United States House of Representatives Committee on Energy and Commerce
Subcommittee on Energy
January 13, 2026 Hearing: Protecting America's Energy Infrastructure in Today's Cyber and Physical Threat Landscape
Questions for Alex Fitzsimmons, Director
Office of Cybersecurity, Energy Security, and Emergency Response

QUESTIONS FROM CHAIRMAN BOB LATTA

Q1. When I asked you about the timeliness of information sharing by smaller utilities as it relates to threats to the system, you confirmed that the information sharing was timely, but that 'there is more we can do in that department.' As a fundamental part of CESERS mission, how can you further enhance information sharing between your office and the private sector, and vise versa.

A1. The Department of Energy's (DOE) Office of Cybersecurity, Energy Security and Emergency Response (CESER) has numerous information sharing activities with the energy sector to provide information about threats, potential threats, and ongoing incidents.

CESER recognizes that utilities, especially smaller ones, have varying degrees of operational maturity, and we work constantly to improve and tailor this information to be most useful across a wide range of owners and operators. For smaller utilities, this may mean including additional 'how to remediate' guidance when sharing threat information.

CESER's Analysis of Risks in the Energy Sector (ARES) Reports provide DOE a mechanism to distribute key cyber and/or physical threat information, derived from DOE's energy sector subject matter expertise, with input from DOE's Office of Intelligence and Counterintelligence and the National Labs. ARES reports are meant to provide unique information about threats and mitigations for energy sector partners.

The Cybersecurity Risk Information Sharing Program, and its associated information sharing pilots it comprises, is a public-private partnership between DOE and the Electricity Information Sharing and Analysis Center that delivers relevant and actionable cybersecurity information to participants from United States electricity industry.

CESER regularly provides classified and unclassified threat briefings to industry partners. This includes threat briefings during meetings of the Sector Coordinating Council(s), regular meetings with the energy sector Information Sharing and Analysis Centers, and topic specific meetings as needed.

The Energy Threat Analysis Center has also established a collaborative environment where government and industry work together to analyze threats and create timely, actionable guidance for the energy sector.

Finally, CESER recognizes that its information sharing can always become faster and more actionable for our private sector partners. These guiding principles are evidence of CESER's ongoing commitment to excellence.

United States House of Representatives Committee on Energy and Commerce
Subcommittee on Energy
January 13, 2026 Hearing: Protecting America's Energy Infrastructure in Today's Cyber and Physical Threat Landscape
Questions for Alex Fitzsimmons, Director
Office of Cybersecurity, Energy Security, and Emergency Response

QUESTIONS FROM REPRESENTATIVE BRETT GUTHRIE

Q1. A culture of constant improvement is important for DOE, energy stakeholders, and their mutual work to safeguard the energy sector.

Q1A. All the bills today reflect measures that would support constant improvement, as a general principle. Will these be useful to strengthening the Department's energy sector responsibilities?

A1. The Department of Energy is actively reviewing the bills and appreciates the opportunity to work with Congress on the details.

United States House of Representatives Committee on Energy and Commerce
Subcommittee on Energy
January 13, 2026 Hearing: Protecting America's Energy Infrastructure in Today's Cyber and Physical Threat Landscape
Questions for Alex Fitzsimmons, Director
Office of Cybersecurity, Energy Security, and Emergency Response

QUESTIONS FROM REPRESENTATIVE MARIANNETTE MILLER-MEEKS

Q1. There's approximately $160 million remaining in the Rural and Municipal Utility Cybersecurity (RMUC) program, with less than a year left in its current authorization. Many cooperatives and municipal utilities have told us that while they appreciate DOE's creative efforts with programs like the ACT Prize, the competitive application process for technical assistance has created barriers for smaller, resource-constrained utilities.

Q1A. What specific barriers have you observed that prevent smaller utilities from accessing RMUC resources?

A1A. The Trump Administration shares your concerns with the RMUC program. As discussed during the hearing, the previous Administration squandered three years of potential progress with a burdensome process that delivered minimal results.

In a series of listening sessions during the previous Administration, utilities listed several barriers: cost share requirements, minimal experience applying for federal funding, or engaging in federal programs, limited staff and budget resources to pursue resource opportunities (e.g. no program manager to write the application or budget for travel to training), limited time to identify and respond to announcements, limited awareness of resources—especially true for the smaller utilities that do not have strong connections with their trade association—application materials that are too long or too complicated, and limited utility leadership support to participate.

Despite this feedback, the previous Administration failed to address many of these barriers. While the Infrastructure Investment and Jobs Act specifically required cooperative agreements, the last Administration's policies made the application process needlessly confusing and burdensome. As discussed in the hearing, the Trump Administration is committed to streamlining the RMUC program to strengthen the security and resilience of rural and municipal utilities.

Q1B. How would the proposed legislative changes, particularly making technical assistance non-competitive, improve program implementation and reach?

A1B. Even under current statute, the Trump Administration is committed to streamlining the RMUC program to pair technical assistance with program offerings at a much lower administrative burden to the participants. This will make it easier for all eligible utilities to participate, especially smaller utilities navigating capacity constraints. This legislation would create a non-competitive assistance program. If enacted, DOE would evaluate current administrative requirements to improve program implementation.

Q2. 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.

Q2A. How do you think about this balance?

A2A. Artificial Intelligence (AI) presents a tremendous technological and economic opportunity, but also includes cyber risks that can and should be addressed. This duality is what led CESER to launch AI For Operationally Resilient Technologies and Systems with three key objectives: (1) Secure With AI, which leverages AI to enhance energy security by developing a full suite of cutting-edge tools for threat detection, operate-through-compromise, enhanced network monitoring, and more; (2) Secure From AI, which tracks and mitigates a broad spectrum of AI-enabled attacks against energy infrastructure; and (3) Secure AI itself, which ensures the security of AI-based systems used to operate, control or defend United States (U.S.) energy systems.

We know that our adversaries are already using AI to enhance their capabilities to attack the U.S. grid. This means that failure to respond is simply not an option. We must ensure that we use next generation technologies to defend our energy systems. At the same time, we must ensure that these tools are thoroughly tested and sufficiently understood so that we can deploy them rapidly.

Q2B. Are there certain applications where simpler, lower-tech approaches might actually be more secure?

A2B. Yes, in some applications, simpler and lower-tech approaches can improve security by reducing digital complexity, limiting connectivity, and eliminating unnecessary cyber exposure. Cyber-Informed Engineering and Consequence-driven Cyber-informed Engineering are built around this idea: identifying critical functions and considering whether simpler, more deterministic, or non-digital approaches can better reduce the likelihood or consequences of cyber compromise. The right solution depends on the mission, but in some cases the most secure option is not adding more technology but engineering the system to be less dependent on vulnerable digital functions.

Q2C. How do we ensure that the AI tools we're deploying to defend the grid don't become the vector for attack?

A2C. Although AI can perform a variety of tasks that improve energy sector performance and effectiveness, AI models have unique vulnerabilities. Adversaries can attack an AI model in an attempt to manipulate its behavior or extract private information from it. CESER is developing a new AI assurance testbed that will enable energy sector stakeholders to better understand how adversaries can attack AI models, how resilient AI models are to attacks, and what impacts these attacks can have on energy applications.

AI tools are also often fairly complicated software systems. As such, it is critically important to ensure that they are held to the same high standards for cybersecurity as other tools. This necessitates robust end-to-end cybersecurity practices and evaluations to ensure that the coding practices, development environments, update mechanisms, and more create fully secure end-to-end AI systems.

United States House of Representatives Committee on Energy and Commerce
Subcommittee on Energy
January 13, 2026 Hearing: Protecting America's Energy Infrastructure in Today's Cyber and Physical Threat Landscape
Questions for Alex Fitzsimmons, Director
Office of Cybersecurity, Energy Security, and Emergency Response

QUESTIONS FROM REPRESENTATIVE FRANK PALLONE, JR.

Q1. During questioning, you asserted that political retribution – if an awardee is located in a state that voted for President Trump – has nothing to do with whether or not an award was canceled by the Department of Energy (DOE) last October. However, in a court filing dated December 23, 2025, that was signed by an Assistant Attorney General, the Department of Justice stipulated that, "A primary reason for the selection of which DOE grant termination decisions were included in the October 2025 notice tranche was whether the grantee was located in a 'Blue State.'" I entered this court filing into the hearing record during my questioning.

Q1A. In response to Representative Tonko's question about the Department of Justice's stipulation, you stated that "we do not agree with the court's filing." Is it DOE's stance that the Department of Justice stipulation quoted above is incorrect or misleading?

Q1B. Why did DOE consider if an awardee was in a "blue state" when deciding to cancel or announce the cancellation of an award?

Q1C. Who directed DOE to consider if an awardee was in a "blue state" when deciding to cancel or announce the cancellation of an award?

A1. As part of Department of Energy's (DOE) Portfolio Review Process (PRP), program offices that were involved in the process were tasked with assessing their financial assistance awards against a number of criteria including whether a project has achieved the milestones set forth in the terms of the award; whether a project remains technically and economically feasible; and whether, pursuant to 2 C.F.R. 200.340(a)(4), a project continues to effectuate the purpose of the program or the Department's priorities. These criteria do not include political geography or a financial assistance award recipient's location. Based on this assessment, program offices developed proposals to retain, modify, or terminate projects which were then presented to a cross-functional committee for feedback, with program offices then making (and implementing) the final decisions whether to retain, modify or terminate projects. To date, program offices have reviewed more than 2,000 awards against these criteria.

The May 2025 Office of Clean Energy Demonstrations termination notices and the October 2025 termination notices were part of a much larger tranche of awards reviewed by different offices, with the bulk of the proposed decisions being to proceed with awards either as written or subject to modifications.

At issue in the *City of St. Paul* litigation was whether DOE's termination of seven awards relevant to the plaintiffs was consistent with the First Amendment and Fifth Amendment. Defendants, DOE and Office of Management and Budget, explained that the initial tranche of termination notices sent in October 2025 was drawn from the broader list of termination decisions, as described above, which had nothing to do with political geography or a financial assistance award recipient's location. In a decision filed January 12, 2026, the court dismissed the First Amendment claim but ruled that termination of seven awards was inconsistent with the Fifth Amendment. Although DOE disagrees with the court's decision on the Fifth Amendment claim, DOE has complied with the court's Order and reinstated the awards at issue in the case.

As noted, the decision in *City of St. Paul* vacated seven termination notices but did not address the overwhelming majority of awards for which DOE has sent termination notices. In accordance with 2 C.F.R. 910.128, DOE offices continue to engage in informal dispute resolution with award recipients that have disputed a termination notice they received.

Q2. Beyond the awards illegally canceled by DOE throughout 2025, we have received countless anecdotes of other awards where DOE has simply refused, without cause, to definitize a final award or move from one gate stage to the next. In other cases, DOE has simply ignored outreach from an award recipient, refusing to answer questions from the award recipient.

Q2A. Why has DOE ceased engaging with recipients of awards it has not canceled?

A2A. As indicated above, the October notice tranche was part of a subset of a much larger set of awards—more than 2,200—that DOE program offices reviewed as part of the PRP. Litigation was filed before DOE took final action on the balance of the reviewed awards. DOE has since taken final action to retain or modify 75% of the reviewed awards. DOE has also taken steps to ensure that program offices are continuing to fund projects on which final action has not been taken.

Q2B. Has Secretary Wright or anyone from the Executive Office of the President directed any DOE employee to cease engaging with certain award recipients?

A2B. No. DOE has continued to engage in informal dispute resolution with terminated award recipients. It has taken final action to retain or modify 75% of the more than 2,200 awards that have been reviewed to date. And, it has taken steps to ensure that program offices are continuing to fund projects on which final action has not been taken. It is also meeting with recipients of conditional awards that the prior Administration never definitized to explore whether project proposals can be modified to effectuate program goals or to further DOE priorities.

Q2C. Has Secretary Wright or anyone from the Executive Office of the President directed any DOE employee to refuse to advance projects through their milestone phases?

A2C. No. As part of the PRP process, program offices assess whether—if applicable under the terms of an award—a project has met agreed-to milestones. This assessment is conducted by program offices working with technical staff and program counsel.