enabled path around the plant firewall.

Plan for bounded compromise

Define the critical function, independent protections, safe state, and trusted recovery. A compromised component cannot contain itself.

REQUESTED DOE ACTION

Enable robust software, firmware, and network assessment of fielded equipment, with required independent review, verified local protections, and targeted laboratory escalation.

Scaling CyTRICS through qualified providers

DOE defines the standards

Set equipment profiles and escalation criteria. National labs support reference methods, quality assurance, and difficult cases.

Suppliers provide evidence

Provide firmware, technical documentation, and test results at every tier. Permit self-attestation for defined lower-risk profiles.

Certified independent bodies

Qualify providers for defined testing scopes. Require independent verification for designated high-consequence equipment.

REQUESTED DOE ACTION

Scale CyTRICS-style evaluations through a common firmware assessment baseline (see **Appendix A**), supplier participation, and certified independent testing bodies, with targeted escalation to deeper testing.

RECOMMENDATION 4 · RFIB-4 TO B-6, D-4, E-1, F-3 TO F-5

Keep manufacturer evidence **current**

Build-specific evidence

Maintain firmware, architecture, and test evidence tied to each build, reusable across procurements and authorized assessors.

Access and timely fixes

Continuing access to assessable firmware; prompt remediation, with security fixes separate from features.

Safe deployment

Review each release for security impact. Scale independent testing to the profile and changes. Utilities control installation.

REQUESTED DOE ACTION

Require maintained evidence, authorized access, timely fixes, and continuing independent review where designated, with expedited assessment for urgent updates and safe deployment.

A practical path to national grid assurance

Prioritize

Consequential equipment and material access paths

Standardize

Assessment profiles and qualified testing scopes

Reuse

Applicable product findings across utilities

Protect

Local controls, safe operation, and recovery

A common assessment baseline

Substantive firmware assessment, with independent verification where required and targeted hardware escalation.

Implementation support

Give smaller utilities usable evidence and engineering support for procurement, mitigation, and updates.

REQUESTED DOE ACTION

Define priority equipment, publish assessment profiles, qualify independent testing bodies, and support utility adoption for new and fielded equipment.

What **every** evidence record should hold

01

Identity and applicability

Model, variants, firmware, configuration, and profile.

02

Coverage and methods

What was examined or excluded, and why deeper testing was or was not needed.

03

Composition and control

Declared and derived inventories; build, signing, and update authority.

04

Functionality and findings

Confirmed flaws, unvalidated indicators, and gaps, tied to builds.

05

Operating conditions

Assumptions, required controls, and local verification.

06

Responsibility and acceptance

Who produced, assessed, reviewed, and accepted it.

07

Maintenance and access

Support period, retest triggers, fixes, and access rights.

08

Interoperable by design

SPDX or CycloneDX inventories, VEX statements, protected exchange.