



iDefender, LLC
225 Foxborough Blvd., Suite 202
Foxborough MA 02035

June 3, 2021

Industrial Defender is pleased to provide the following response to questions posed in the Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure that was released by the Office of Electricity, Department of Energy (DOE).

Founded in 2006, Industrial Defender was the first operational technology (OT) cybersecurity provider in the market. Our solution has been widely adopted by some of the largest critical infrastructure companies in the world to provide asset management and cybersecurity monitoring for their OT environments. In the USA, our technology monitors the power grid and gas control systems in 20 of the largest MSA's as well as many smaller markets.

Our response is based on over a decade of experience providing OT cybersecurity solutions to the energy industry, with a specific focus on electric utilities.

Response to Section A. Development of a Long-Term Strategy

1. What technical assistance would States, Indian Tribes, or units of local government need to enhance their security efforts relative to the electric system?

Creating the Appropriate Incentives

The challenge with improving cybersecurity in the electric industry is not primarily a technical issue. To ensure success, any directive requires both proper incentives and auditable compliance. Two recent major failures within the energy industry, the Texas winterization failure and the Colonial Pipeline incident, both had one thing in common: voluntary guidelines. The NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) requirements have been successful in incentivizing utilities and operators to evolve their security maturity because it is both funded via rate case investment and audit finding penalties.

Expand NERC CIP to include all aspects of the Electric Grid

We recommend extending the NERC CIP framework to all interconnected resources regardless of impact. This would include Generation, Transmission, Distribution, Distributed Energy Resources (DERS), Advanced Metering Infrastructure (AMI), Microgrids, and Outage Management Systems (OMS). Policies should properly incentivize all the interconnected entities to make the proper process and technical security improvements. These improvements should be funded either via tax credits, grants, or investment recovery.

Defense in Depth

When it comes to cybersecurity to protect the electric system (or any system), there is no magic bullet. There is not one product, one service, one company, one individual, or one methodology that can by itself solve all or most cybersecurity issues. We recommend a "Defense in Depth" approach that embodies the spirit of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The key elements of this framework (IDENTIFY, PROTECT, DETECT,

RESPOND, and RECOVER) should be normalized across our critical national infrastructure to provide visibility and consistent monitoring of the OT assets supporting these systems.

2. What specific additional actions could be taken by regulators to address the security of critical electric infrastructure and the incorporation of criteria for evaluating foreign ownership, control, and influence into supply chain risk management, and how can the Department of Energy best inform those actions?

The federal government should consider additional funding mechanisms to assist critical infrastructure companies who implement and maintain cybersecurity programs using software and services developed and delivered in the United States. In the past, the government provided investment tax credits (ITCs) as an incentive for purchase of industrial plants and machinery. Similar ITCs would help fund the proper investments to keep the country safe.


In addition, it might be valuable to enhance NERC/FERC requirements to properly incentive the use of ICS technology that has the capability to identify and inventory hardware and software components on a network to help determine where foreign products have already been deployed.

Response to Section B. Prohibition Authority

1. To ensure the national security, should the Secretary seek to issue a Prohibition Order or other action that applies to equipment installed on parts of the electric distribution system, i.e., distribution equipment and facilities?

Before a Prohibition Order is enacted, it is important for utilities to have the capability to automate discovery and drive visibility on the components that are most at risk, and to identify and prioritize critical infrastructure areas within their respective networks. This will enable them to better understand their Software Bill of Materials (SBOM) and remediate any uncovered vulnerabilities.

Respectfully submitted,

DocuSigned by:

740855F6C13C472...

Jim Crowley
Chief Executive Officer
iDefender, LLC
225 Foxborough Blvd, Suite 202
Foxborough, MA 02035
Telephone: 617-675-4245
Email: jcrowley@industrialdefender.com