



U.S. Department of Energy Issues Additional Request for Information on Supply Chain Security and Starts New, 100-Day Cybersecurity Initiative

May 4, 2021

Reading Time : **1 min**

By: Scott Daniel Johnson

On April 20, 2021, DOE issued a [Request for Information](#) (RFI) intended “to develop a strengthened approach to address the supply chain security of the U.S. electricity subsector,” and kicked off a new, 100-day plan to address cybersecurity risks to the U.S. electric system. Concurrently, DOE “launched an initiative to enhance the cybersecurity of electric utilities’ industrial control systems (ICS) and secure the energy sector supply chain” to help “safeguard U.S. critical infrastructure from persistent and sophisticated threats.”²⁸ According to a DOE press release, “[t]his 100 day plan—a coordinated effort between DOE, the electricity industry, and the Cybersecurity and Infrastructure Security Agency (CISA)—represents swift, aggressive action[] to confront cyber threats from adversaries who seek to compromise critical systems that are essential to U.S. national and economic security.”

To read the full post, please click [here](#).

Categories

Federal Privacy Policy

© 2025 Akin Gump Strauss Hauer & Feld LLP. All rights reserved. Attorney advertising. This document is distributed for informational use only; it does not constitute legal advice and should not be used as such. Prior results do not guarantee a similar outcome. Akin is the practicing name of Akin Gump LLP, a New York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.