Formal Testimony to the Energy and Environment Committee on HB24-1246
March 13, 2024

Joseph Weiss, PE, CISA, CRISC
Managing Partner, Applied Control Solutions LLC

My name is Joseph Weiss. I am a control system engineer and have been involved in cyber security of the grid and other critical infrastructures since January 2000 when I helped start the control system cyber security program for the electric utilities while at the Electric Power Research Institute (EPRI). I have provided control system cyber security expertise to the National Institute of Standards and Technology (NIST), the Federal Energy Regulatory Commission (FERC), the Nuclear Regulatory Commission (NRC), the International Atomic Energy Agency (IAEC), the U.S. Department of Defense, among others. I have also testified or provided expert testimony to five House and Senate Hearings on control system cyber security. I have published one book – Protecting Industrial Control Systems from Electronic Threats, chapters in Electric Power Substations Engineering, Water and Wastewater Systems, Data Center Handbook, and Cyber Policy Handbook. For 12 years, I was the Managing Director of the international standards on control system cyber security – ISA99. I have also amassed a database of more than 1,200 control system cyber incidents in the electric grid. I am providing this testimony as a private citizen concerned about the lack of adequate cyber security in our electric grids and the threat from China and other adversaries.

Background
The electric grid is interconnected, whether old grid or new. The interconnectivity goes not only between utilities but also between facilities connected to the grid. This fact is pointed out in various interoperability studies. The Chinese (and other threat actors) are exploiting this cyber security gap.

China has been targeting the U.S. electric system (and other critical infrastructures) for more than 25 years. In 2001, the Chinese cyberattacked the California Independent Systems Operator (CAISO) attempting to take over CAISO's SCADA system. In the 2012-time frame, the Chinese cyberattacked Telvent, a control system supplier to the gas and electric industry.

In May 2020, Presidential Executive Order (EO) 13920 was issued to address the discovery of hardware backdoors in a large (approximately 400 ton) Chinese-made transformer installed in a critical substation, WAPA's Ault substation outside Ault, Colorado. Concerns of what might have been installed in the transformer led to a Chinese power transformer being sent to the U.S. Department of Energy's Sandia National Laboratory (SNL) for detailed inspection. Chillingly, **the results of the SNL inspection report were highly classified**. From the publicly available information from the U.S. electric industry, the Chinese learned what cyber security requirements were required and by when, what equipment was in scope and what was not, and therefore, what was monitored and what was left unmonitored. Additionally, many utilities have moved away from substation inspections on a scheduled basis. This change has led to a lack of consistent information that can be used to analyze any changes that may have occurred. **The Chinese used that information in their approach, but the cyber defenders have not addressed this gap.** This is like the Maginot Line from World War II: strong, but easily bypassed. Yet, SANS prepared a report that took strong exception to the Ault incident being real by pointing to a lack of direct confirmation of concerns about a hardware vulnerability in the transformer supply chain. The SANS report was based entirely on a network assessment. Unfortunately, this wasn't a network problem that could be detected by either network security monitoring or network threat intelligence.

In 2021, the Director of National Intelligence (DNI's) National Intelligence Council's National Intelligence Estimate wrote: "China is the world's leading supplier of advanced grid components for ultra-high-voltage systems, such as transformers, circuit breakers, and inverters, **which we assess creates cyber vulnerability risks**."

Lack of utility response
From 2006 through 2023, the US has imported almost 450 transformers over 10,000 kVA from China. Of these, more than 360 of these Chinese-made transformers exceeded 100,000 kVA (these are the large transmission system transformers necessary for the operation of the grid). Moreover, after EO-13920 was

suspended by the Biden administration, **utilities continue to buy Chinese equipment, more than 125 large Chinese transformers since 2020.**

Inverters are used in solar panels, electric grids, power generation, manufacturing, water/wastewater, etc. The U.S. has imported more than 170,000,000 inverters from China since 2002 (5 million in 2021). It is unclear if the Chinese have backdoors in these devices.

Chinese attacks against electric grids do not just involve compromised transformers and inverters. In 2019, Yokogawa, a major international control system supplier, issued a notice to their customers that counterfeit pressure and differential pressure transmitters were found in North America. These devices are critical for reliable operation and process safety. Counterfeit process sensors and transmitters have been found from multiple control system suppliers. Making a counterfeit transmitter that looks similar enough to a real device to be accepted is not cheap and wouldn't be done on a one-off basis. These counterfeit transmitters can even be found on eBay and Amazon, where they cost significantly less than a real device when purchased from an authorized distributor. Making matters worse, process sensors have no cyber security, authentication, or cyber forensics. Yet in February 2024, DOE and NARUC issued "Cybersecurity Baselines for Electric Distribution Systems and DER" and process sensors were not mentioned. Process sensors are also not addressed in NERC's Supply Chain Criteria and in the NERC CIP standards. An example of why process sensors are so important was a case in Florida where the failure of a single sensor in a medium-sized power plant that caused a 200 MW load swing in Florida caused a 50 MW load swing in New England.

February 27, 2024, the Report to the President, "Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World" was issued. According to the report, "Cyber-physical resilience is the capacity of an integrated system to keep running—even if not at peak performance—should it lose specific functions. Challenges include degradation or cessation of one or more aspects of the computational or physical functions due to component failures, human errors, natural disasters, or malicious attacks. For instance, if one or more computer-based controls, sensors, or Internet communications fail, the system should continue to operate. We should have an understanding in advance of how and how well such operations will proceed in light of one or more failures." However, there are processes where a compromise of one sensor, whether unintentional or malicious, can cause unexpected catastrophic failure such as the load swing example. Compromising one sensor can also provide critical information to an adversary even though the sensor appears to be operating properly or mislead the operator which contributed to the Three Mile Island core melt.

There is a concern that the hardware backdoors in large electric transformers will be able to receive spoofed sensor signals compromising transformer operation without being detected by any cyber security monitoring. One means of providing spoofed sensor signals would be cellular modems installed in the transformers. This is not an idle consideration as **cellular modems have been found in Chinese port cranes (see below) and a bio-pharma manufacturing facility** (I expect there are probably many other cases).

The grid can operate even if a transformer is inoperable. However, engineers can be limited to react due to unexpected voltage fluctuations when a transformer malfunctions. The components on a Chinese transformer don't necessarily need to be used for sabotage to cause a problem with the grid. Knowing the load going through the transformer would allow the Chinese to know the best time for cyberattacks.

As the grid is interconnected, a compromised Chinese transformer connected to a non-Chinese transformer can compromise the non-Chinese transformer. Examples of this include a case of two Chinese transformers not owned by Duke Energy that directly interface with Duke Energy's system and a neighboring utility with a large Chinese transformer that interconnects with AEP. It is unclear what the impact could be on AEP's and Duke's grids if the Chinese transformers are compromised.

Some of the largest utilities in the country, including the "leaders in grid security", have Chinese transformers and other critical grid equipment. Why aren't U.S. utilities removing Chinese components from our grids?

<u>DOD is waking up</u>

Duke Energy agreed under pressure from the US Congress to decommission energy storage batteries produced by Chinese battery giant CATL installed at Marine Corps Base Camp Lejeune in North Carolina over concerns that the batteries pose a security risk. Reuters reported that Duke Energy had made plans to decommission the CATL-made batteries that were commissioned less than a year ago in March 2023. However, by year's end, Duke Energy had disconnected the battery storage project, citing concerns raised by lawmakers and experts about CATL's close ties to China's ruling Communist Party. The batteries and their inverters may have cyber vulnerabilities that could be used to compromise the electricity grid. **Duke Energy stated that the battery system had nevertheless been designed with "security in mind" and that the batteries "were not connected in any way to Camp Lejeune's network or other systems."** This is very dubious, especially from a leader in grid cyber security.

US Government is partially awake

In December 2023, Brandon Wales, executive director of CISA, stated "It is very clear that Chinese attempts to compromise critical infrastructure are in part to pre-position themselves to be able to disrupt or destroy that critical infrastructure in the event of a conflict, to either prevent the United States from being able to project power into Asia or to cause societal chaos inside the U.S.— to affect our decision-making around a crisis. **That is a significant change from Chinese cyber activity from seven to 10 years ago that was focused primarily on political and economic espionage**."

On February 18, 2024, FBI Director Wray confirmed that China has "offensive weapons within our critical infrastructure poised to attack whenever Beijing decides the time is right." Citing Volt Typhoon, the name given to the Chinese hacking network that was discovered last year lying dormant inside U.S. critical infrastructure, Wray said that Beijing-backed actors were pre-positioning malware that could be triggered at any moment to disrupt U.S. critical infrastructure. The Justice Department and FBI took action in December after obtaining court approval to dismantle a botnet, or network of hacked devices, consisting of small office and home office, or SOHO, routers. Mostly from Cisco or Netgear, the routers were vulnerable because they had reached their so-called end-of-life, meaning they were no longer receiving routine security updates from the manufacturers. Yet **there was no mention of the compromised Chinese transformers**.

National security concerns at U.S. ports are increasing as Congress investigates potential espionage and disruption risks presented by Chinese-built cargo cranes. An eight-month probe into the deployment of the cranes at the ports found communications equipment including cellular modems that could be remotely accessed, says the House Committee on Homeland Security and the Select Committee on the Strategic Competition between the United States and the Chinese Communist Party (CCP).

More than a dozen cellular modems were found on crane components in use at one U.S. port, and another modem was found inside another port's server room that houses cranes' firewall and networking equipment, according to a report from the Wall Street Journal. An unnamed aide of the House Homeland Security Committee told the WSJ some of the modems had active connections to operational components to the cranes.

Cranes can often be controlled remotely, meaning hackers with access to the cranes' networks could collect intelligence from ports or, in theory, even cause disruptions of equipment.

The Biden administration plans to invest billions in the domestic manufacturing of cargo cranes, seeking to counter fears that the prevalent use of China-built cranes with advanced software at many U.S. ports poses a potential national-security risk. In 2021, three of the largest port cranes in North America arrived at the Port of Oakland from China. This did not appear to be a problem to PG&E even though the Biden administration's actions follow a Wall Street Journal investigation last year that revealed fears that giant cranes made by a Chinese, state-owned company in use at a number of America's ports could present an espionage and disruption risk. Cranes at some ports used by the US military were flagged as surveillance threats. Officials also raised the concern that the software on the cranes could be manipulated by China to impede shipping or, worse, disrupt or damage the operation of the crane. "By design these cranes may be controlled, serviced and programmed from remote locations," said Rear Admiral John Vann, who leads the Coast Guard cyber command, during a press briefing. "These features potentially leave Chinese-

manufactured cranes vulnerable to exploitation," he said. There was no mention of the potential impact on the electric grids that supply power to the ports including Chinese port equipment that can be a trusted backdoor back into the electric grid.

Despite these alarming words, **U.S. electric utilities continue to make the US grid more vulnerable by using critical Chinese-made equipment and the US government continues to focus on network vulnerabilities which is not what the Chinese are targeting**. Just like the Chinese transformers, the Chinese cranes are comparably well-made and inexpensive and account for nearly 80% of ship-to-shore cranes in use at US ports.

U.K. is taking action

The U.K. appears to be concerned about China's efforts to cyberattack critical infrastructure. As a result, **Britain's National Grid has started removing Chinese components from their electricity transmission network over cyber security fears**. In 2015 French state-owned nuclear giant EDF announced that it had agreed to develop the Sizewell C nuclear plant with China General Nuclear Power Group (CGN). But over the years, increasing tensions between London and Beijing finally led to the Government deciding it did not want a Chinese company involved in one of the U.K.'s biggest infrastructure projects and bought out CGN. Why aren't U.S. utilities removing Chinese components from our grids?

Australia is starting to move

Australia also has Chinese-made transformers and is similarly concerned. Cybersecurity standards for solar inverters, batteries and electric vehicle chargers are being developed by the Australian government amid concerns some equipment could leave the nation exposed to foreign interference particularly equipment from Chinese manufacturers. The questions came **months after a report from the Cyber Security Co-Operative Research Centre warned internet-connected devices, including solar inverters, could introduce security vulnerabilities if not correctly regulated**. But federal energy department told the committee the government had established a dedicated division to look at "security issues associated with distributed energy resources" including rooftop solar technology, EV chargers, and large batteries, and would develop a set of safety standards to regulate their use. "We have providers, including Huawei, which were banned from the NBN, our 4G and 5G networks, who are finding a back way into providing, not just services to the broader economy and presumably critical infrastructure providers, but also federal government services". The questions came after the report by the Cyber Security Co-operative Research Centre in August last year identified potential issues with internet-of-things devices, "notably photovoltaic inverters". Why didn't DOE and NARUC address the use of Chinese inverters in their February 2024 report?

What needs to be done

The utility industry cyber security efforts have not been useful to address the threat from Chinese-made equipment. Assume all Chinese equipment is compromised and, per Executive Order 13920, that the Chinese equipment have bypassed network cyber security protections. Given this, there are three general near-term categories and one long-term that need to be addressed.

Policies: The Software Bill of Material (SBOM) approach doesn't work with the Chinese where you can't trust the vendor. Acceptance testing at the vendor and on-site becomes critical (site acceptance testing is how the hardware backdoors in the Ault transformer were found). The NERC Supply Chain Criteria and NERC CIP scope doesn't include control system field devices and must be expanded to include all control system devices. The NERC requirements for identifying and disclosing cyber incidents are inadequate as NERC CIP-008-6 defines a cyber incident as only affecting bulk electric systems and only of the electronic security perimeter. Consequently, control system field devices and electric distribution, which provide power to the port cranes, are not addressed. This obviously must be changed. Modify procurement specifications to preclude use of Chinese hardware, software, or component parts.

Control system cyber security training: Power plant and substation engineers generally are not required to take control system cyber security training. OT network security personnel generally are not required to take an introduction to system and power plant operation. Neither engineers nor network security personnel have training to identify control system cyber incidents such as the cellular modems in port cranes or the hardware backdoors in Chinese transformers. Provide specific control system cyber security training to the engineers and network security personnel to identify any anomalous process conditions and how to recognize control system cyber incidents. This training needs to be from control system (not OT) cyber security experts knowledgeable in the field (there are very few which is a problem in itself).

Field Actions: Disconnect all remote access to Chinese-made equipment and do not allow Chinese personnel on-site support of the equipment. Understand the scope of the problem by developing a detailed compilation of all Chinese-made equipment in US electric systems. Monitor process sensors at the physics level to know if the signals to equipment such as transformers are being spoofed.

Long term: Reestablish US manufacturing capability and associated trained workforce for all equipment used in power generation and the grid.

Summary

Chinese transformers, cranes, inverters, process sensors, etc. are comparably well-made and inexpensive leading to their continued use in U.S. critical infrastructures. Despite warnings from the U.S., U.K., and Australian governments about their use, the U.S. utility sector continues to ignore the cyber threat from Chinese equipment. Moreover, the U.S. government and private industry continue to focus on network vulnerabilities to the exclusion of hardware issues that can cause long term physical damage. Why aren't U.S. utilities removing Chinese components from our grids?

TESTIMONY -- HB24-1246 Electric Grid Resilience Temporary Carbon DioxideRegulation

by John Spence, Director of the Colorado EMP Task Force on National and Homeland Security

I am in favor of HB24-1246 for many reasons and especially the provisions that pertain to protecting the Colorado electric grid from an Electromagnetic Pulse such as from a GeoMagnetic Disturbance (GMD). A severe GMD (solar storm) would likely result in a long term power outage that would have catastrophic consequences on our population from lack of food, clean water, sewage treatment, medicine, transportation, etc. **Chaos would result!**

This type of severe weather event happened before with the **Carrington Event (Sept. 1, 1859).** Telegraph capabilities were destroyed. However, **this size solar storm would have destroyed much of our electric grid if it were to happen today.** According to the Space Weather Prediction Center at the the National Oceanic and Atmospheric Administration in Boulder, we are at a solar maximum where the risk of severe solar activity is very high. Scientists predict that major storm disturbances occur with a frequency of one every 150 years so **another solar superstorm is overdue!**

NOAA FORECASTS QUICKER, STRONGER PEAK OF SOLAR ACTIVITY