BRETT GUTHRIE, KENTUCKY
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED NINETEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-3641
Minority (202) 225-2927

March 9, 2026

Mr. Scott I. Aaronson
Senior Vice President, Energy Security and Industry Operations
Edison Electric Institute
701 Pennsylvania Avenue NW
Suite 400
Washington, DC 20004

Dear Mr. Aaronson:

Thank you for agreeing to testify at the Subcommittee on Energy hearing on Tuesday, January 13, 2026, at 10:15 a.m. in 2123 Rayburn House Office Building. The hearing is entitled "Protecting America's Energy Infrastructure in Today's Cyber and Physical Threat Landscape."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Wednesday, November 12, 2025. Your responses should be mailed to Seth Ricketts Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed to Seth.Ricketts@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Energy

cc: Kathy Castor, Ranking Member, Subcommittee on Energy

Attachment

Additional Questions for the Record

The Honorable Bob Latta (R-OH)

1. The Infrastructure Investment and Jobs Act (IIJA) included the Cyber Sense Act and Enhancing Grid Security through Public Private Partnerships Act, both of which I had championed in previous Congressional sessions. These bills sought to improve cybersecurity equipment testing and leverage expertise of government agencies through public private partnerships.

    a. Can you discuss how these provisions have assisted cybersecurity protection since the implementation through IIJA?

The Honorable Brett Guthrie (R-KY)

1. DOE is the energy sector authority and must work with other agencies and States. To do this effectively, it must have a culture of constant learning and improvement, which will benefit the whole federal approach to support the energy sector.

    a. Would you speak to the importance of a culture of constant learning and constant improvement for the stakeholders you represent?

The Honorable Rick Allen (R-GA)

1. The Savannah River National Lab (SRNL) is adjacent to my district. As I mentioned in the first panel, national labs play a critical role in grid security.

    a. How can national labs be leveraged to use their trained cyber operators to enhance security operating technologies?

The Honorable Mariannette Miller-Meeks (R-IA)

1. Congress passed significant cybersecurity provisions in the Infrastructure Investment and Jobs Act, including the authorization for ETAC and RMUC. Your member companies have been working with these programs for several years now. From the investor-owned utility perspective:

    a. Have the IIJA cyber provisions fulfilled the needs of the electricity sector, or do gaps remain?

    b. What additional authorities, resources, or programs would strengthen your members' ability to defend against sophisticated nation-state adversaries?

    c. Are there specific areas where you've seen the most value from federal partnership, and areas where more work is needed?

2. Iowa State University is leading CyDERMS, a regional cybersecurity center focused on securing Distributed Energy Resources. As we integrate millions of new devices we're dramatically expanding the attack surface of our grid. At the same time, we're deploying AI and machine learning tools to detect attacks and manage these distributed systems. This creates a paradox: we're using high-tech AI solutions to secure increasingly complex systems, but that technology itself could be a vulnerability.

    a. How do you think about this balance?

    b. Are there certain applications where simpler, lower-tech approaches might actually be more secure?

    c. How do we ensure that the AI tools we're deploying to defend the grid don't become the vector for attack?