

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

**Joint Staff White Paper on Notices of
Penalty Pertaining to Violations of Critical
Infrastructure Protection Reliability Standards**

Docket No. AD19-18-000

Comments on Transparency/Further Recommendations

Submitted to FERC on September 20, 2019

Joseph M. Weiss, a private citizen and control system cyber security expert, respectfully submits comments on FERC Docket No. AD19-18-000, Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards.

Background

I am considered to be an international authority on control system cybersecurity with more than 45 years of experience in control systems and cyber security of control systems. I have worked with numerous people, manufacturers, end-users, and consensus standards organizations including being part of the original North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Working Group (before it became NERC CIPC). I also helped start the control system cyber security program for the electric utilities at the Electric Power Research Institute (EPRI) in 2000. I am currently the Managing Director of the International Society of Automation (ISA) S67 (Nuclear Plant Standards), ISA77 (Fossil Plant Standards), ISA99 (Control System Cyber Security) and various Institute of Electrical and Electronics Engineers (IEEE), International Electrotechnical Commission (IEC), NERC, and CIGRÉ (International Council on Large Electric System) committees. I maintain a blog entitled "Unfettered" on the website ControlGlobal.com and have authored the book *Protecting Industrial Control Systems from Electronic Threats* and various book chapters on control system cyber security. I also supported the Federal Energy Regulatory Commission (FERC), the Nuclear Regulatory Commission (NRC), and the National Institute of Standards and Technology (NIST).

Transparency Can Change Corporate Culture, but NERC CIP is Ineffective

I have assisted hundreds of companies and individuals with improving their organization's control system cybersecurity and have witnessed an overall lack of priority on control system cyber security among corporate leaders in the electric power industry. I believe that an increase of transparency in the method by which FERC and NERC process Notices of Penalty (NOPs) for violations of Critical Infrastructure Protection (CIP) Reliability Standards would result in a higher prioritization by corporate leadership in preventing their organization from violating these CIP reliability standards. However, this makes the assumption that the current NERC CIPs are actually effective in maintaining the reliability, resilience, and cyber security of the bulk transmission system. Based on my experience, I believe this is a false assumption.

For example:

- There have been utilities who have been fined for doing MORE than what the NERC CIPs require;
- NERC CIPs require disclosure only on "critical assets";
- NERC CIP auditors have an incentive to find problems but generally do not understand the implications to the reliability of the electric grid;
- Many NERC CIP violations are "paper" issues that have nothing to do with the actual protection of electric grid assets;

- The most important devices for the reliability of the electric grid are not even in scope for the NERC CIP and Supply Chain requirements such as process sensors, actuators, drives, as well as serial communications, etc.;
- Known security issues such as connecting SCADA and control systems directly to the Internet are allowed so this real violation is not even considered a violation; and
- NERC CIP002 is the requirement for defining critical assets. Violations of this requirement are what NERC references as the "\$1 million per day fine". However, there haven't been any \$1 million per day violations of this requirement cited by NERC.

For Improved Cybersecurity, NERC Must Acknowledge Cyber Incidents

I also believe that for any enforcement regime for cybersecurity to be effective, NERC must be willing to acknowledge when grid assets have had a cyber incident, whether it is known to be malicious or unintentional. This is because it may not be possible to discriminate between a malfunction versus a malicious event as a sophisticated attacker can make a cyber attack appear to be a malfunction. Disclosure requirements identified by the FERC/NERC white paper on incident reporting - "Joint Staff White Paper on Notices of Penalty Pertaining to Violation of Critical Infrastructure Protection Reliability Standards" - will be meaningless if NERC continues to refuse to call cyber incidents "cyber".

For example, on September 5, 2019, NERC posted a Lesson Learned document to its website that described a cyberattack taking place on 5 March 2019 which has been reported by EE News¹ as the "first" U.S. grid cyberattack. Yet, cybersecurity experts know that malicious cyber incidents affecting the US grid from compromising control system vendors as well as the utilities themselves have been on-going for more than 15 years. Unintentional cyber incidents (at least they appear to be unintentional) have also been occurring for years with similar impacts as malicious incidents. Since 2010, the electric industry has reported 29 cyber-attacks in the mandatory DOE OE-417 reporting forms. Additionally, my database has identified more than 300 actual control system cyber incidents in the North American electric system including 6 major outages affecting at least 90,000 customers. There have been numerous cyberattacks through both properly and improperly configured firewalls.

Here are just a few of the examples of the types of "cyber" incidents that have preceded that 5 March 2019 cyberattack:

- In 2001, China cyber attacked CAISO. The Chinese were not successful at compromising SCADA, but they tried.
- In 2004, a US utility's SCADA system was maliciously compromised and inoperable for 2 weeks. The attacker was not identified as the trail was lost on the second or third hop into Eastern Europe.
- The 2008 Florida outage which affected more than 6 million customers for almost 8 hours was a major incident that while an apparent accident, had many of the hallmarks of a malicious incident. In this case, an engineer was sent to an electric substation to perform diagnostics on a large substation device - a capacitor bank switch (viewed as a distribution device and so outside NERC CIP scope). Instead of only disabling the protection on this device and leaving all of the other protection in place, the engineer disabled ALL relay protection and then called the SCADA operator to remotely energize the affected device. However, the SCADA operator was not told that all protection had been disabled and the SCADA system did not identify the loss of protection. Consequently, the SCADA operator remotely energized the suspect device via a serial link (again, outside NERC CIP scope) resulting in the capacitor bank switch exploding with the

¹ <https://www.eenews.net/stories/1061111289>

resulting cascading outage. The Florida event gets magnified as the Russians targeted capacitor banks in 2018.

- In 2012, the major control system supplier Telvent had its internal firewall and security systems breached by the Chinese. This was a major issue as Telvent had direct remote access to its customers' control systems many of which were in the electric and energy industries.
- The Russians were in the US grid in April 2014 through a Microsoft flaw affecting three major control system vendors' HMI's with Havex and BlackEnergy2 malware. In December 2015, the Russians exercised their "lessons learned" by cyber attacking Ukrainian distribution systems with upgraded Havex and BlackEnergy3 malware. As the NERC CIPs have no requirements to remove malware, the Russian malware is likely still in our electric grids.

NERC Must Re-Scope CIP & Supply Chain Requirements

Not only must NERC be willing to acknowledge cyber incidents for its cybersecurity enforcement regime to be effective, it must also ensure that the NERC CIPs and Supply Chain requirements are of appropriate scope to include important matters such as counterfeit process transmitters which are the heart of reliability and safety.

For example, take the situation of NERC CIP and process sensors:

May 28, 2019, Yokogawa - a major international control system vendor - issued a warning² to their customers about counterfeit process transmitters. Process transmitters measure pressure, level, flow, temperature, etc. Pressure and differential pressure transmitters are used in process control applications across commercial, industrial, manufacturing, and defense applications including nuclear power plant safety applications and non-nuclear Safety Integrated Systems (SIS). Process transmitters are the true "edge devices" in a control system but generally lack cyber security or authentication. Specifically, Yokogawa transmitters are extensively used globally including in North America. The first Yokogawa notification³ on counterfeit transmitters was in 2014 and was based on counterfeit devices found outside North America.

Per Yokogawa, the 2019 announcement was based on a new report of counterfeit products in North America. The known affected counterfeits were limited to the EJA-110E series. The counterfeit products were procured through an unauthorized, counterfeit supply chain with which Yokogawa has no business relationship. Most likely the counterfeits were sold for profit like selling fake Prada purses for a discounted price. Yet, counterfeit transmitters can act as Trojan horses to deliver malware behind firewalls. Counterfeit transmitters can also be misconfigured, inaccurate, or incapable of meeting design requirements.

Counterfeit transmitters are not a unique problem to Yokogawa. There have been numerous cases where counterfeit or "gray market" transmitters from other vendors have been used but there hasn't been a formal notification from other transmitter vendors as with Yokogawa. Sinclair Koelemij from Honeywell responded to the Linked-in discussions on the Yokogawa announcement with the following: "There are numerous other examples of counterfeit field devices and sensors, even in combination with counterfeit ATEX (ATmospheric EXplosible) certifications (ATEX certification is a requirement for all companies who manufacture electrical equipment that is used in hazardous environments and is intended to be marketed in the European Union). The supply chain is critical for control system cyber security and safety, including all elements of an automation system. Not only from a cyber risk perspective, installing counterfeit equipment in the field can lead to very serious accidents. In the case of a false ATEX certification even massive explosions." Other control system suppliers have had customer calls concerning transmitter

² <https://www.controlglobal.com/blogs/unfettered/the-ultimate-control-system-cyber-security-nightmare-using-process-transmitters-as-trojan-horses/>

³ <https://www.yokogawa.com/news/notices/2014/2014-12-08/>

performance where the supplier cannot reconcile the installed transmitter serial number with the supplier's records.

Counterfeit transmitters can be a common-cause failure mechanism which is VERY dangerous. Counterfeit transmitters are also a major concern for process safety applications as many safety systems use the same transmitters as in basic process control applications. Moreover, they can be pre-programmed defeating any cyber security program. Consequently, there is a need to have a program to identify counterfeit devices before they are installed as well as after in case they get through the screening process.

Process instrumentation and safety systems that utilize counterfeit transmitters can cause kinetic damage across multiple facilities – potentially a significant grid reliability problem. Because counterfeit transmitters can be pre-programmed independent of Ethernet (routable) OT networks and yet feed the OT networks, counterfeit transmitters can impact NERC High, Medium, or Low impact systems defeating NERC CIP protections.

Meanwhile, despite these significant concerns regarding the prospect of counterfeit transmitters, NERC has no cyber security program to address counterfeit transmitters. In its Staff Report and Recommended Actions on NERC Cyber Security Supply Chain Risks⁴, NERC staff identify only motion sensors for physical security. NERC continues to avoid addressing control system field devices and networks (sensors being inside the Electronic Security Perimeter makes them out-of-scope). The irony is process sensors are critical for reliability (the "R" in NERC) yet NERC continues to ignore them.

Alternative Processes for Improved Cybersecurity

In her August 27, 2019 "Statement on FERC/NERC Staff White Paper on CIP Standards Notices of Penalties" Commissioner Cheryl LaFleur invited "a wide range of comments on the White Paper, including any suggestions for alternative processes, which will allow FERC and NERC to move forward on this issue." Therefore, I suggest the following:

On Defining a "Cyber Incident":

It is first important to understand what is meant by a cyber incident. I suggest using the NIST definition of electronic communication between systems that impacts Confidentiality (C), Integrity (I), or Availability (A). Note that Safety (S) is missing and needs to be added. Also recognize that Availability may be different than Reliability and Productivity which are also important for control system applications. The NIST definition does not mention the word "malicious." For control systems, the distinction between malicious and unintentional is not as important as understanding if systems are working as they should. People, equipment, and the environment can be at risk in a control system cyber incident. (A brief history of control system cyber incidents can be found on my blog⁵.)

On Control System Cyber Security In General:

For control systems, something basic is consistently overlooked: control system incident hunting. It is not easy to determine if a control system's upset condition is a malfunction, unintentional cyber incident, or malicious cyberattack. Attacks, accidents, and failures can look very much alike. What they have in common is they produce physical effects. Identifying and understanding those physical impacts should be central to control system cyber security.

Additionally, control system cyber security needs to address both networks and control system field devices. This includes people (having instrumentation experts involved), process (monitoring for counterfeit sensors and certifications), and technologies (on-line sensor monitoring). The bottom line is if

⁴ NERC Cyber Security Supply Chain Risks: Staff Report and Recommended Actions Docket No. RM17-13-000.

⁵ <https://www.controlglobal.com/blogs/unfettered/control-system-cyber-incident-hunting-input-for-a-playbook-on-control-system-cyber-incident-investigations-2/>

you have control of the transmitters at the raw signal level in real time, you have control of the process which should be the point of performing control system cyber security.

Fingerprinting process sensors, which included the specific Yokogawa series of sensors, should be able to detect the difference between original (OEM) and counterfeit Yokogawa sensors particularly as the website states there is a difference in the circuit structure and principles of measurement (there were no counterfeit sensors in the fingerprinting work). Moreover, the OT network monitoring and threat detection vendors start by assuming sensors are uncompromised, authenticated, and correct which may not be correct assumptions. ISA99 is addressing cyber security of process sensors at the policy level in ISA/IEC62443-4-2.

I felt out-of-band monitoring of sensors could help with supply chain before I read the Yokogawa announcement. Given the Yokogawa announcement and the Stuxnet and Triton attacks which needed to compromise operator displays, real time out-of-band sensing is needed ASAP.

It has been evident that control system cyber security has suffered from cultural gaps/governance issues which often led to the lack of cyber security in process sensors/transmitters and the lack of instrument engineers/technicians participating in cyber security teams. This also brings up the question as what is meant by the term Operational Technology (OT). If the transmitters are not considered part of OT, this is NOT an IT/OT convergence problem, but a safety and reliability problem. If the transmitters are considered OT, it becomes critical that instrument engineers and technicians become part of the cyber security team.

On NIST 800-53

NERC CIP needs to be replaced by NIST SP800-53. It is already mandatory for the federal utilities such as the Tennessee Valley Authority (TVA), Bonneville Power Administration (BPA), and the Western Area Power Administration (WAPA). NIST SP800-53 does not allow the utilities to *a priori* ignore any system or device. No other industry or organization gets to decide what to address and what to ignore without even looking. There is a problem when a Human Resources organization in a small retail organization is held to a higher cyber security level than the most important electric systems in this country. NIST SP800-53 requires an assessment as to whether the system or device is low, medium, or high priority. This is the only way to have confidence that subtle threats that can cascade to bigger ones and unintended consequences are addressed.

Developing a Cyber Incident Playbook:

Additionally, there is a need for a control system cyber security incident playbook to help with control system cyber incident investigations. Sanitized cases from the Applied Control Solutions database can help form the input for the playbook and, in fact, has been used as such. In the 2007-8 time frame, NIST tasked Marshall Abrams from MITRE (IT and NIST800-53 expertise) and myself (control system expertise) to analyze three publicly-identified control system cyber incidents to help non-Federal entities justify using NIST SP800-53 (recognizing NIST SP800-53 was an IT-based set of requirements). Consequently, we analyzed the 1999 Bellingham, WA Olympic Pipeline Rupture, the 2000 Maroochyshire wastewater attack, and the 2007 Browns Ferry Unit 3 nuclear plant broadcast storm. The results are on the NIST website and in my book, *Protecting Industrial Control Systems from Electronic Threats*. We asked the following:

- What do we know now that wasn't known at the time of the event or initial event analysis?
- What NIST SP800-53 controls were violated that enabled the event to occur?
- If the NIST SP800-53 controls were followed, could the event have been prevented or at least minimized?
- If not, what additional controls were necessary?

In 2015, I did a similar study for the International Atomic Energy Agency (IAEA). The intent was to use real cases to teach nuclear plant system engineers what to look for that could be cyber-related when an upset condition occurs. Consequently, I took 3 of the more than 30 nuclear plant control system cyber incidents that had real physical impacts, occurred in non-nuclear facilities, were not identified as being cyber-related, and most importantly were not IP-network-related so would not be seen by network monitoring.

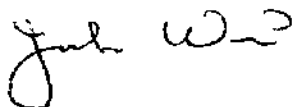
Regarding a cyber incident playbook, using experts from multiple disciplines and relevant control system cyber incident case histories can be very valuable to get IT, OT, system engineers, network threat hunters, and forensics experts on the same page and to "connect the dots". As an example of the need, from a control system cyber perspective, the 1999 Bellingham gasoline pipeline rupture was similar to the 2010 San Bruno natural gas pipeline rupture but was missed as the focus was on piping integrity. Another example of why deep expertise is needed is the recently released Dragos report— "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack". Dragos involved SEL and ORNL which should have been sufficient. However, what was missing was a discussion, or even mention, of the Aurora vulnerability. That is, the reclosing of breakers out-of-phase with the grid which can cause significant long-term equipment damage.

The commonality of control system cyber incidents across industries shouldn't be surprising as multiple industries use similar control system equipment from common control system vendors using common control system protocols. Unfortunately, the incidents keep recurring and the "dots" are not being connected. It is important for engineers and IT/OT to work together (this is not just cross-training and IT/OT convergence) and expand the scope from network threat hunting to include ICS incident hunting. I encourage further discussion on these topics. Perhaps the industry could collaborate on this important, but missing, task.

Transparency Risks vs. Gains

Since FERC posted the White Paper, there have already been articles written by industry-related outlets and industry-related lobbying organizations that warn of releasing identifying information for NERC CIP violations due to this pointing a "red flag" for attackers. I too am concerned about the disclosure of entity names and technical details of how CIP standards being violated, and an adversary correlating this database with the DOE OE-417 reports and ICS-CERT reports. I am also concerned that utilities will begin to share *less* forensic information on cyber incidents for fear of being "named and shamed" as has occurred in the past. Nevertheless, a careful reading of the proposal in the White Paper also shows appropriate protections can be built into the disclosure process that would allow public transparency while leaving out technical details that may be valuable to a potential attacker.

With those suggested considerations, and the reality of the enormous civil and national security dependencies on the bulk power electric system, I see the need for a significant increase in the type of transparency required to change corporate culture. I hope FERC/NERC will make the change toward transparency and also adopt the other alternative processes I have provided in this docket filing.



Joseph Weiss, PE, CISM, CRISC