Response to the DOE RFI on Securing Critical Electric Infrastructure

Joe Weiss PE, CISM, CRISC

Managing Partner Applied Control Solutions, LLC

DOE has requested input on developing a long-term strategy that includes technical assistance needs, supply chain risk management, procurement best practices, and risk mitigation criteria.

My perspectives come from having helped start the control system cyber security program for the electric utilities in 2000 while at EPRI, preparing utility control system cyber security primers and guidelines, written a chapter on “Cyber Security of Substation Control and Diagnostic Systems” for Electric Power Substations Engineering, performed electric industry cyber risk assessments, given industry short courses on control system cyber security, and having amassed a database of 350 control system cyber incidents in the North American electric industry including more than 5 major outages (each outage affected more than 96,000 customers and some affected multi-million customers).

Given my unique background, it is inconceivable to me that there are minimal to no cyber security disclosures by NERC’s Lessons Learned program or with DOE’s Electric Emergency Incident and Disturbance Report Form OE417. Many of the Lessons Learned incidents are obviously control system cyber incidents but NERC refuses to call them cyber-related (see later discussion where “cyber incident” is defined). There needs to be more disclosures by industry of actual cyber incidents which is clearly not happening. Moreover, there also needs to be “controlled” disclosure by DOE to industry particularly when cyber-related incidents are found. This is especially true of the inspection results from the Chinese transformer at the Sandia National Laboratory.

If it is DOE’s intent to secure the grid, it must consider all aspects of the traditional and microgrids including non-nuclear power plants, substations, control centers, all communications between systems and people, and appropriate training. DOE must not ignore any of the critical pieces of the grid that are ignored by NERC. That is, low voltage transmission, distribution, and all power plants, real, and virtual, need to be addressed. It also includes monitoring of all power flows.

The long-term strategy for securing the electric must require a basic cyber security program consisting of a current inventory of all installed devices (control system devices and OT network devices) and OT networks including firmware and patch revisions. The program must also be an ability to identify those devices with identified vulnerabilities. Patch management needs to be performed using patch management guidelines for control systems such as ISA62443-2-3. Network segmentation is also critical.

Specifically, a control system cyber security program to secure critical electric infrastructure assets must focus on the programmable devices used in power plants, substations, and control centers including the traditional grid and microgrids. This includes the list of equipment specifically identified in EO 13920. Currently, there is no cyber security, authentication, or cyber logging in many of the devices identified in EO 13920 or has there been attention to the hardware cyber issues in these devices.

Training and procurement specifications must be based on actual case histories and that includes physics-based incidents such as Aurora. Reporting must include all malicious and unintentional cyber incidents which has not been occurring (see above). The May 2021 GAO report “CYBER INSURANCE Insurers and Policyholders Face Challenges in an Evolving Market” (<https://www.gao.gov/assets/gao-21-477.pdf>) also make it clear that you have to identify cyber incidents whether they are malicious or unintentional. Specifically, the report defined a cyber incident as an event that jeopardizes the cybersecurity of an information system or the information the system processes, stores, or transmits; or an event that violates security policies, procedures, or acceptable use policies, **whether resulting from malicious activity or not**. Cyber incidents, including cyberattacks, can damage information technology assets, create losses related to business disruption and theft, release sensitive information, and expose entities to liability from customers, suppliers, employees, and shareholders.”

DOE seeks input on the depth and breadth of a future prohibition authority:

There are more than 200 large Chinese-made electric transformers installed in the US bulk electric grid. It is unknown how many of these transformers have hardware implants, software logic bombs, or Chinese-made chips. Moreover, there are no requirements or proposed requirements to address the potential of hardware implants in electric industry equipment manufactured or supplied from China. It is one thing to prohibit new Chinese-made equipment, but existing equipment must also be addressed. It is recommended that all equipment identified in EO 13920 be periodically tested to assure that the equipment will perform as expected.