UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Complaint of Michael Mabee and Petition	**)**	
to Order Mandatory Reliability Standards	**)**	**Docket No. _____**
for Equipment and Monitoring Systems	**)**	
Marketed from the People's Republic of China	**)**	

COMPLAINT AND PETITION
Submitted to FERC on August 26, 2021

Introduction

I am a private citizen who conducts public interest research on the security of the electric grid because I recognize the vital role of this infrastructure in powering every one of the nation's 16 critical infrastructures and in undergirding not just the well-being but the very survival of our modern society. I am also an electric utility ratepayer and would be adversely impacted by a failure of the Bulk Power System.

I am filing this complaint under 16 U.S. Code § 824o(d)(5)[1] because:

1) Entities in the U.S. Bulk Power System (BPS) as well as the overall U.S. electric grid are buying critical equipment from the People's Republic of China to install into our critical electric infrastructure that the Communist regime's state sponsored and state supported hackers are already probing and attacking.
2) There is no requirement that existing Chinese equipment or systems already installed in the electric grid be checked and tested for risks and vulnerabilities.
3) There is no requirement that newly imported Chinese equipment or systems be checked and tested for risks and vulnerabilities before being installed on the electric grid

Request for Investigation

I request that the Commission issue a public notice of this Complaint pursuant to 18 CFR § 385.206(d), investigate this Complaint and issue an appropriate order to the Electric Reliability Organization ("ERO") to strengthen the security of the bulk power system.

[1] "The Commission, upon its own motion ***or upon complaint***, may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section." [Emphasis added.]

Background

The Cyber Threat from China

On April 8, 2009 the Wall Street Journal reported[2]:

> Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.
>
> The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war.
>
> "The Chinese have attempted to map our infrastructure, such as the electrical grid," said a senior intelligence official. "So have the Russians."

In 2019 Daniel R. Coats, Director of National Intelligence (DNI) informed Congress[3] that:

> China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems… China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States.

On June 6, 2021 Secretary of Energy Jennifer Granholm confirmed in a CNN interview that U.S. adversaries have the capability to shut down our power grid.[4] And the following month, the U.S formally accused China of a campaign of cyber-attacks and indicted several Chinese nationals who conducted the hacks on behalf of the government of the People's Republic of China.[5]

The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency has been issuing alerts for years about China's cyber-attacks against the U.S including the energy sector and currently assesses[6]:

> The Chinese government—officially known as the People's Republic of China (PRC)—engages in malicious cyber activities to pursue its national interests. Malicious cyber activities attributed to the Chinese government targeted, and continue to target, a variety of industries and organizations in the United States, including healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and

---

[2] Wall Street Journal, "Electricity Grid in U.S. Penetrated By Spies." April 8, 2009. https://www.wsj.com/articles/SB123914805204099085

[3] "Worldwide Threat Assessment of the U.S. Intelligence Community." Before the Senate Select Committee on Intelligence. January 29, 2019. http://bit.ly/357Iakx

[4] See https://www.cnn.com/2021/06/06/politics/us-power-grid-jennifer-granholm-cnntv/index.html

[5] Steve Holland and Doina Chiacu. Reuters. "U.S. and allies accuse China of global hacking spree." July 20, 2021. https://www.reuters.com/technology/us-allies-accuse-china-global-cyber-hacking-campaign-2021-07-19/

[6] See: https://us-cert.cisa.gov/china

> aerospace), communications, IT (including managed service providers), international trade, education, video gaming, faith-based organizations, and law firms.

As far back as 2003, Congress expressed concern about China conducting "coordinated cyber reconnaissance" and "probing" U.S. electric utilities in a hearing entitled: "Implications of Power Blackouts for The Nation's Cybersecurity and Critical Infrastructure Protection."[7]

Alarmingly, despite almost two decades of knowledge that China is hacking the U.S. Energy sector, U.S electric utilities have been buying large transformers and other equipment from China to install in the U.S. electric grid.

An April 25, 2019 E&E News article titled "China and America's 400-ton electric albatross"[8] quoted a sobering statement from the U.S. Department of Energy:

> "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."

The U.S. Government Seizes a Chinese-Manufactured Transformer

On May 27, 2020, Wall Street Journal reporter Rebecca Smith reported that a large Chinese transformer purchased by the Western Area Power Authority (WAPA) from JiangSu HuaPeng Transformer Co., Ltd. (JSHP) was seized by the U.S. government at the Port of Houston in the summer of 2019. The transformer was taken to Sandia National Laboratories.[9] Nobody from the government would comment on the seizure.

In an interview on July 16, 2021 Latham Saddler, the former Director of Intelligence Programs at the National Security Council in the last administration, confirmed that after the Chinese transformer was taken to the National Lab "They found hardware that was put into that that had the ability for somebody in China to switch it off."[10]

One would think after finding a security issue in a Chinese-manufactured transformer in 2019 that by 2021 the U.S. would have addressed the threat.

One would be wrong.

---

[7] Implications of Power Blackouts for The Nation's Cybersecurity and Critical Infrastructure Protection, Before the US House, Joint Hearing of the Subcommittee on Cybersecurity, Science, and Research and Development, and the Subcommittee on Infrastructure and Border Security of the Select Committee on Homeland Security, (108th Congress) September 4 & 23, 2003. http://bit.ly/2qV9La3

[8] See: https://www.eenews.net/stories/1060216451/

[9] See: Wall Street Journal. "U.S. Seizure of Chinese-Built Transformer Raises Specter of Closer Scrutiny." May 27, 2020https://www.wsj.com/articles/u-s-seizure-of-chinese-built-transformer-raises-specter-of-closer-scrutiny-11590598710

[10] See: https://youtu.be/x0EawFC18MI

The U.S Continues to Import Large Transformers from China for the Electric Grid

According to U.S. International Trade Commission (USITC) data, the U.S. imported 66 Chinese large power transformers in 2020. 54 of these were classified as "having a power handling capacity exceeding 100,000 kVA."[11]

Since 2006, USITC data shows that the U.S. has imported 366 "liquid dielectric transformers having a power handling capacity exceeding 10,000 kVA" from China—294 of these have a power handling capacity exceeding 100,000 kVA.[12]

Figure 1:
Electrical transformers; liquid dielectric, having a power handling capacity exceeding **10,000** kVA:

Year	**USITC Data**
2020	66
2019	34
2018	24
2017	24
2016	32
2015	48
2014	47
2013	22
2012	19
2011	18
2010	10
2009	13
2008	6
2007	1
2006	2
2005	0
2004	0
2003	0
2002	0
2001	0
Total Over 10,000 kVA	**366**

[11] For details and underlying U.S. International Trade Commission data, see: https://michaelmabee.info/u-s-electric-grid-imports-more-chinese-transformers/
[12] Id.

Figure 2:
Electrical transformers; liquid dielectric, having a power handling capacity exceeding **100,000** kVA:

Year	**USITC Data**
2020	54
2019	25
2018	23
2017	22
2016	27
2015	47
2014	31
2013	10
2012	16
2011	15
2010	9
2009	11
2008	4
Total Over 100,000 kVA	**294**

A 2012 U.S. Department of Energy publication "Large Power Transformers and the U.S. Electric Grid"[13] contained a chart that separately showed power transformers imported from China exceeding 100,000 kVA. However, in the April 2014 Update[14] to this chart, the number of rows listing individual countries were reduced and China disappeared (falling into the "All Others" category). This publication has not been publicly updated since 2014.

Here are both charts:

[13] See: http://bit.ly/2rzi4IQ
[14] See: https://bit.ly/39tpBMO

Figure 3:
Department of Energy 2012 Chart

Table D2. Large Power Transformers Imports by Country, 2005–2011 (in quantity)

(Liquid dielectric transformers having a power-handling capacity exceeding 100,000 kVA)

Country	2005	2006	2007	2008	2009	2010	2011	Market Share 2011 (%)	Annual Growth (%) 2005–2011
	In Actual Units of Quantity								
Korea	82	77	123	160	180	223	204	40%	25%
Mexico	57	85	190	156	107	63	77	15%	6%
Austria	64	38	47	45	69	33	43	9%	-5%
Netherlands	24	21	21	33	22	30	40	8%	11%
Spain	3	2	5	0	0	14	29	6%	144%
Canada	56	36	34	34	44	43	26	5%	-9%
Germany	11	21	23	42	36	11	26	5%	23%
China	0	0	0	4	11	9	15	3%	N/A
Colombia	5	10	30	37	29	2	14	3%	30%
Brazil	9	17	27	25	37	12	13	3%	7%
Subtotal	311	307	500	536	535	440	487	96%	9%
All Others	52	30	28	23	75	61	18	4%	-11%
Total	**363**	**337**	**528**	**559**	**610**	**501**	**505**	**100%**	**7%**

Source: USITC Interactive Tariff and Trade DataWeb, http://dataweb.usitc.gov/scripts/user_set.asp, accessed June 5, 2012.

Figure 4:
Department of Energy 2014 Chart

Table C2. Large Power Transformer Imports by Country from 2005 to 2013 (by quantity)

(Liquid dielectric transformers having a power-handling capacity exceeding 100,000 kVA)

Country	2005	2006	2007	2008	2009	2010	2011	2012	2013	Market Share 2011-2013 (%)
	In Actual Units of Quantity									
Korea	82	77	123	160	180	223	204	142	76	29%
Mexico	57	85	190	156	107	63	77	97	162	23%
Canada	56	36	34	34	44	43	26	37	28	6%
Austria	64	38	47	45	69	33	43	76	59	12%
Netherlands	24	21	21	33	22	30	40	36	72	10%
Brazil	9	17	27	25	37	12	13	30	27	5%
Germany	11	21	23	42	36	11	26	16	9	3%
Subtotal	303	295	465	495	495	415	429	434	433	88%
All Others	60	42	63	64	115	86	76	38	63	12%
Total	**363**	**337**	**528**	**559**	**610**	**501**	**505**	**472**	**496**	**100%**

Source: USITC Interactive Tariff and Trade DataWeb, http://dataweb.usitc.gov/scripts/user_set.asp, accessed January 5, 2014.

Imports and orders of large Chinese transformers into the critical electric infrastructures continued in 2020 and 2021.

In August of 2021, a Chinese company, JiangSu HuaPeng Transformer Co., Ltd. (JSHP) posted on their website that "JSHP has been awarded to design, build, and supply of a 345KV 610MVA Step-up Power Transformer by a US comapny" [sic].[15]

Step-up transformers are a key component of the U.S. electric grid. Moreover, JSHP claims that their transformers handle 10% of the load of New York City and 20% of the load in Las Vegas, NV.[16]

JSHP also boasts of several recent U.S. orders and deliveries. In sum, evidence from the USITC and this Chinese manufacturer demonstrates that the U.S. electric grid continues to import large Chinese transformers in 2020 and 2021. Here are a few examples – screenshots straight from the JSHP's website – of U.S. imports of large Chinese transformers in 2020 and 2021:

Figure 5:
Screen Shot from JSHP Website, taken August 12, 2021

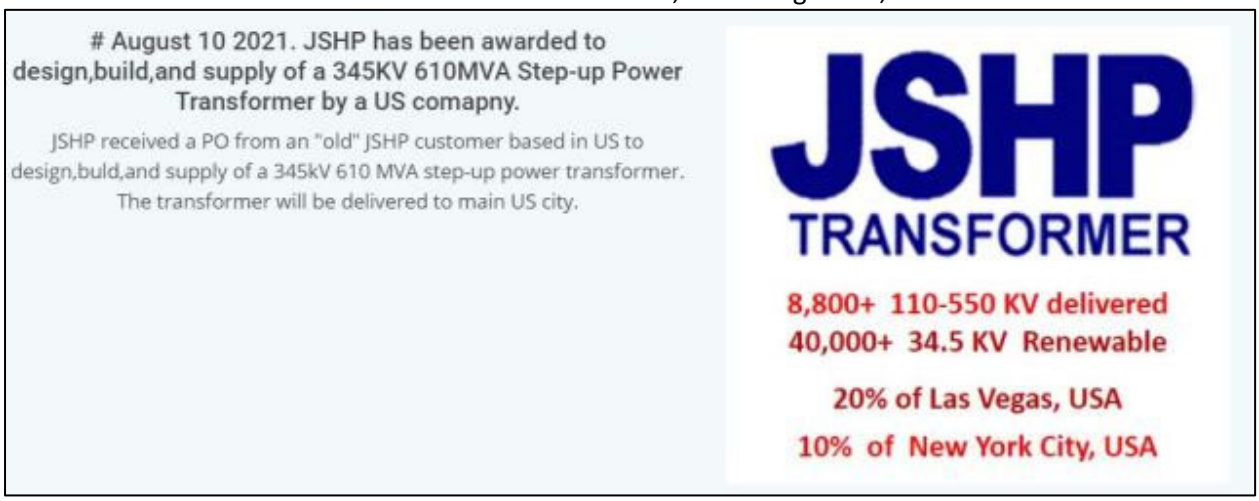
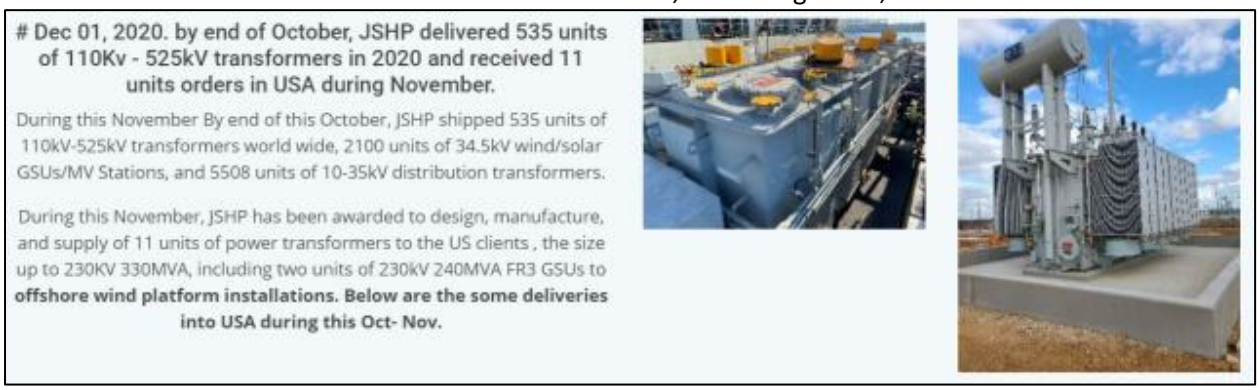


Figure 6:
Screen Shot from JSHP Website, taken August 12, 2021



[15] See: http://www.jshp.com/news.html
[16] Id.

Figure 7:
Screen Shot from JSHP Website, taken August 12, 2021

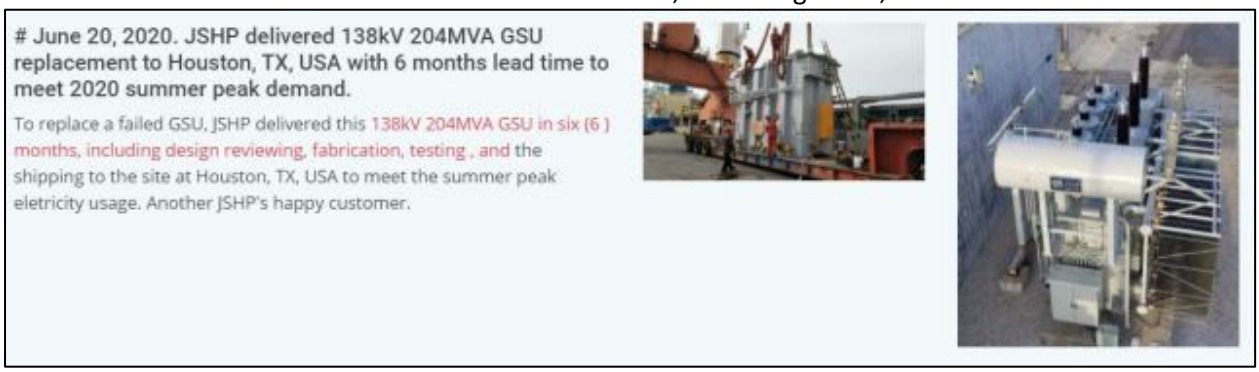
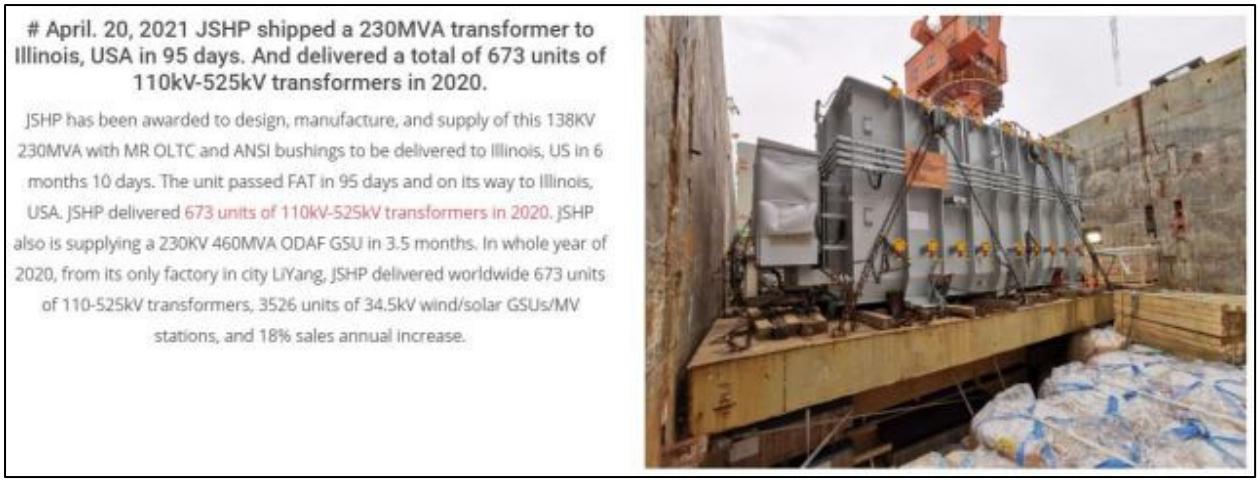


Figure 8:
Screen Shot from JSHP Website, taken August 12, 2021



Attached as Exhibit A is a partial listing of transformers and equipment imported from China that are believed to be installed in the U.S. Energy sector.

Attached as Exhibit B are numerous bills of lading for imported Chinese-manufactured transformers and components between 2018 to 2020.

None of the current mandatory reliability standards address risks and vulnerabilities to the Bulk Power System (and the electric grid in general) represented by the imports in Exhibits A and B.

A Direct Line to the Government of the People's Republic of China

Behind many of the U.S. imports of Chinese-manufactured transformers, other equipment and components is a company called Doubletree Systems, Inc. Doubletree Systems, Inc. also represents several other Chinese companies that sell transformers and other equipment imported for use in the

U.S. Critical Electric Infrastructure.[17] In addition, Doubletree sells grid security and monitoring systems and works with the Electric Power Research Institute (EPRI) on grid security issues.

There is evidence that the government of the People's Republic of China has an ownership and/or control interest in Doubletree Systems, Inc. This relationship is detailed below.

According to Doubletree Systems, Inc.'s successful contract bid to WAPA for a JSHP transformer obtained under the Freedom of Information Act (FOIA):[18]

> "Doubletree Systems, authorized by JSHP (see attached letter), acts as exclusively partner for JSHP in North America market, provides marketing and service support (pre-sale and warranty service) and so far, in about 8 years, with this partnership, there are over a hundred of JSHP power transformers are in operation in USA & Canada. The biggest one is a 345KV 610MVA transformer connected to Con Edison New York from the Bayonne Energy Center." [sic.]

Starting, for example, with JSHP which has sold hundreds of transformers in the U.S., what follows is the relationship to the government of the People's Republic of China, step-by step:

- JiangSu HuaPeng Transformer Co., Ltd., (who manufactured the transformer seized by the U.S. government), is located in the People's Republic of China.[19]
- JSHP Transformer USA Corporation was registered in California on December 5, 2008.
- JSHP Transformer USA Corporation is a U.S. subsidiary or close affiliate (and certainly an agent) of JiangSu HuaPeng Transformer Co., Ltd.[20]
- The CEO and "General Manager" of JSHP Transformer USA Corporation is "Yunqing (Jim) Cai."
- Another listed Officer of JSHP Transformer USA Corporation is Hongjin Qian, whose listed address is the same address in China as JiangSu HuaPeng Transformer Co., Ltd.
- Doubletree Systems, Inc. was registered in California on February 9, 2000.
- The CEO of Doubletree Systems, Inc. is "Jim Y Cai."
- The California address for Doubletree Systems, Inc. and JSHP Transformer USA Corporation is the same.
- Numerous documents I found on Doubletree's website identifies Doubletree Systems, Inc. as "A XJ Group Company."[21] (Xuji Group Co., Ltd. d.b.a XJ Group)

---

[17] In addition to JiangSu HuaPeng Transformer Co., Ltd. (JSHP), Doubletree is also listed as the U.S. office/contact or markets for Suzhou Porcelain Insulator Works Co., Ltd. (d.b.a. Suz Insulators); Ningbo Orient Wires & Cables Co., Ltd. (d.b.a. Orient Cables); Beijing Power Equipment Group; Nanjing Electric Group Co., Ltd. ("a Baiyun Power Group company"); TGC (parent: Jiansu Tongguang Electronic Wire & Cable Co. Ltd.); Henan Tong-Da Cable Co. Ltd. (d.b.a. TDDL Cable); Sieyuan Electric Co., Ltd.; Changshu Fengfan Power Equipment Co. Ltd. (d.b.a. CS Tower); China Electric Power Equipment and Technology Co., Ltd.; Jiangsu Shuanghui Power Development Co., Ltd., (d.b.a. JS Hardware); Liling Huaxin Insulator Technology Co., Ltd (d.b.a. HPK Insulators)

[18] Document available at: https://michaelmabee.info/wp-content/uploads/2021/08/WAPA-Doubletree-Systems-Bid-and-Contract.pdf

[19] See: http://www.jshp.com/index.html

[20] Note the same U.S. address on the JiangSu HuaPeng Transformer Co., Ltd. website and on the CA Secretary of State Statement of Information. There is also a letter of agency in the WAPA bid, available at: https://michaelmabee.info/wp-content/uploads/2021/08/WAPA-Doubletree-Systems-Bid-and-Contract.pdf

[21] See for example: http://www.dsius.com/lib/Library/2002418.pdf and http://www.dsius.com/lib/Library/XJ_Facticer_flyer.pdf and

- Another page on Doubletree's website states: "the XJ group and the China State Grid signed a 'Cooperation Structure agreement' through China Electric Power Research Institute. Based on the agreement, the China State Grid will acquire 100% share of the XJ group and will become the sole owner of the XJ group."[22]
- XJ Group's website says: "XJ Group Corporation, directly subordinate to SGCC [State Grid Corporation of China], is a high-tech modern industry group focused on electric power, automation and intelligent manufacturing."[23]
- State Grid Corporation of China [SGCC] is a state-owned corporation, owned by the government of the People's Republic of China.[24]
- Jim Cai's 'LinkedIn profile says he is a Director of "C-EPRI" (China Electric Power Research Institute) which is also part of State Grid Corporation of China[25]; President of Doubletree Systems, Inc.; and Manager of JSHP Transformer USA, Inc.[26]

Thus, we have clear connection from Doubletree Systems, Inc. → XJ Group → State Grid Corporation of China → government of the People's Republic of China.

All Chinese companies have an obligation under the 2017 Chinese National Intelligence Law[27] to "support, assist and cooperate with the state intelligence work." Moreover, under China's 2014 Counter-Espionage Law[28] a company may not refuse the Chinese government when asked for information. In fact, according Dr. Murray Scot Tanner's[29] Lawfare Institute analysis:

> "The Intelligence Law, by contrast, repeatedly obliges individuals, organizations, and institutions to assist Public Security and State Security officials in carrying out a wide array of 'intelligence' work. Article Seven stipulates that 'any organization or citizen shall support, assist, and cooperate with state intelligence work according to law.' Article 14, in turn, grants intelligence agencies authority to insist on this support: 'state intelligence work organs, when legally carrying forth intelligence work, may demand that concerned organs, organizations, or citizens provide needed support, assistance, and cooperation.' Organizations and citizens must also protect the secrecy of 'any state intelligence work secrets of which they are aware'."

Doubletree Systems, Inc. not only imports and markets Chinese-manufactured transformers and other equipment in the U.S., but is sells a variety of grid protection and monitoring products, which according to their promotional materials include:

- POLARIS (substation monitoring system)[30]

---

http://www.dsius.com/lib/Library/PMUTester_intro_OETD_Oct.pdf and
http://www.dsius.com/lib/Library/papers/WAMS_IEEE_2005.pdf

[22] See: http://www.dsius.com/lib/news.htm

[23] See: http://www.xjgc.com/html/xjen/col2015100652/column_2015100652_1.html. Also see: http://www.sgcc.com.cn/html/sgcc_main_en/col2017112321/column_2017112321_1.shtml

[24] See directory of the State-owned Assets Supervision and Administration Commission of the State Council: http://en.sasac.gov.cn/directory.html

[25] See: http://www.epri.sgcc.com.cn/html/eprien/index.html

[26] See: https://www.linkedin.com/in/jim-cai-5236089/

[27] See: https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense

[28] See: https://www.reuters.com/article/us-china-lawmaking-spy-idUSKBN0IL2N520141101

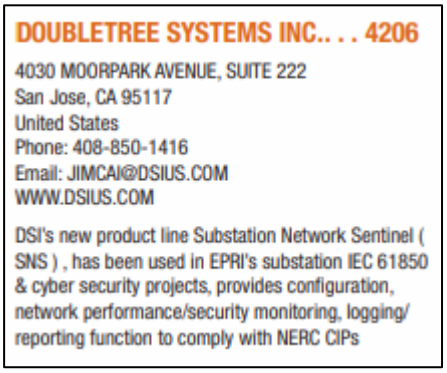
[29] See: https://www.uscc.gov/sites/default/files/Murray Scot Tanner_Bio.pdf

[30] See: http://www.dsius.com/lib/Library/POLARIS%20brochure.pdf

- SA200 (substation automation)[31]
- Substation Network Sentinel (SNS)[32]
- Wide Area Measurement System (WAMS).[33] According to Doubletree's website: "WAMS solution provided is field-proven in Bonneville of Power Administration of WSCC"[34] [35]
- Generator Testing & Model Validation. According to Doubletree's website: "The standard generator testing and model validation provided by Doubletree Systems, Inc. has extensive experience and has been certificated by Western Systems Coordinating Council (WSCC)."[36]
- A wide variety of XJ Group (SGCC) grid protection and monitoring products[37]
- Special Protection System (SPS)[38]
- Transfer Limits Monitoring[39]
- SCADA/EMS/DMS/DA consulting[40]

In a vendor listing for the 2015 DISTRIBUTECH Conference and Exhibition,[41] Doubletree held itself out as collaborating with EPRI to help the industry comply with NERC's Critical Infrastructure Protection (CIP) Standards through Doubletree's Substation Network Sentinel (SNS) product:

Figure 9



In other words, an entity owned or controlled by the People's Republic of China – which is hacking the U.S. energy sector – is also helping our electric grid "to comply with NERC CIPs." [North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards.]

In fact, in EPRI's write up on DISTRIBUTCH Conference and Exhibition in 2014[42], they noted:

---

[31] See: http://www.dsius.com/lib/Library/SA200%20Brochure.pdf
[32] See: http://www.dsius.com/lib/Library/dsi_SNS_flyer.pdf
[33] See: http://www.dsius.com/lib/Library/WAMS-brochure.pdf
[34] See: http://www.dsius.com/lib/wams/wams-1.htm
[35] See: http://www.dsius.com/lib/Library/papers/WAMS_IEEE_2005.pdf
[36] See: http://www.dsius.com/lib/wams/gen.htm
[37] See: http://www.dsius.com/lib/Library/XJ_Products_Brochures_En.pdf
[38] See: http://www.dsius.com/lib/Library/SPS-brochure.pdf
[39] See: http://www.dsius.com/lib/Library/Transferlimits-brochure.pdf
[40] See: https://www.electricnet.com/doc/doubletree-systems-inc-0001 and https://www.poweronline.com/doc/doubletree-systems-inc-0001
[41] See: https://digital.pennwell.com/pennwellevents/dtech_2015_showguide?pg=132#pg132 (Page 131 of the PDF file)
[42] See: https://smartgrid.epri.com/doc/EPRI%20DistribuTECH_Brief_Feb2014.pdf

> "Network Security: A kickoff meeting was held on the floor of DistribuTECH for a group of vendors currently interested in participating in the 'Protective Measures for Securing T&D Systems' project, which involves validating the mapping of IEC 62351-7 network security events. Vendors currently engaged in the project include SISCO, Ruggedcom, OSIsoft, Doubletree Systems, and Radiflow. Other vendors expressing interest include Cisco, Schneider Electric, and SEL. The project will be driven by use cases developed in early 2014 with proof-of concept implementations to be developed and demonstrated in the EPRI Cyber Security Research Lab throughout 2014." [Emphasis added.]

It is of great concern that the People's Republic of China (and its controlling Chinese Communist Party) is marketing equipment or systems to the same U.S. critical infrastructures that multiple U.S. government agencies have confirmed – for years – are the target of China's past and present cyberespionage, probing, and cyberattacks.

This raises security concerns. But there are no U.S. government requirements or mandatory reliability standards that such equipment or systems be checked.

In sum, it appears that not only are we importing transformers from China, we may be employing grid monitoring systems that have a direct tie to the People's Republic of China.

Conclusions

1) Entities in the U.S. Bulk Power System (BPS) as well as the overall U.S. electric grid are buying critical equipment from the People's Republic of China to install into our critical electric infrastructure that the Communist regime's state sponsored and state supported hackers are already probing and attacking.
2) There is no requirement that existing Chinese equipment or systems already installed in the electric grid be checked and tested for risks and vulnerabilities.
3) There is no requirement that newly imported Chinese equipment or systems be checked and tested for risks and vulnerabilities before being installed on the electric grid.

"The Commission, upon its own motion ***or upon complaint***, may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section."[43] [Emphasis added.]

The Commission must use its authority to order mandatory reliability standards to address the risks and vulnerabilities presented by the import and installation of equipment or systems originating from adversaries of the U.S., including China.

[43] 16 U.S. Code § 824o(d)(5)

Relief Sought

1. The Federal Energy Regulatory Commission should direct the North American Electric Reliability Corporation (NERC) to conduct a comprehensive survey of all registered entities in the Bulk Power System to determine what Chinese equipment or systems are currently in use in the Bulk Power System.

2. The Federal Energy Regulatory Commission should direct the North American Electric Reliability Corporation (NERC) to submit to the Commission a proposed reliability standard for testing and security of Chinese equipment or systems are currently in use in the Bulk Power System or purchased for future use.

3. The Federal Energy Regulatory Commission should work with all State Public Utility Commissions to encourage adoption of the reliability standard promulgated as a result of #2 above (or a state equivalent standard) for the protection of generation and distribution portions of the electric grid under state jurisdiction.

Respectfully submitted,

Michael Mabee

Attachments: 18 CFR § 385.206 Compliance Information
Draft Notice
Exhibits A & B

18 CFR § 385.206 Compliance Information

I Michael Mabee, hereby state the following:

18 CFR § 385.206(b) Contents. A complaint must:
(1) Clearly identify the action or inaction which is alleged to violate applicable statutory standards or regulatory requirements;

- The threat to reliability posed by equipment or systems being imported and installed in the Bulk Power System sourced from a U.S. adversary with a history of hacking the electric grid is not addressed in existing reliability standards.

(2) Explain how the action or inaction violates applicable statutory standards or regulatory requirements;

- The threat to reliability posed by equipment or systems being imported and installed in the Bulk Power System sourced from a U.S. adversary with a history of hacking the electric grid is not addressed in existing reliability standards.

(3) Set forth the business, commercial, economic or other issues presented by the action or inaction as such relate to or affect the complainant;

- The threat to reliability posed by equipment or systems being imported and installed in the Bulk Power System sourced from a U.S. adversary with a history of hacking the electric grid is not addressed in existing reliability standards.

(4) Make a good faith effort to quantify the financial impact or burden (if any) created for the complainant as a result of the action or inaction;

- As an electric ratepayer, a widespread power outage due to a cyber-attack from China, facilitated by equipment or systems we have imported from China would have a devastating impact on me and my family and on the economy on which we depend.
- As an example, the widespread power outage in Texas on February 15, 2021 caused the loss of life (at least 210 deaths) and tens of billions of dollars in damage to the economy.
- A widespread power outage due to a cyber-attack from China, facilitated by equipment or systems we have imported from China would have a devastating impact on the U.S. economy as well as substantial loss of life.

(5) Indicate the practical, operational, or other nonfinancial impacts imposed as a result of the action or inaction, including, where applicable, the environmental, safety or reliability impacts of the action or inaction;

- A widespread power outage due to a cyber-attack from China, facilitated by equipment or systems we have imported from China would have a devastating impact on the U.S. economy as well as substantial loss of life and impact to the environment. For example, major wastewater treatment plants might cease to function.

(6) State whether the issues presented are pending in an existing Commission proceeding or a proceeding in any other forum in which the complainant is a party, and if so, provide an explanation why timely resolution cannot be achieved in that forum;

- I am unaware of any public FERC docket which addresses the threats presented by the import of Chinese equipment or systems into the Bulk Power System.

(7) State the specific relief or remedy requested, including any request for stay or extension of time, and the basis for that relief;

- Contained in "Relief Sought" section of Complaint.

(8) Include all documents that support the facts in the complaint in possession of, or otherwise attainable by, the complainant, including, but not limited to, contracts and affidavits;

- Attached as exhibits to the Complaint

(9) State

(i) Whether the Enforcement Hotline, Dispute Resolution Service, tariff-based dispute resolution mechanisms, or other informal dispute resolution procedures were used, or why these procedures were not used;

- N/A

(ii) Whether the complainant believes that alternative dispute resolution (ADR) under the Commission's supervision could successfully resolve the complaint;

- N/A

(iii) What types of ADR procedures could be used; and

- N/A

(iv) Any process that has been agreed on for resolving the complaint.

- N/A

(10) Include a form of notice of the complaint suitable for publication in the Federal Register in accordance with the specifications in § 385.203(d) of this part. The form of notice shall be on electronic media as specified by the Secretary.

- Draft Notice Attached

(11) Explain with respect to requests for Fast Track processing pursuant to section 385.206(h), why the standard processes will not be adequate for expeditiously resolving the complaint.

- N/A

18 CFR § 385.206(c) Service. Any person filing a complaint must serve a copy of the complaint on the respondent, affected regulatory agencies, and others the complainant reasonably knows may be expected to be affected by the complaint. Service must be simultaneous with filing at the Commission for respondents. Simultaneous or overnight service is permissible for other affected entities. Simultaneous service can be accomplished by electronic mail in accordance with § 385.2010(f)(3), facsimile, express delivery, or messenger.

- A copy of this Complaint will be sent electronically to the North American Electric Reliability Corporation (NERC) simultaneously with my filing with the Commission.

Respectfully submitted,

Michael Mabee

Draft Notice

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Complaint of Michael Mabee and Petition	)	
to Order Mandatory Reliability Standards	)	Docket No. _____
for Equipment and Monitoring Systems	)	
Marketed from the People's Republic of China	)	

NOTICE OF COMPLAINT

( )

Take notice that on [date filed], pursuant to section 215(d) of the Federal Power Act, 16 U.S.C. 824o(d) and Rule 206 of the Federal Energy Regulatory Commission's (Commission) Rules of Practice and Procedure, 18 CFR 385.206 (2019), Michael Mabee, (Complainant) filed a formal complaint alleging: 1) Entities in the U.S. Bulk Power System (BPS) as well as the overall U.S. electric grid are buying critical equipment from the People's Republic of China to install into our critical electric infrastructure that the Communist regime's state sponsored and state supported hackers are already probing and attacking; 2) There is no requirement that existing Chinese equipment or systems already installed in the electric grid be checked and tested for risks and vulnerabilities; and 3) There is no requirement that newly imported Chinese equipment or systems be checked and tested for risks and vulnerabilities before being installed on the electric grid.

Complainant certifies that copies of the complaint were served on the contacts as listed on the Commission's list of Corporate Officials.

Any person desiring to intervene or to protest this filing must file in accordance with Rules 211 and 214 of the Commission's Rules of Practice and Procedure (18 CFR 385.211 and 385.214). Protests will be considered by the Commission in determining the appropriate action to be taken but will not serve to make protestants parties to the proceeding. Any person wishing to become a party must file a notice of intervention or motion to intervene, as appropriate. The Respondent's answer and all interventions, or protests must be filed on or before the comment date. The Respondent's answer, motions to intervene, and protests must be served on the Complainants.

The Commission encourages electronic submission of protests and interventions in

lieu of paper using the "eFiling" link at http://www.ferc.gov. Persons unable to file electronically should submit an original and 5 copies of the protest or intervention to the Federal Energy Regulatory Commission, 888 First Street, NE, Washington, DC 20426.

This filing is accessible on-line at http://www.ferc.gov, using the "eLibrary" link and is available for review in the Commission's Public Reference Room in Washington, DC. There is an "eSubscription" link on the web site that enables subscribers to receive email notification when a document is added to a subscribed docket(s). For assistance with any FERC Online service, please email FERCOnlineSupport@ferc.gov, or call (866) 208-3676 (toll free). For TTY, call (202) 502-8659.

Comment Date: 5:00 pm Eastern Time on (insert date).

Kimberly D. Bose,
Secretary.