The Electric Power Sector Supports
S. 754, the Cybersecurity Information Sharing Act (CISA)
And Opposes Weakening Amendments

The electric power sector is committed to protecting the nation's electric grid from cyber threats and to enhancing its cyber defenses. The North American power grid is a complex, interconnected network of electric generation, transmission, distribution, and communications technologies that can be damaged by natural events, such as severe storms, as well as by malicious events, such as cyber and physical attacks.

Enactment of cybersecurity information sharing and liability protection legislation is needed to further enhance and incentivize communication among the federal government, the power sector, and other critical infrastructure sectors, which in turn will improve our ability to defend against cyber attacks.

While the electric power sector already engages in significant information sharing activities and has in place mandatory and enforceable reliability and cybersecurity standards, there remains a great need for the government and industry to better share actionable security information in a timely and confidential manner. Bipartisan legislation such as **S. 754*, the Cybersecurity Information Sharing Act (CISA),*** would provide a framework necessary to foster even more meaningful information sharing while maintaining the proper balance between liability and privacy protections.

The electric sector encourages passage of S. 754 and opposes amendments that would significantly undermine the information sharing incentives and legal protections in the bill or unnecessarily complicate information sharing efforts. Two amendments are of particular concern:

- **Leahy amendment #2587**, which would eliminate from the bill any references to express Freedom of Information Act (FOIA) protections when sharing cyber threat indicators (CTIs) and defensive measures (DMs) with the federal government pursuant to CISA. The Burr-Feinstein managers' amendment already would delete a *new* FOIA exemption that would have been created by the bill. The Leahy amendment would go even farther, eliminating from the bill all specific references to FOIA protections. Protection against public disclosure of cyber threat information shared with the federal government is an essential private sector incentive in CISA. Eliminating all specific references to FOIA protections from the bill would have a chilling effect on voluntary information sharing, undermining public-private security partnership efforts and thus potentially making critical infrastructure more vulnerable to cyber attacks. Further, Leahy would remove any protection against disclosure under state, local, and tribal laws.

- **Franken amendment #2612**, which would narrow the definitions of "cybersecurity threat" and "cyber threat indicator" in the bill in a way that would likely result in more litigation, thus creating another legal disincentive to voluntary information sharing, contrary to the fundamental purpose of the legislation.

Other amendments also raise concerns:

- **Heller amendment #2548**, which would impose a more subjective "reasonably believe" test for private entity "scrubbing" of personal information before sharing of information can occur.
- **Coons amendment #2552**, which would require a second "scrubbing" of personal information by Department of Homeland Security (DHS), slowing down the sharing of information in a timely manner.
- **Flake amendment #2582**, which would add a six-year sunset of authorizations and safeguards provided in the bill. Early termination of the program creates uncertainty and will negatively impact participation.
- **Wyden amendment #2621**, which would create a new standard for required scrubbing of personal information when private entities share information with government, giving rise to legal ambiguity and creating a disincentive to sharing information.

The electric sector takes very seriously its responsibility to maintain the reliability, safety, and security of the electric grid. Beyond mandatory standards, the industry employs a "defense-in-depth" mitigation strategy against cyber and physical threats that combines preparation, prevention, resiliency, and response and recovery efforts. We also work closely with the federal government and other critical infrastructure sectors on which the electric sector depends through the Electric Subsector Coordinating Council, and share electric sector threat information through the Electric Sector Information Sharing and Analysis Center. Passage of CISA—without weakening amendments—will enhance these activities.

Senators should support CISA and oppose amendments that would weaken the clarity and effectiveness of the information sharing incentives in the bill.

American Public Power Association (APPA)
Edison Electric Institute (EEI)
Canadian Electricity Association (CEA)
Electric Power Supply Association (EPSA)
GridWise Alliance
Large Public Power Council (LPPC)
National Association of Regulatory Utility Commissioners (NARUC)
National Rural Electric Cooperative Association (NRECA)
Transmission Access Policy Study Group (TAPS)