503.276.7500 MAIN
503.223.0182 FAX

Tripwire, Inc | 308 SW 2nd Avenue, Suite 400 | Portland, Oregon 97204 | USA

tripwire.com

DEPARTMENT OF ENERGY

Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure

AGENCY: Office of Electricity, Department of Energy (DOE).

ACTION: Request for information.

RFI Comments

Tripwire, Inc., and its parent company Belden Inc. applaud the Department of Energy's (DOE) engagement of public and private contributors, operators, and benefactors of the Critical Electric Infrastructure (CEI) with their Request for Information (RFI) in securing the United States electrical grid. Tripwire and its parent company Belden offer over 20 years of experience in leading global IT-OT cybersecurity solutions—and over 100 years in supporting the government's critical infrastructure sectors. Tripwire is trusted across many electrical utilities, water utilities, numerous intelligence agencies and their mission partners, federal departments, and independent agencies. Additionally, both companies are positioned to provide unique insights and solutions that will help to maintain the continuity of our economy and livelihood that is so intertwined with our critical electrical infrastructure. In concert with Executive Order 14017 "100-day sprint", common solutions exist to fulfill the need for visibility and detection of threats that can act as a backstop to the supply chain concerns raised in the RFI. Simplicity, redundancy and cost of implementation will be key factors in determining any future actions by the DOE and other United States Government (USG) agencies. We urge the DOE to seek solutions that can satisfy both the RFI and the 100-day sprint requirements.

Per RFI section II. A. 1., technical assistance needs to come in the form of public or private advisory assistance to establish basic and foundational cyber security solutions to identify, assess and protect CEI assets. The basics of asset inventory and visibility is a critical first step to fully understanding the composition, architecture, and assets on the CEI network. Currently, this is an informal and often manual process. Technology exists to electronically gather and assemble a proper CEI inventory to comprehensively understand the inventory of assets. Secondly, the same technology can obtain asset configuration and supply chain information to better understand vulnerabilities and supply chain threats by assets and sub-components. In addition, simple asset log management tools can record and assist in assessing threats and perform post-event forensic analysis. Thus, cybersecurity advisory assistance can readily point to existing technologies that provide a proper inventory of CEI assets, configuration of assets and identify vulnerabilities to the supply chain or operation of the CEI.

Per RFI section II. A. 2., Regulators should look to extend the most critical and basic cyber security principles of the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) beyond the existing and limited critical asset perimeter. These principals should be expanded to include additional generation, transmission, and distribution assets to construct a more comprehensive CEI asset inventory and associated cyber and supply chain vulnerabilities.

Per RFI section II. B. 1., the distribution system is a vital part of the electrical infrastructure and should be evaluated using the basic and foundational cyber security solutions identified above, per RFI section II. A. 1. A Prohibition Order would be favorable to reducing the exposure to foreign adversaries/threat actors on installed distribution equipment. Mitigations should be considered, specifically, cyber security solutions can be implemented to properly assess the existing cyber or supply chain risks, identify vulnerabilities for each and provide additional information to construct and execute remediation plans.

Per RFI section II. B. 2., since national security is also dependent upon the safe and reliable operation of all critical infrastructures, reliant or not on the safe operation of the electrical infrastructure, the Secretary should extend Prohibition Orders to reduce threat exposure per RFI section II. A. 1.

Per RFI section II. B. 4., since the inception and guidance of NERC CIP, utilities have proven the ability to identify critical cyber assets. The extension of this existing guideline signals the ability to properly identify additional and future critical infrastructure. As with NERC CIP, cyber security solutions exist to identify the majority of critical assets efficiently and remotely. In addition, these cyber solutions can simultaneously provide additional supply chain configuration and vulnerability data.

In summary, we continue to applaud and support the USG, DOE, and Biden Administration in their efforts to better understand foundational security controls for electric grid and utilities. This can easily be accomplished by implementing tools that maintain current asset inventory; identify configuration anomalies and changes to baselines; recognize supply chain and cyber vulnerabilities and contribute to basic guidelines that support the security journey. In addition to these tools, Tripwire offers a dedicated content and security research team who provide real time risk and vulnerability analysis for the electrical utility and critical infrastructure providers we work with. Tripwire and Belden are eager to further support and enhance the United States critical infrastructure. We are honored to participate in this RFI to protect our economy and way of life.