Department of Energy

Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats

APRIL 20, 2021

DOE Kicks Off 100-Day Plan to Address Cybersecurity Risks to the U.S. Electric System, Seeks Input from Stakeholders on Safeguarding U.S. Critical Energy Infrastructure

WASHINGTON, D.C. — As part of the Biden Administration's effort to safeguard U.S. critical infrastructure from persistent and sophisticated threats, the U.S. Department of Energy (DOE) launched an initiative to enhance the cybersecurity of electric utilities' industrial control systems (ICS) and secure the energy sector supply chain. This 100 day plan—a coordinated effort between DOE, the electricity industry, and the Cybersecurity and Infrastructure Security Agency (CISA) —represents swift, aggressive actions to confront cyber threats from adversaries who seek to compromise critical systems that are essential to U.S. national and economic security.

"The United States faces a well-documented and increasing cyber threat from malicious actors seeking to disrupt the electricity Americans rely on to power our homes and businesses," said **Secretary of Energy Jennifer M. Granholm**. "It's up to both government and industry to prevent possible harms—that's why we're working together to take these decisive measures so Americans can rely on a resilient, secure, and clean energy system."

"The safety and security of the American people depend on the resilience of our nation's critical infrastructure. This partnership with the Department of Energy to protect the U.S. electric system will prove a valuable pilot as we continue our work to secure industrial control systems across all sectors," said **CISA Director (Acting) Brandon Wales.**

Advancing Technologies to Protect U.S. Electric Power System from Cyber Threats

Over the next 100 days, DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER)—in partnership with electric utilities—will continue to advance technologies and systems that will provide cyber visibility, detection, and response capabilities for industrial control systems of electric utilities.

The initiative modernizes cybersecurity defenses and:

- Encourages owners and operators to implement measures or technology that enhance their detection, mitigation, and forensic capabilities;
- Includes concrete milestones over the next 100 days for owners and operators to identify and deploy technologies and systems that enable near real time situational awareness and response capabilities in critical industrial control system (ICS) and operational technology (OT) networks;
- Reinforces and enhances the cybersecurity posture of critical infrastructure information technology (IT) networks; and
- Includes a voluntary industry effort to deploy technologies to increase visibility of threats in ICS and OT systems.

Seeking Energy Industry Input on Securing the U.S. Energy System

In addition, DOE released a new Request for Information (RFI) to seek input from

electric utilities, energy companies, academia, research laboratories, government agencies, and other stakeholders to inform future recommendations for supply chain security in U.S. energy systems.

Following a 90-day suspension, EO 13920 resumes effect. With the release of the RFI and to provide a consistent and clear policy environment, DOE is revoking the "Prohibition Order Securing Critical Defense Facilities." The comments received in response to the RFI will enable DOE to evaluate new executive actions to further secure the nation's critical infrastructure against malicious cyber activity and strengthen the domestic manufacturing base. Accordingly, the Department expects that, during the period of time in which further recommendations are being developed, utilities will continue to act in a way that minimizes the risk of installing electric equipment and programmable components- that are subject to foreign adversaries' ownership, control, or influence.

The RFI is available on the Office of Electricity's web page, www.energy.gov/oe/securing-critical-electric-infrastructure, and responses will be due by 5 PM Eastern Time on Monday, June 7, 2021.

DOE's actions support the Administration's comprehensive strategy and are part of a whole of government effort, including the recent "America's Supply Chains" Executive Order 14017, to strengthen the resilience, diversity, and security of American supply chains and industrial control systems to ensure economic prosperity and national security.

###

1000 Independence Ave. SW

Washington DC 20585

202-586-5000

Sign Up for Email Updates

ABOUT ENERGY.GOV

ENERGY.GOV RESOURCES

FEDERAL GOVERNMENT