



Promoting Innovation Worldwide

Via Electronic Filing

October 8, 2026

Eric Rollison
Assistant Director - Technology Development
Office of Cybersecurity, Energy Security, and Emergency Response
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0121

Re: Ex Parte Meeting on ITI's Response to U.S. Department of Energy (DOE) Request for Information (RFI) on Securing the U.S. Bulk-Power System (BPS), Docket No. DOE-HQ-2026-1123

Dear Mr. Rollison:

On October 2, 2026, Courtney Lang, Megan Petersen, Rachel Ross, and Stephanie Patel of the Information Technology Industry Council (ITI) met virtually with Andrew McClure, Director of DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER). The purpose of this ex parte meeting was to discuss ITI's forthcoming comments in response to DOE's RFI on Securing the U.S. BPS, Docket No. DOE-HQ-2026-1123.

ITI expressed its support for DOE's and the Trump Administration's objective to protect the BPS from malicious cyber activity and mitigate supply chain vulnerabilities through a risk-based approach. ITI also expressed concerns about the unintended consequences of regulatory uncertainty and potential supply chain disruption that could result from DOE's actions implementing EO 14421.

In this context, ITI offered the following recommendations to help DOE advance its national security objectives while promoting innovation, regulatory clarity, and continued access to secure and affordable technologies:

- **Take a targeted, risk-based approach that defines covered equipment through objective characteristics that demonstrate a direct and material impact on BPS operation.** Factors may include whether equipment is deployed in a BPS asset or facility; supports transmission-level operations (69 kV+); performs protection, control, monitoring, communications, or operational functions; and could materially affect BPS reliability if compromised. ITI further recommends general data-center and other enterprise IT equipment should not be considered BPS equipment merely because it is deployed by a utility or at a BPS or critical-infrastructure facility, unless it is specifically configured to directly operate, protect, or control BPS assets.
- **Apply a risk-based approach when considering requirements specific to supply chain tracing and provenance,** including bill of material requirements, rather than automatically applying requirements to all equipment potentially implicated by EO 14421.
- **Recognize and align with existing standards to avoid creating duplicative security frameworks.** For example, ISA/IEC 62443, secure development lifecycle standards, software bill of

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

@ info@itic.org
www.itic.org
@iti_techtweets

materials (SBOM) processes, and existing supply chain security risk management programs can be viewed as evidence of meaningful risk mitigation. They should not be viewed as a security guarantee.

- **Recognize existing vulnerability disclosure processes, and consider severity, exploitability, deployment context, and the effectiveness of mitigations when assessing risk.** For example, NIST, CISA, and international standards provide established approaches for receiving, remediating, validating, prioritizing, and communicating vulnerabilities.
- **To reduce administrative burdens and confusion, use existing, well-established contracting processes or regulations,** such as the Federal Acquisition Regulation (FAR) contracting regulations that include comprehensive requirements and procedures for reporting, testing, inspection, attestation, changes, and recordkeeping.
- **Avoid overly restrictive domestic sourcing requirements for commercial technologies; focus on balancing risk with innovation.** For example, use The Federal Acquisition Security Council (FASC) to maintain sound, risk-based Supply Chain Risk Management (SCRM) policy governmentwide, and avoid applying blanket country-of-origin restrictions to technology.
- **Develop a transparent, deliberative process for EO 14421 implementation and governance,** which should include a notice-and-comment rulemaking, clear implementation guidance, and processes for appropriate transition periods and continued engagement with industry. ITI further recommends that DOE include defined timelines and procedures for transaction reviews, apply appropriate confidentiality protections for information submitted. We also suggest that any new restrictions account for good-faith submissions already under review and provide reasonable protections for existing contracts, inventory, and products in transit.

ITI appreciates DOE's engagement and welcomes further collaboration to advance shared national security goals while supporting innovation and resilient BPS technology supply chains

Pursuant to DOE's Guidance on Ex Parte Communications (Federal Register / Vol. 74, No. 197), this letter is being electronically filed with DOE. Please contact the undersigned if you have any questions on this filing.

Respectfully submitted,

/s/ Courtney Lang

Courtney Lang
Senior Vice President for Trust, Data, and Technology Policy

/s/ Megan Petersen

Megan Petersen,
Senior Vice President of Policy for Public Sector



/s/ Rachel Ross

Rachel Ross
Vice President of Energy and Infrastructure Policy

/s/ Stephanie Patel

Stephanie Patel
Director of Government Affairs