WHITE PAPER / **CYBERSECURITY**

# Executive order adds momentum to mitigation of cyberthreats to U.S. power industry

BY **Jeff Macre,** CISSP, PMP, AND **Matt Morris,** EMBA

In the face of increasingly sophisticated cyberattacks in recent years, the U.S. utility industry has responded with an array of strategies designed to reduce and eliminate vulnerabilities to increasingly digitized systems. Now, with the recent issuance of an executive order from President Donald Trump, utilities will expand this effort to other assets touching the bulk electric system.

The clock is now ticking for the U.S. power industry. The recent executive order (EO) from President Trump sets in motion a timeline to eventually result in sourcing of bulk electric system (BES) equipment only from North American or other "friendly" regions.

While sourcing and the supply chain were already a focal point in response to the North American Electric Reliability Corp.'s (NERC) CIP 013-1 cyber protection rule, the new EO has clear ramifications for cybersecurity. CIP-013-1 — which will now go into effect on Oct. 1, reflecting a three-month extension from its original July 1 effective date — is intended to set rules for utilities to follow in mitigating risks to supply chains for equipment needed for BES cybersystems.

U.S. utilities have been the targets of increasingly sophisticated cyberattacks for more than 10 years and, as a consequence, the threat intelligence continues to improve. The power industry is already well-along in sourcing information technology (IT) and operational technology (OT) equipment from U.S. companies or their affiliates, or other companies in countries that are friendly to U.S. interests.

Now, given the known history of attacks and ongoing efforts to address vulnerabilities within the industry, the EO allows us to take a next step and formalize many processes that, for some, have already been underway.

The power industry is far more dependent on devices and equipment that may contain components from foreign countries than the general public realizes. Substations, for example, are loaded with a variety of hardware and software as are control rooms in most generating plants.

While it depends on the component, some components and assets will be easy to address. Supply chains for copper or other raw materials are well-defined and manufacturers of large transmission, distribution and generation equipment are well-established.

But for technology-dependent elements of the grid — such as supervisory control and data access (SCADA) systems, programmable logic controllers (PLCs), distributed control systems (DCSs), as well as pumps, actuators, pressure valves, and sensors — it will be more complex because many individual components in substations or other key locations typically have a large number of subcomponents that may originate from locations across the globe.

We already know that certain subcomponents can be programmed to "call home" periodically for the purported reason of checking for firmware or logic updates that can be downloaded. Even for systems that utilities believe are air-gapped — i.e., not connected via wired or wireless interfaces to outside networks — we can often plug in diagnostic tools showing that some components are not air-gapped at all.  While most of these connections usually make their way back to an IT administrator, some of these may also be unsuspectedly pointed to nefarious places. These are usually subcomponents in hardware that are designed to perform a relatively innocuous function. Though the design feature may have innocent intent, the reality is this can open backdoors that hackers can take advantage of.

Even in the heightened security environment of the utility industry, networks are usually still vulnerable, and the reality is that air-gapped systems no longer exist. Occasionally, whether purposefully or not, there may be systems that are not plugged into a wired network, yet they have a wireless network interface controller (Wi-Fi) connection that may be connecting to nearby networks, unbeknownst to network administrators. Wireless, or Wi-Fi, is surprisingly common and requires that the Wi-Fi controller be permanently disabled or physically removed.

The CIP-013-1 effort begins to address some of these issues and, to some extent, dovetails with the recent EO as it addresses these two fundamental questions:

- How much risk is posed to U.S. organizations as a result of supply chain risk?
- How vulnerable are the components and equipment themselves to external attacks from hackers and others with malevolent intent?

Both questions are of fundamental importance and must be a high priority for cybersecurity professionals.

There is no question that cyberthreat levels are increasing. The 2015 attack in Ukraine that took down portions of the power grid serving Kyiv was among the most publicized warnings to all in the cybersecurity profession.

The attack is known to have employed grid-sabotaging malware that was automated to create mass outages. From the forensic analysis that followed, we know the attack originated from groups that were likely sponsored by Russian interests and the attack was most likely a test of a variety of swappable malware components that can be used to attack a number of utility systems.

The attack was centered around automated grid controls and was designed to make it very difficult to override those controls and restore power. Because many of these systems are similar to U.S. technology and some are even designed and installed by U.S. consultants, it is widely believed the attack was simply a dress rehearsal to see what could be accomplished in an attack on the U.S. grid.

As it turned out, the attack was not as serious as it could have been in Ukraine, primarily because automation of critical systems in Ukraine is much further behind than for such systems in the United States. Ukrainian utility managers were able to manually dispatch crews to substations to reset controls, restoring power.

The Ukraine attack was a wake-up call that underscored one of the issues that is fundamental and foundational to any successful cybersecurity program, which is to establish and maintain accurate asset inventories. At 1898 & Co, we recommend utilities develop an asset inventory, containing both software and hardware, for their operating technology (OT) environment. By having such an asset inventory, utilities will more easily be able to align with the new EO as it is gradually translated into concrete action.

The combination of an asset inventory with vulnerability management information is a powerful mitigation approach. Vulnerability management capabilities allow for risk level rankings to be assigned to each component or subcomponent in order to correlate assets with known vulnerabilities that exist (based off known attacks logged by security researchers, OEM vendors, consultants, and the market at large). This becomes an important mitigation capability when specific assets, components or subcomponents are identified as being problematic — whether those are hardware or software — so that practitioners are able to issue a query across their asset inventory, identify the location of those components, and put together a remediation plan.

Vulnerability databases are already well-along in development and most major equipment vendors push out detailed listings of components with all potential vulnerabilities identified. These cover a range of issues, from design flaws that have been identified to known instances of adversaries creating backdoors in certain pieces of software. Many times, a forensic analysis will reveal that certain pieces of equipment are connecting with suspicious web servers. This commonly happens as researchers conduct vulnerability and malware analyses, and the vulnerability databases are continually updated with these findings.

We know there are many malevolent actors on the global stage who would love nothing more than to take down the North American electrical grid, the backbone of our economy. With this risk-mitigation approach now extended to all BES equipment and components under the momentum of the recent EO, vulnerabilities in supply chains and within the design of increasingly digital equipment and components themselves will be addressed in a more rigorous manner.

## Biographies

**Jeff Macre, CISSP, PMP,** is a senior cybersecurity specialist and project manager for 1898 & Co., part of Burns & McDonnell. As an experienced leader specializing in information technology security, NERC CIP compliance and implementation, infrastructure management, and systems administration, he helps clients design and implement standards, procedures and processes that improve their business efficiency.

**Matt Morris, EMBA,** director of critical infrastructure cybersecurity at 1898 & Co., has more than two decades experience in digitalization and industrial cybersecurity with a focus on helping companies, governments and nations manage risks to safety, operations and productivity.

## About 1898 & Co.

1898 & Co. is a business, technology and security solutions consultancy where experience and foresight come together to unlock lasting advancements. We innovate today to fuel your future growth, catalyzing insights that drive smarter decisions, improve performance and maximize value. As part of Burns & McDonnell, we draw on more than 120 years of deep and broad experience in complex industries as we envision and enable the future for our clients. For more information, visit **1898andCo.com**.