

Comments of disclose.io

Docket No. DOE-HQ-2026-1123, "Bulk-Power System Executive Order RFI"

Securing the United States Bulk-Power System, 91 FR 57322 (September 9, 2026)

Submitted October 9, 2026, by Casey Ellis, Co-founder, disclose.io

Summary

We support DOE's work to keep compromised equipment out of the bulk-power system. Our comments focus on one part of the problem the RFI asks about: making sure that vulnerabilities in this equipment, whether found by vendors, asset owners or independent researchers, are reported and fixed. We have five recommendations.

1. Make a published vulnerability disclosure program a baseline condition for prequalification under Section 2(e) of Executive Order 14421 and for mitigation agreements under Section 2(c). (B-6(a), B-7(a), H-3, F-4, G-6)
2. Tie how quickly a vulnerability is handled, and who is responsible for handling it, to the consequences of compromising the equipment it affects. (C-1, A-6, B-7(a), B-7(e))
3. Treat the legal regime that governs a vendor's vulnerability handling as a supply chain risk factor in its own right. (A-5(b), B-7(a), C-2)
4. Confirm, through a general or categorical license under Sections 2(d) and 3(b) or in the implementing rules, that good-faith security research and independent testing of covered equipment remain lawful. (H-2, A-6, D-4, B-7(e))
5. Require prequalified vendors to publish hashes of their firmware images and keep older images available to asset owners. (B-5, D-1)

About us (A-1)

disclose.io is a nonprofit focused on standardizing vulnerability disclosure and protecting the people who report vulnerabilities in good faith. We maintain a public directory of more than 27,000 vulnerability disclosure policies and security contacts, along with free, open-source safe harbor terms and policy templates that organizations use to stand up their own programs. Our co-founder, Casey Ellis, founded Bugcrowd in 2012 and has spent the years since working between independent security researchers and the organizations that receive their findings.

Disclosure: Casey Ellis founded Bugcrowd, a commercial crowdsourced security company, and remains a shareholder. He no longer holds an operating role there. These comments are submitted on behalf of disclose.io, not Bugcrowd.

We are not an asset owner, manufacturer or vendor of bulk-power system equipment. Our perspective is the path a vulnerability report takes from the person who finds a flaw to the person who can fix it, and the things that stop it from getting there.

1. A published vulnerability disclosure program as a prequalification and mitigation baseline (B-6(a), B-7(a), H-3, F-4, G-6)

B-6(a) lists vulnerability disclosure among the software and firmware security practices DOE asks about, and B-7(a) asks how vulnerabilities reported by researchers and other external parties are received, validated, prioritized, remediated and communicated. Practice across grid equipment vendors is uneven. Some run mature product security teams. Others publish no clear route for an outside researcher to report a flaw, and offer no assurance that the person reporting it will not face legal threats for doing so. A report that never gets made never gets fixed.

The building blocks to address this already exist, and most of them are familiar to the sector:

- **NERC CIP-013, Part 1.2.4** already requires Responsible Entities' supply chain cyber security risk management plans for high and medium impact BES Cyber Systems to include procurement processes that address "disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity." Today that obligation sits with the utility and reaches the vendor only through contract terms. We recommend DOE extend it upstream to the vendor directly.
- **CISA Binding Operational Directive 20-01** (September 2020) required federal civilian agencies to publish vulnerability disclosure policies. The **IoT Cybersecurity Improvement Act of 2020** directed NIST to issue disclosure guidelines that cover contractors supplying information systems and IoT devices to federal agencies, which NIST published as **SP 800-216** in May 2023.
- **ISO/IEC 29147** (vulnerability disclosure) and **ISO/IEC 30111** (vulnerability handling) give an established international baseline DOE can reference instead of writing a new one (H-3). **RFC 9116** (security.txt) gives a standard, machine-readable way to publish a security contact.

We suggest that a vendor seeking prequalification under Section 2(e), or a mitigation agreement under Section 2(c), be able to show that it:

- **(a)** publishes a vulnerability disclosure policy covering the products in question, consistent with ISO/IEC 29147 and 30111 or with NIST SP 800-216;
- **(b)** publishes a working security contact, preferably using RFC 9116;
- **(c)** commits not to pursue legal action against researchers who report in good faith and follow the policy. This commitment should be limited to testing of equipment the researcher owns or is authorized to test, and should never extend to probing live operational systems without the operator's authorization;
- **(d)** commits to coordinate vulnerabilities affecting U.S. bulk-power system equipment with a U.S. coordinator DOE designates, such as DOE (through CESER) as the energy Sector Risk Management Agency, CISA, or both; and
- **(e)** can show the program works in practice, for example through response times and the number of reports received and remediated.

The same criteria could be carried into the FAR revisions DOE must recommend under Section 4(a), and into the waiver and exception criteria F-4 asks about.

On burden (G-6): a basic program is inexpensive to stand up. NIST SP 800-216, CISA's VDP template and disclose.io's open-source policy terms are all free. Accepting alignment with NIST SP 800-216 as an alternative to the ISO standards would give smaller vendors a simple, no-cost route to meeting the baseline. For a small vendor the real cost is staff time to respond to reports, which is capacity a vendor of bulk-power system equipment should have regardless.

We see this as working alongside the origin-based determinations in the order. A working disclosure program is one of the few supply chain controls DOE can verify from the outside, which makes it a useful prequalification criterion.

2. Tie disclosure handling to consequence (C-1, A-6, B-7(a), B-7(e))

Not every vulnerability report carries the same weight. A flaw in a protection relay, a control system used for restoration or blackstart, or equipment serving a defense-critical load has very different consequences from a flaw in a vendor's customer web portal. Today, how urgently a report is handled depends largely on the vendor's own triage, often guided by a CVSS score. The CVSS base score measures the technical severity of a vulnerability, not the consequence of exploiting it in a particular deployment, so it cannot tell a vendor that one of its products sits at the center of a regional grid.

DOE is already asking, under C-1, how to evaluate the consequence and system criticality of covered equipment, and under A-6, which equipment classes to prioritize for early implementation. We recommend DOE use the consequence criteria it develops in response to those questions to set expectations for vulnerability handling as well. For equipment DOE places in the highest-consequence category, a prequalified vendor, or a vendor operating under a mitigation agreement, should:

- **(a)** notify the U.S. coordinator described in Recommendation 1(d) and affected asset owners within a short, defined period after receiving a credible report, sharing any details that could aid exploitation only through protected channels;
- **(b)** set remediation or mitigation timelines that reflect the consequences of compromising the affected equipment, not severity scores alone; and
- **(c)** maintain a named point of responsibility for those reports, with authority to act on them.

Responsibility should also be clear on the other side. The vendor owns the fix. The asset owner owns the deployed mitigation, and should have the information needed to put one in place before a fix ships. DOE, as the energy Sector Risk Management Agency, should lead coordination with CISA when a vulnerability affects several vendors or asset owners, or when a vendor does not respond. A researcher who finds a flaw in high-consequence equipment should know where to escalate it if the vendor goes quiet, and DOE should state that route publicly, whether it is CISA's existing coordinated vulnerability disclosure process, a DOE channel, or both.

This is the same consequence-first thinking behind DOE's National Cyber-Informed Engineering Strategy and Idaho National Laboratory's Consequence-driven Cyber-informed Engineering methodology, applied to the point where a vulnerability first becomes known.

3. Vulnerability-handling jurisdiction is a supply chain risk factor (A-5(b), B-7(a), C-2)

A-5(b) asks what facts DOE should consider when deciding whether software, firmware or services were "designed, developed, manufactured, or supplied" by persons subject to the jurisdiction or direction of a Covered Foreign Entity. We suggest DOE include where a vendor's vulnerability intake and triage take place, and which country's law governs it.

China's Regulations on the Management of Network Product Security Vulnerabilities, issued by MIIT, CAC and MPS and in force since September 1, 2021, require network product providers in China to report information on vulnerabilities in their products to MIIT's Cybersecurity Threat and Vulnerability Information Sharing Platform within two days of discovering or learning of them. Separately, the rules bar organizations and individuals in China that discover or collect vulnerabilities, and publish them, from providing undisclosed vulnerability information to overseas organizations or individuals other than the product's provider. A vendor bound by those rules that receives a report from a U.S. researcher or utility is legally obliged to report it to a government ministry, potentially before a fix reaches U.S. customers. We are not alleging that any particular vendor has misused vulnerability information. The obligation exists in law, and DOE's evaluation of technical and supply chain risk under C-2 should treat it as relevant evidence.

A published disclosure program does not resolve this on its own, since several vendors subject to these rules operate one. Recommendation 1(d) offers a practical test: a vendor that cannot commit to coordinating vulnerabilities affecting U.S. bulk-power system equipment with a U.S. coordinator, before or alongside any reporting to a foreign government, is showing DOE the kind of jurisdictional risk the order is concerned with.

4. Keep good-faith security research and independent testing lawful (H-2, A-6, D-4, B-7(e))

Section 2(a) prohibits "any acquisition, importation, transfer, or installation" of covered equipment "by any person," and Section 5(f) defines a person to include an individual. Once DOE makes a determination covering an equipment class, the text could be read to reach a university lab, an independent testing firm, or an individual researcher buying or importing a single unit in order to take it apart. We do not believe that is the intent, and we ask DOE to say so in the implementing rules.

Much of what the order is concerned about has come to light through independent testing. In May 2025, Reuters reported, citing people familiar with the matter, that U.S. experts who dismantle grid-connected equipment had found undocumented communication components in some Chinese-made solar inverters and batteries. DOE's own CyTRICS program tests energy-sector components at the national laboratories, but it works through voluntary partnerships with manufacturers and

asset owners. The vendors DOE should be most concerned about are the least likely to partner, so independent acquisition of their products is often the only way anyone outside the vendor gets to examine them.

We recommend that DOE, using the licensing authority in Sections 2(d) and 3(b), issue a general or categorical license, or address it in the implementing rules, covering the acquisition, importation and transfer of covered equipment for good-faith security research, academic research, independent laboratory testing (including CyTRICS partners) and conformity assessment, provided the equipment is not connected to the bulk-power system and the holder keeps basic records of what it acquired and where it is held. DOE would not need to define "good-faith security research" from scratch: the Copyright Office's security research exemption under 17 U.S.C. 1201 (37 CFR 201.40) and the Department of Justice's May 2022 charging policy for the Computer Fraud and Abuse Act both already define it.

For existing equipment under Section 2(b), we also ask that any conditions on "servicing" or "updating" not prevent asset owners from commissioning independent testing of their own installed equipment or spare units, including firmware extraction and analysis. Independent assessment is one of the verification methods D-4 asks about, and it only works if it is permitted.

5. Firmware provenance (B-5, D-1)

D-1 asks which data fields asset owners and operators currently maintain. Firmware version is commonly recorded; the firmware image itself usually is not, and vendors often remove older images from their support sites once a newer release ships. That makes it hard, after the fact, to verify what was actually installed or to compare a fielded unit against what the vendor distributed. We suggest that prequalified vendors publish a cryptographic hash for every firmware and software image they release for covered equipment, keep historical images available to asset owners for the supported life of the product, and provide hardware and software bills of materials on request, with hardware bills of materials consistent with CISA's 2023 Hardware Bill of Materials framework.

Contact

Thank you for the opportunity to comment. We can provide more detail on any of these points, or on how disclosure programs operate in practice, at casey@disclose.io.

Casey Ellis

Co-founder, disclose.io