UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Complaint of Michael Mabee	**)**	
Related to Critical Infrastructure	**)**	**Docket No. EL20-46-000**
Protection Reliability Standards	**)**	

Motion of Complainant Requesting FERC Take Official Notice

Submitted to FERC on June 5, 2020

I am a private citizen who conducts public interest research on the security of the electric grid. I am also the Complainant in this docket.

I request that the Commission take official notice of two press reports related to supply chain cybersecurity which are relevant to this docket.

The first, "China and America's 400-ton electric albatross"[1] (attached as Exhibit A) quotes Charles Durant, deputy director of counterintelligence at the Department of Energy, who notes that: "There have been over 200 Chinese transformers that have come into the U.S. energy sector in the last 10 years."

The second, "U.S. Seizure of Chinese-Built Transformer Raises Specter of Closer Scrutiny"[2] (attached as Exhibit B) describes a recent instance of a Chinese transformer bound for a substation that supplies Denver Colorado being seized by the federal government, presumably over cybersecurity concerns.

These two reports support the necessity to order the Electric Reliability Organization ("ERO") to correct deficiencies in CIP-013-1 (Cyber Security Supply Chain Risk Management).

Respectfully submitted,

Michael Mabee

---

[1] Blake Sobczak and Peter Behr. E&E News. "China and America's 400-ton electric albatross." April 25, 2019. https://www.eenews.net/stories/1060216451/ (accessed June 5, 2020).

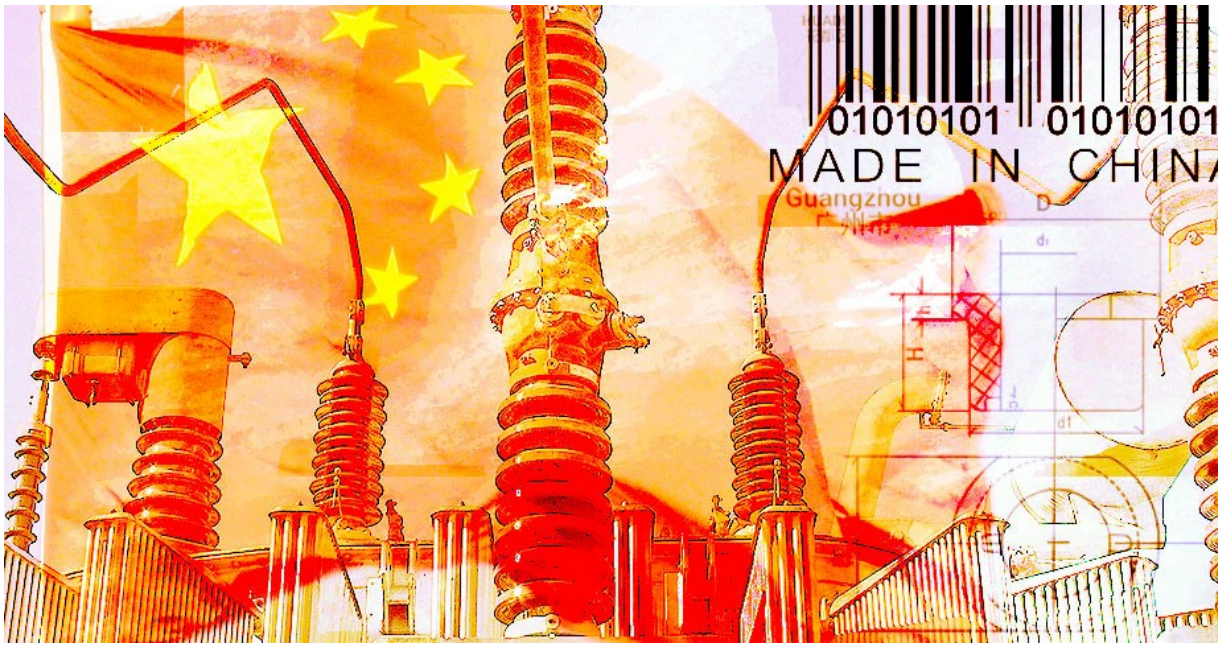
[2] Rebecca Smith. The Wall Street Journal. "U.S. Seizure of Chinese-Built Transformer Raises Specter of Closer Scrutiny." May 27, 2020. https://www.wsj.com/articles/u-s-seizure-of-chinese-built-transformer-raises-specter-of-closer-scrutiny-11590598710 (accessed June 5, 2020).

Exhibit A
To June 5, 2020 Motion
In Docket No. EL20-46-000
Submitted by Michael Mabee

SECURITY

China and America's 400-ton electric albatross

Blake Sobczak and Peter Behr, E&E News reporters • Energywire: Thursday, April 25, 2019



Claudine Hellmuth/E&E News(illustration); Daderot/Wikipedia(flag); Federico Candoni/Flickr (transformer bushings); Library of Congress (diagram)

The White House has blacklisted the Chinese telecommunications companies that dominate the market for 5G wireless systems.

For months, Trump administration officials have hopscotched across Europe to warn governments that China's telecom giants are duplicitous and their real aim is to spy on the West.

But one layer under the high-profile U.S.-China telecom fight are concerns about other core technology that rolls off China's factory lots. In the U.S. energy sector, China's emergence as a maker of large power transformers has grabbed the attention of industry executives and U.S. officials. Transformers are the backbone of America's power grid.

"There have been over 200 Chinese transformers that have come into the U.S. energy sector in the last 10 years," said Charles Durant, deputy director of counterintelligence at the Department of Energy. "Before that, there were zero."

Karen Evans, DOE's assistant secretary for cybersecurity, energy security and emergency response, said her office is looking at the supply-chain threat posed by transformers. "We know the risk associated with that," she said.

Yet against the backdrop of a U.S.-China trade war, security experts rush to separate fact from fiction when scrutinizing a vital grid component often sourced outside U.S. borders.

In a global economy, Durant pointed out, any transformer manufacturer could be sourcing parts from China. "The rules say you have to go to the lowest bidder," he said. "Most transformers come from overseas."

Severe disruptions

Electricity flows out of step-up transformers at the high-voltage levels needed to move power over long-distance lines. Then transformers on the other end step down the voltage for delivery to homes and businesses.

They're the electrical equivalent of on- and off-ramps to major highways.

Security planning for the power grid has centered on threats to the approximately 2,000 extra high-voltage transformers that carry 345 kilovolts of power or more, since these units — often containing several hundred tons of steel, copper and aluminum — cannot easily be replaced.

"Without sufficient spares or timely access to replacements, the loss of large power transformers can result in severe disruptions for long periods of time," said Ken Collison, vice president of energy consulting at ICF.

About 85 percent of new utility transformer orders have come from abroad in the past decade. Since 2010, domestic production has increased, but DOE reported in 2017 that only one U.S. manufacturer produced the special-grade electrical steel required for transformer cores.

In 2010, JiangSu HuaPeng Transformer Co. delivered a 345-kilovolt large power transformer to a utility in Oklahoma, according to company marketing materials, teeing up a boomlet in U.S.-bound large power transformers, or LPTs. Just two years later, the Changzhou-based manufacturer boasted that it supported 10 percent of New York City's electricity load.

German conglomerate Siemens and Swiss manufacturing giant ABB Group are among the largest foreign transformer manufacturers to invest in factories in China.

"The actual iron core and copper coils [inside the transformers], I don't think the origin of that is any real concern," said Craig Stiegemeier, an ABB product manager for transformers. "ABB builds those in more than 50 countries around the world. There is nothing that inherently comes on the transformer that's at risk."

Instead, he indicated that components added to transformers such as digital monitoring devices and remote sensors could open the door to hacking. Such devices could monitor power loads, equipment temperature, oil levels or other vital signs.

"Most manufacturers have some kind of smart devices in the transformer so you can understand the condition of the equipment. If those devices are tampered with, it could have a significant cyber impact," Stiegemeier said.

For instance, a false alarm signaling the need for maintenance or replacement of a "smart" transformer could pose a hazard. So could manipulating "tap changers" that set voltage levels, or the temperature gauges that trigger fans, he said. A hacker could, at least in theory, cause a digitized transformer to overheat.

"Utilities are taking this really seriously," he said. "They are looking to the traceability of every component, potentially down to the chip level, to make sure they know what the origin of the component is."

Huawei tug-and-pull

Multiple sources in the utility industry confirmed the vetting process in place for multimillion-dollar pieces of equipment like high-voltage power transformers.

Power companies typically dispatch "expert witnesses" to manufacturing plants to monitor transformer production from the outset, and various parts of the transformer, from the tap changers to the stacked-pancake bushings, undergo rigorous testing before being installed in the grid.

"If that thing catches on fire, it'll require a foam truck or better to put it out," noted Patrick Miller, managing partner at Archer Energy Solutions. "The whole substation would likely burn. That creates a much bigger problem than just a bad transformer."

Unlike China's telecom giants Huawei and ZTE, where concerns over cyberespionage or "logic bombs" are paramount in U.S. national security circles, counterfeit or faulty parts are seen as the larger threat in power transformers.

"Transformer components are not typically sensitive; they do have sensors, pumps and fans that utilities use to monitor and maintain cooling," noted Chris Sistrunk, principal industrial control system consultant at cybersecurity firm FireEye. "If the transformer has manufacturing defects or is installed incorrectly and there is a failure, there's language in the contract to cover liability."

A deliberately faulty or booby-trapped component has yet to be uncovered in any Chinese equipment, whether in hardware or software. Still, U.S. national security officials say the potential for subversion is every bit as dangerous as more direct threats to supply chains.

Suspicion within the Trump administration and Congress about security risks tied to China's Huawei is a heavy burden for the company, said Paul Triolo, geotechnology practice leader at the Eurasia Group consultancy, during a recent podcast for the SupChina digital media site.

"Huawei is a global company, operating in 170 countries. If it became clear that Huawei was simply an arm of the Chinese government and was doing Beijing's bidding at every turn, then they wouldn't be able to operate as a global company," he said. "The problem here is that the company is forced to prove a negative; it's really difficult."

Chinese leaders are likely to make the case against trade protectionism and security concerns at the second Belt and Road Forum for International Cooperation, which kicks off this week in Beijing. Russian President Vladimir Putin, among other global leaders, is set to attend.

"All too often in this context, the security of a product or service, or the threat from a company that sells it, is debated as if the test is binary: whether there is proof, a 'smoking gun,' so to speak, that the company in question is currently breaking the law by, say, conducting illicit surveillance," said Adam Hickey, deputy assistant U.S. attorney general, at a recent telecom conference.

"But whether a company has a culture that promotes theft, dishonesty or obstruction of justice is just as relevant," he said. "It tells you how the company will behave when it suits its interests."

Twitter: **@BlakeSobczak** | Email: **bsobczak@eenews.net**

Exhibit B
To June 5, 2020 Motion
In Docket No. EL20-46-000
Submitted by Michael Mabee

THE WALL STREET JOURNAL.

◆ WSJ NEWS EXCLUSIVE

U.S. Seizure of Chinese-Built Transformer Raises Specter of Closer Scrutiny

Federal officials haven't said publicly why they sent the transformer to a national lab, but experts said the move signaled possible grid-security concerns

By Rebecca Smith

Updated May 27, 2020 3:07 pm ET

A Chinese transformer weighing more than 500,000 pounds arrived by ship at the Port of Houston last summer, en route to an electrical substation in Colorado that funnels electricity to Denver.

It never made it there.

Instead, federal officials commandeered the electrical transformer, built by closely held Jiangsu Huapeng Transformer Company, at the port and had it trucked under federal escort to Sandia National Laboratories in Albuquerque, N.M., according to people with knowledge of the matter.

What engineers at Sandia found still isn't publicly known, nor why it was seized. The laboratory, operated by Honeywell International Inc., is under contract with the U.S. Energy Department and tasked with solving national-security threats.

Mike Howard, chief executive of the Electric Power Research Institute, a utility-funded technical organization, said that the diversion of a huge, expensive transformer is so unusual—in his experience, unprecedented—that it suggests officials had significant security concerns.

It also raises questions about whether more interventions could be ahead as the federal government begins to enforce an executive order President Trump signed on May 1 that gives federal officials authority to block utilities from using gear sourced from companies deemed influenced or controlled by "foreign adversaries" of the U.S. While the order didn't identify these adversaries, it was widely seen as targeting primarily Russia and China.

Mr. Trump has used trade policy, including tariffs on Chinese goods, in his attempt to steer manufacturing back to the U.S. People familiar with these actions said the executive order is an extension of that effort, targeting growing imports of electrical equipment like large transformers from China.

The transformer was taken to a temporary storage yard in Houston in June 2019 while awaiting transport to Sandia National Laboratories in Albuquerque, N.M.

PHOTO: PORT OF HOUSTON

These current and former federal officials and lobbyists said the Trump administration wants to improve grid security with trade barriers against large Chinese transformers, over concerns that they could wind up at choke points in the grid or near important military bases.

Jim Cai, U.S. representative for Jiangsu Huapeng in San Jose, Calif., said that for months he didn't know where the enormous transformer had been hauled and learned it was taken to Sandia only when he was informed by The Wall Street Journal.

He said his company has "no intention of doing anything harmful to the U.S." and he wants an opportunity to clear his company's name. He said he hopes the U.S. government will disclose any concerns it had, so there can be an open dialogue and "transparency about what has happened."

SHARE YOUR THOUGHTS

Should U.S. authorities heighten scrutiny of technology and infrastructure components built overseas? Why or why not? Join the conversation below.

Sandia, the Energy Department and the utility that purchased the transformer all declined to answer questions. Other people, with more limited knowledge of the situation, said federal officials probably commandeered the transformer because they suspected its electronics had been secretly given malicious capabilities, possibly allowing a distant adversary to monitor or even disable it on command. But these people said they didn't know whether any such alterations were found.

Energy Secretary Dan Brouillette, in comments early this month about the executive order, mentioned concerns about the security of transformers, which are critical to electrical-grid functioning, but he didn't provide any specifics. The order gives him the power—in consultation with the directors of defense, national intelligence and other agencies—to prevent compromised gear from being installed in the nation's transmission system and to root out any gear that is already installed if deemed hazardous.

The transformer that wound up at Sandia originally was headed for the Ault substation, owned by the Western Area Power Administration, which helps direct electricity to Denver. WAPA, a federally owned utility, supplies wholesale electricity to dozens of utilities scattered across 15 states in the western and central U.S., giving it one of the biggest footprints of any utility in the country. WAPA declined to comment.

A satellite view of the Ault substation in Colorado, where the transformer was originally intended to go. The substation funnels electricity to Denver.

PHOTO: GOOGLE

Federal officials have long worried that foreign adversaries might hack into the utility computer networks that control power flows on transmission lines and cause blackouts.

However, transformers hadn't typically been seen as products that could be easily isolated and hacked. That is because they don't contain the software-based control systems that foreign actors could access. They are passive devices that increase or reduce voltages in switchyards, substations and on power poles according to the laws of physics.

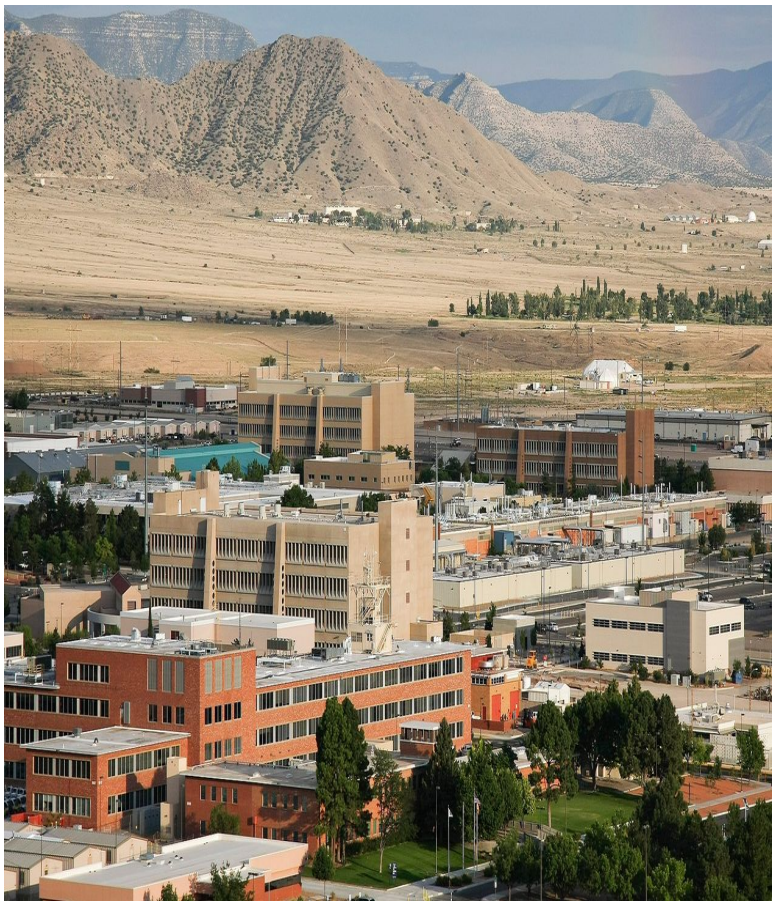
Modern units do contain diagnostic electronics, though, typically with one-way communications. In fact, this particular transformer was supposed to have diagnostic electronics allowing WAPA to keep track of its temperature and look for problems like dissolved gases, in its gigantic oil-filled tank, that could pose a fire risk.

Mr. Cai said that even if someone had access to the transformer's diagnostic data, it wouldn't matter. "You couldn't do anything," he said.

But the fear, other experts said, is that malicious electronics might get added surreptitiously and wouldn't be detected.

Tom Fanning, chief executive of Atlanta-based Southern Company, which owns several utilities in the Southeast, said transformers "have always been on the list of stuff we're worried about" because they are expensive and hard to replace and are custom-built for specific locations. He said there was a general awareness that a foreign entity might install something that could "potentially damage it on command," but he said he had never heard of an actual case.

Jiangsu Huapeng, also known as JSHP, says it has sold more than 7,000 power transformers globally in the past 20 years, including more than 100 big units to utilities in the U.S. and Canada in the past decade. In addition to WAPA, JSHP buyers include the New York Power Authority, EDF Renewables, B.C. Hydro and MidAmerican Energy Co.



The main campus of Sandia National Laboratories on Kirtland Air Force Base in Albuquerque, N.M., shown in 2009. The site is tasked with researching national-security threats.

PHOTO: SANDIA NATIONAL LABORATORIES VIA ASSOCIATED PRESS

Mr. Cai said the first hint of trouble came last June when WAPA abruptly changed the original $2.8 million contract for the 345/230 kV transformer. He said the utility said it didn't want JSHP to haul the unit to Colorado and do the installation. Nor did it want the five-year equipment warranty. Instead, it wanted a $400,000 credit for services not provided. "Something like that never happened before," said Mr. Cai.

He said he later heard from a port official that the transformer was taken to a federal facility, but didn't know which one. He said he assumed they intended to tear the transformer apart and "that is why they don't care about the warranty anymore."

He said he had no idea what authorities thought they might find since the transformer had been built to WAPA's exact specifications, down to the parts numbers for the electronics that were sourced from companies WAPA chose in the U.S. and U.K.

"They picked the brands, and we ordered and put it on," he said.

—Timothy Puko contributed to this article.

Corrections & Amplifications

Dan Brouillette is the U.S. secretary of energy, and Sandia National Laboratories is operated by Honeywell International. An earlier version of this article misspelled his surname as Brouilette and incorrectly said Sandia is owned by Honeywell. (Corrected on May 27)

Write to Rebecca Smith at rebecca.smith@wsj.com