June 9, 2026

Charlie Mlcek
Legislative Assistant
Office of Representative Bob Latta (OH-05)
U.S. House of Representatives
Washington, DC 20515

Sent via electronic mail

Re: Comments on the Working Draft of the SHARE AI Act

Dear Charlie:

Thank you for sharing the working draft of the Safe Harbor for AI Risk Exchange, Analysis, and Information-Sharing Act (SHARE AI Act) and for inviting the Large Public Power Council (LPPC) to comment. We appreciate the office's engagement with us on this legislation.

LPPC supports reauthorizing the Cybersecurity Information Sharing Act of 2015 (CISA 2015), which our members rely on as critical-infrastructure operators and information-sharing participants, and which is set to expire on September 30, 2026. We are glad to see the draft carry a long-term extension of that authority. Because public power's stake in this legislation lies chiefly in how it affects the information-sharing framework our members use, our comments focus on the information-sharing provisions and their workability for electric utilities.

LPPC is a national organization comprising 29 of the nation's largest public power systems (the Members) and over 80 percent of the assets of public power utilities nationwide. LPPC's Members are locally owned and governed not-for-profit electric utilities committed to the people and communities they serve. From New York to California and Washington State to Florida, LPPC Members provide reliable, low-cost electric service to 30.5 million people and represent a cross-section of the nation's utility industry, owning and operating 45,000 circuit miles of high voltage transmission lines and 80,000 megawatts of electric generation capacity.

Preserve the draft's voluntary character with an Act-wide rule of construction

The draft frames AI security submissions as voluntary, and new Section 106(c)(3) confirms that operating an AI defensive measure creates no duty to do so. That no-duty language, however, is scoped only to the defensive-measure liability provision. To avoid any argument that the Act as a whole creates a new mandatory reporting obligation, a duty to monitor or test, or a new standard of care, we suggest a single Act-wide rule of construction making the voluntary character explicit across all of the new AI provisions. Placing it Act-wide, rather than within

Section 104A, ensures it reaches the liability, antitrust, submission, and definitional provisions as well. Suggested language appears in the appendix.

Confirm confidentiality and limited-dissemination procedures in the implementation guidance

The draft protects sensitive submissions well, exempting them from disclosure and authorizing the Secretary to limit dissemination of sensitive technical, operational, proprietary, or security-sensitive details (Section 7, new Section 105(c)(5)(D)). We suggest a modest addition to the implementation-guidance contents in Section 6(d)(3)(C), directing that the guidance address confidentiality protections and limited-dissemination procedures. Suggested language appears in the appendix.

Consult critical-infrastructure owners and operators during implementation

The draft directs the Department of Homeland Security to stand up an interim submission process within 30 days and to update procedures within 180 days, in consultation with Federal entities and, as appropriate, the National Institute of Standards and Technology. It does not provide for consultation with the critical-infrastructure owners and operators who will actually use the channel. Utilities and other operators have a direct interest in whether the process is secure, practicable, and protective of sensitive information. We suggest adding a consultation requirement, framed at the level of critical-infrastructure owners and operators generally to remain consistent with the draft's sector-neutral construction. Suggested language appears in the appendix.

Clarify the consent requirement and the treatment of licensed AI systems

The liability condition in new Section 106(c)(1)(D) withholds protection for a defensive measure applied to an AI model or system "not owned by" the operating entity absent consent, but it requires that consent from "a non-Federal entity... authorized to provide such consent" without stating that the consenting party is the owner, and it is not clear how ownership applies to an AI system a utility licenses and runs on its own information system. We read new Section 104A(c)(3) to permit non-federal entities to employ without exposure to legal liability AI defensive measures on systems they own or operate, and to call for permission only with respect to the modification of systems they do not own or operate. To remove any doubt, we suggest two clarifications. First, that the required consent comes from the owners of the affected models, systems, or information that the entity employing AI defensive measures does not own (versus the current draft's non-specific reference to consent by a "non-federal entity"). Second, that the provision be modified to clarify that entities operating AI and other systems against which AI defensive measures are applied are deemed to be the "owners" of such systems. This clarification reasonably ensures that utilities can protect themselves vis-à-vis AI systems operating within their networks. Suggested language appears in the appendix.

A clarifying question

The defensive-measure framework authorizes a non-Federal entity to operate a measure, and treats a Federal entity as a consent-giver, but does not authorize a Federal entity to operate a

measure itself. This tracks CISA 2015's existing design and may be deliberate, on the understanding that federal agencies act under separate authorities. We raise it because several federal entities operate grid assets directly and contend with these risks, including the Power Marketing Administrations, from which a number of LPPC members obtain power. We would welcome the Committee's view on whether such federal grid operators are adequately addressed, here or under their existing authorities.

CISA 2015 reauthorization

The draft reauthorizes CISA through 2035, and apart from that extension it appears to leave the base statute's core provisions in place. LPPC raises two refinements to the base statute.

First, the channels eligible for liability protection should be expanded. Under Section 106(b), sharing a cyber threat indicator with the Federal Government receives liability protection only when shared through the Department of Homeland Security capability and process established under Section 105(c)(1)(B). In practice, however, an entity responding to an active incident often shares directly with a Federal investigative agency, such as the Federal Bureau of Investigation or the Secret Service, rather than through that channel. As written, such sharing may fall outside the express protection, leaving the entity exposed to a claim, for example by a vendor alleging unauthorized disclosure of a product flaw, even though the disclosure was made in good faith to the government. LPPC recommends extending the same protection to good-faith sharing with Federal investigative and sector regulatory agencies and with sector Information Sharing and Analysis Centers, so that the protection follows the realities of incident response rather than a single channel. Suggested language appears in the appendix.

Second, the Act should preempt private contractual restrictions on good-faith sharing. CISA 2015 shields good-faith sharing from civil liability, but it does not address private agreements that penalize disclosure. A vendor can use a nondisclosure agreement or master service agreement to claim that an entity reporting a threat or vulnerability breached its contract, then rely on that claim to terminate the agreement or seek damages. For public power utilities, which often depend on a small number of critical vendors, that exposure is a real deterrent to reporting precisely the security risks the Act is meant to surface. LPPC recommends a provision making any contractual term unenforceable, as a matter of public policy, to the extent it restricts good-faith sharing for a security purpose under the Act, while leaving the rest of the agreement intact. We recognize that such a provision should be drawn narrowly to respect settled contract-law principles, and we would welcome working with the Committee on language calibrated to that end. Suggested language appears in the appendix.

We appreciate the opportunity to comment and would welcome the chance to meet to discuss any of the above. Please feel free to contact either me or LPPC's Senior Director of Policy, Sarah Vilms (sarah@lppc.org) at your convenience.

Sincerely,

Tom Falcone
President

Appendix: Suggested Redlines

Redlines are shown against the working draft. Deleted text is shown with strikethrough; added text is shown in bold. Citations are to the bill's sections and to the Cybersecurity Information Sharing Act of 2015 as it would be amended.

1. Act-wide rule of construction preserving voluntary character

Where: New section, placed to govern the Act as a whole.

> **SEC. __. RULE OF CONSTRUCTION. In addition to any other rule of construction in this Act, nothing in this Act, or in any amendment made by this Act, shall be construed to require a non-Federal entity to monitor for, evaluate, share, or report an artificial intelligence security indicator, artificial intelligence defensive measure, artificial intelligence security risk, or artificial intelligence adverse action; to create a new mandatory reporting obligation; to create a duty to warn or act; to establish, modify, or expand any standard of care or basis for liability under Federal, State, tribal, or local law; or to condition eligibility for any authorization or protection under this title on a non-Federal entity's participation in any voluntary submission or information-sharing process.**

2. Confidentiality protections in implementation guidance

Where: Section 6(d)(3)(C).

> (C) privacy and civil liberties protections**, confidentiality protections, and limited-dissemination procedures,** applicable to the receipt, retention, use, and dissemination by Federal entities of such indicators, measures, and information;

3. Consultation with critical-infrastructure owners and operators

Where: Section 6(d)(3), new subparagraph.

> **(F) procedures developed in consultation with owners and operators of critical infrastructure to ensure that submission, routing, dissemination, and feedback mechanisms are secure, practicable, and protective of sensitive information.**

4. Consent from owner; treatment of licensed AI systems run on an entity's own system

Where: New Section 106(c)(1)(D).

First, clarify that the required consent comes from the owner:

> (D) in the case of a measure applied to an artificial intelligence model or system, information system, or information not owned by the non-Federal entity operating the measure, such non-Federal entity has obtained authorization and written consent from **the owner of such model, system, information system, or information** ~~a non-Federal entity~~, or ~~from~~ an authorized representative of a Federal entity, authorized to provide such consent;

Where: A clarifying rule of construction in new Section 104A(c)(3) applicable to Sections 106(c)(1)(D) and 106(c)(2)(D).

Second, confirm that a licensee running an AI system on its own information system is treated as the owner for this purpose:

> **For purposes of section 106(c)(1)(D) and section 106(c)(2)(D), a non-Federal entity that operates or runs an artificial intelligence model or system on an information system it owns or controls, including under a license or other right of use, shall be treated as the owner of such model or system with respect to a defensive measure applied to that model or system, or to information associated with it, on such information system.**

5. Expand channels eligible for liability protection

Where: Section 106(b)(2) of CISA 2015 (6 U.S.C. 1505(b)(2)).

> (2) in a case in which a cyber threat indicator or defensive measure is shared with the Federal Government, the cyber threat indicator or defensive measure is shared **in a manner that is consistent with section 105(c)(1)(B), or with a Federal investigative or law enforcement agency, a Federal regulatory agency with responsibility for the security of the affected entity or sector, or an Information Sharing and Analysis Center or Organization,** ~~in a manner that is consistent with section 105(c)(1)(B)~~ and the sharing or receipt, as the case may be, occurs after the earlier of—

6. Contract preemption for good-faith sharing

Where: New subsection in CISA 2015 (Section 106 or 104).

> **(__) CONTRACTUAL RESTRICTIONS.—Any provision of a contract or agreement, including a nondisclosure agreement, terms of service, or vendor or service agreement, that purports to restrict, penalize, or prohibit a non-Federal entity from sharing a cyber threat indicator or defensive measure in good faith for a cybersecurity purpose in accordance with this subchapter shall be unenforceable as to such sharing and void as a matter of public policy. Nothing in this subsection shall be construed to affect the enforceability of such a provision for any purpose other than such good-faith sharing.**