UNITED STATES OF AMERICA
BEFORE THE
U.S. DEPARTMENT OF ENERGY

Request for Information (RFI) on Ensuring	**)**	
the Continued Security of the United States	**)**	**86 Fed. Reg. 21,309**
Critical Electric Infrastructure	**)**	**April 22, 2021**

Comments and Recommendations of Michael Mabee on
Security of the U.S. Critical Electric Infrastructure
Submitted to DOE on June 4, 2021

Introduction

I am a private citizen who, for over a decade, has conducted public interest research on the security of the electric grid because I recognize the absolutely 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 country. I am a retired U.S. Army Command Sergeant Major, and I maintain one of the world's most comprehensive grid security databases as an unpaid volunteer grid security researcher.[1] I have been quoted by the Wall Street Journal, the Washington Post and many other publications on grid security and have intervened and submitted testimony in over 200 federal dockets on electric grid security issues.

The Department of Energy needs to keep in mind that everybody filing in this RFI has an agenda. My agenda is that I took an oath to "support and defend the Constitution of the United States against all enemies, foreign and domestic." This is the same oath taken by every uniformed and civilian employee of the United States government, including those at the Department of Energy.

The electric utility industry also has an agenda which is not necessarily the same agenda as the United States government.

The Department of Energy's Responsibility to Secure the Critical Electric Infrastructure

The preamble of the U.S. Constitution gives the federal government the responsibility to "provide for the common defense." On February 12, 2013, President Barack Obama implemented Presidential Policy Directive 21 (PPD-21)[2] – Critical Infrastructure Security and Resilience. PPD-21 identifies the 16 critical infrastructures in the U.S. and mandates that:

[1] Available at: https://michaelmabee.info/government-documents-emp-and-grid-security/
[2] Available at: http://bit.ly/2NUr04k

> The Federal Government shall work with critical infrastructure owners and operators and SLTT [state, local, tribal, and territorial] entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof.

PPD-21 identifies the energy sector as uniquely critical due to the enabling functions it provides across all 16 critical infrastructure sectors. The electric grid is the lynchpin: All 16 critical infrastructures, including the rest of the energy sector and our national security apparatus, depends on the electric grid. Therefore, any threat to the electric grid is a threat to U.S. national security. The Department of Energy is designated as the Sector Risk Management Agency for the energy sector.[3]

The North American electric grid is an amazing human accomplishment. It is the largest machine in the history of the world, built piece by piece over many generations. This machine is literally the life support system for the United States.

The entire electric grid must be secured – not just part of it. The "electric grid" is actually thousands of entities, both public and private sector, that operate in an interconnected system to facilitate the generation, transmission and distribution of electrical power. The grid is made up of power generation—such as nuclear, coal and gas-fired power plants, hydroelectric facilities, wind turbines and solar farms, high voltage transmission lines that span long distances across the country and local distribution lines which bring the power to our homes and businesses.

This interconnected—and vulnerable—patchwork is what allows the United States to support her human population. Everything that enables 330 million people in the country to survive is wholly reliant on the electric grid. All of our critical infrastructures, including food, water, fuel, transportation, financial, communications, medical systems and our national defense infrastructure, are all completely dependent on the electric grid. This cannot be overemphasized: *Our national security is dependent on the electric grid.*

As we know from the recent Colonial Pipeline and SolarWinds cyberattacks, the energy sector is targeted by state adversaries and criminals. And as we know from the Texas grid collapse in February of 2021, even extreme weather threatens the grid. We have known about the many vulnerabilities and threats to the critical electric infrastructure and the energy sector for decades.

There are four major challenges to securing the critical electric infrastructure. I will briefly outline each below and provide recommendations. The U.S. Department of Energy must provide extraordinary leadership in order for the U.S. to overcome these challenges.

---

[3] See: https://www.cisa.gov/energy-sector

A dysfunctional regulatory bureaucracy continues to buy the electric industry's bill of goods.

1. The first challenge is the mind-numbingly complex regulatory structure of the electric grid.

There are few mandatory standards in place for the protection of the critical electric infrastructure. The few that do exist *do not apply* to the entire electric grid, just small portions of it. And these few existing standards are insufficient. On the issue of security, some of the grid is self-regulated. Other parts have no mandatory security requirements whatsoever. The federal government under current law does not have clear authority to mandate that the electric grid adopt measures to protect itself from threats.

The North American Electric Reliability Corporation (NERC) is a not-for-profit corporation that acts as the self-regulatory organization "whose mission is to assure the reliability of the bulk power system (BPS) in North America." The Federal Energy Regulatory Commission (FERC) is an independent federal agency that regulates the interstate transmission of electricity, natural gas, and oil. FERC's specific authority over the electric grid is to "oversee the reliability of the bulk power system." The few mandatory reliability standards and "Critical Infrastructure Protection" (CIP) standards that do exist are written by the electric utility industry and, due to the myriad of exemptions written into the standards, apply *only to certain parts* of the bulk power system.

The bulk power system consists of approximately 1,500 entities operating at 100 kilovolts or higher which are regulated by NERC, overseen by FERC. However, the bulk power system does not include power generation or distribution to end-users. Generation and distribution are under the jurisdiction of state public utility commissions (PUCs). This means that there are over 60 state and federal government agencies as well as a number of non-profit corporations involved in the regulation of the electric grid. Unbelievably, there is literally no government authority over the security of the electric grid unless an individual state enacts a mandate on its own. Most have no such state mandates.

The Kleinman Center for Energy Policy charitably said: "Today's electric grid is developing within the confines of a century-old regulatory system."[4] Put more bluntly, the regulatory regime, built over generations like the grid itself, most closely resembles a Rube Goldberg cartoon. From a security standpoint, it is cumbersome, slow, bureaucratic and inefficient. Our decades-long inability to secure the critical electric infrastructure through the existing regulatory regime will continue to put the country in danger.

Since protection of the critical electric infrastructure is imperative for national security, we simply cannot use the current regulatory morass to get the job done. The United States must mandate the protection of the critical electric infrastructure – whether public or private sector. We do not have years or decades to allow protection to soak in or move through osmosis. Protecting the critical electric infrastructure requires immediate and mandatory actions – and accountability for violators.

---

[4] Peskoe, Ari. Kleinman Center for Energy Policy. "Power Over the Twenty-First Century Electric Grid." April 10, 2018. https://kleinmanenergy.upenn.edu/research/publications/power-over-the-twenty-first-century-electric-grid/

We have known for decades that the critical electric infrastructure is vulnerable to threats, yet little has been done. For example, in 1981 – over 40 years ago – the General Accounting Office (now the Government Accountability Office, or GAO) issued a report titled: "Federal Electrical Emergency Preparedness Is Inadequate."[5] GAO noted:

> If saboteurs, terrorists, or an enemy attacked the Nation's electric power system, would the Federal Government be prepared to handle the resulting energy disruptions?
>
> Probably not, because the Department of Energy has failed to prepare required electric emergency preparedness plans. A national plan to cope with the problems caused by a loss of electricity–which would virtually halt communication, transportation, and distribution systems–is essential, because utilities and the States cannot be expected to deal with such emergencies on their own.

The 1981 report further noted:

> The consequences of such a power outage are staggering. Electric power is essential to maintaining the Nation's military readiness. Without adequate or reliable power, most industrial activity would be disrupted. Power outages can disrupt the operation of computers, commercial business, water and sewage treatment plants, mass transit and traffic control systems, as well as many other aspects of life.
>
> In the United States, electric power is generated by some 3,500 utility companies, sent over thousands of miles of high voltage transmission lines, and distributed over low voltage feeder lines to end users. The system is a highly complex, interconnected industry network covering the United States and parts of Canada.
>
> Electric power systems are highly dependable, but are very vulnerable to disruptions from acts of war, sabotage, or terrorism. In the region GAO looked at:
>
> - An attack on just eight substations could disrupt power to the entire region for a long time. (See p. 8.)
> - Damage to just four substations could disrupt power to one city for up to a year. (See p. 8.)
> - Damage to just one substation could leave a key military facility without power. (See p. 8.)

What is most shocking about this 1981 GAO report is that in 2021 there is still no physical security requirement for most of the critical electric infrastructure. The one NERC standard that exists, CIP-14-2, exempts generation facilities, does not apply to distribution and applies to very few facilities in the bulk power system. Moreover, there have been 721 physical attacks against the critical electric infrastructure since 2010.[6] In sum, in 2021 there are still no meaningful physical security requirements for the electric grid.[7]

---

[5] General Accounting Office (GAO). "Federal Electrical Emergency Preparedness Is Inadequate." EMD-81-50. May 12, 1981. http://bit.ly/354ZN4i

[6] See OE-417 data and analysis at: https://michaelmabee.info/oe-417-database/

[7] Attached as Exhibit A is the complaint on the inadequacy of the electric grid physical security filed with FERC on January 29, 2020 and February 19, 2020. FERC dismissed the complaint on a technicality at the urging of the electric utility industry.

Since the industry and the regulators haven't addressed the physical security of our critical electric infrastructure in four decades, extraordinary leadership is needed now to get the job done.

Another example is the lack of supply chain cybersecurity requirements. With the recent SolarWinds and Colonial Pipeline cyberattacks, there is no need to belabor the threats posed by cyberattacks to the energy sector. However, between 2006 and 2019, according to data from the U.S. International Trade Commission, the U.S. imported 300 "Liquid dielectric transformers having a power handling capacity exceeding 10,000 kVA" from China.[8]

At least 200 of these Chinese large power transformers found their way into our electric grid.[9] Others may have been bought by large industries, but it is certain that most of these 300 Chinese large power transformers have embedded themselves in our critical infrastructures in the U.S. There is no requirement that anybody check these hundreds of transformers that have already been installed. There is no supply chain cybersecurity requirement on the thousands of companies that may buy components for the critical electric infrastructure from China.[10]

To summarize the problem: We are buying critical equipment from China to install into our critical electric infrastructure that China is already hacking.

What could possibly go wrong?

The present regulatory scheme relies on thousands of companies who own, operate or supply the critical electric infrastructure to *voluntarily* do the right thing. There is no requirement that they do so. This brings us to the second major challenge.

2. The second challenge is the electric utility industry itself.

The electric utility industry has an agenda which is not necessarily the same agenda as the United States government. In fact, according to The Center for Responsive Politics, the electric utilities in the 2020 cycle:

- Spent $108,468,019 on lobbying the U.S. Congress.[11]
- Made total contributions to the U.S. Congress of $28,562,003.[12]
    - Made $11,626,034 in political contributions to members of the U.S House.
    - Made $5,140,906 in political contributions to members of the U.S. Senate.
- Total lobbying and contributions in the 2020 cycle: over $137 million.

---

[8] See: https://michaelmabee.info/the-u-s-has-300-chinese-large-power-transformers/

[9] E&E News. "China and America's 400-ton electric albatross." April 25, 2019. https://www.eenews.net/stories/1060216451/ Also see: Smith, Rebecca. 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

[10] Attached as Exhibit B is the complaint on the inadequacy of the electric grid cyber security filed with FERC on May 11, 2020. FERC dismissed the complaint on a technicality at the urging of the electric utility industry.

[11] See: https://www.opensecrets.org/industries/lobbying.php?cycle=2018&ind=E08

[12] See: https://www.opensecrets.org/industries/contrib.php?ind=E08&Bkdn=DemRep&cycle=2020

In the last decade the electric utility industry has spent *$1.2 billion* lobbying the U.S. Congress and another $150 million in "contributions." (Not including lobbying and contributions at the state level.) Imagine if this $1.2 billion, which largely originated from the bills of ratepayers, was put towards electric grid security rather than lobbying against further regulation.

The industry's lobbyists have embedded themselves over the years, as "partners" in DOE and FERC via the Electric Subsector Coordinating Council ("ESCC") and trade organizations such as the Edison Electric Institute ("EEI"), the American Public Power Association ("APPA"), the National Rural Electric Cooperative Association ("NRECA"), the Large Public Power Council ("LPPC"), the Transmission Access Policy Study Group ("TAPS"), the Electric Power Supply Association ("EPSA"), WIRES, and the Electricity Consumers Resource Council ("ELCON"). These industry groups have actively *fought against* grid security regulation, mandatory critical infrastructure protection standards and public transparency.

The industry *does not* represent the public interest. They *do not* represent the U.S. government.

Here are a few facts about the electric industry's posture on grid security:

- After the Great Northeast Blackout of 2003, the industry was forced to write a mandatory vegetation management standard. (Yes, the industry writes its own standards.) The standard took a decade to finally be implemented in 2013.[13] Problem solved? Ask the people of Paradise, California where 85 people died in the 2018 Camp Fire and PG&E subsequently plead guilty to 85 felony counts for its role in that catastrophe.[14]
- After the spectacular physical attack against a transformer in Metcalf, California in 2013[15] the industry advised *against* a mandatory physical security standard.[16] They were forced to write the standard. The resulting weak physical security standard that exempts most facilities from compliance. (Generation facilities are specifically exempted.) As a result, there have been hundreds of physical attacks against the grid since the "physical security standard" was implemented.[17]
- Despite the well-documented physical security problem in the critical electric infrastructure[18], the industry continues for fight *against* stronger physical security regulations. The inadequacy of the physical security standards was highlighted in a complaint filed with the Federal Energy Regulatory

[13] See: https://www.ferc.gov/industries-data/resources/tree-trimming-and-vegetation-management
[14] San Francisco Chronicle. "PG&E, a 'killer company,' admits to 85 felony counts. Now what?" March 29, 2020. https://www.sfchronicle.com/business/article/PG-E-a-killer-company-admits-to-85-felony-15163078.php
[15] Smith, Rebecca. The Wall Street Journal. *"Assault on California Power Station Raises Alarm on Potential for Terrorism."* February 5, 2014. https://www.wsj.com/articles/assault-on-california-power-station-raises-alarm-on-potential-for-terrorism-1391570879 and Smith, Rebecca. Wall Street Journal. "U.S. Risks National Blackout From Small-Scale Attack." March 12, 2014. https://www.wsj.com/articles/SB10001424052702304020104579433670284061220
[16] NERC's then CEO Gerry Cauley told Congress in a February 12, 2014 letter: "I do not believe it makes sense to move to mandatory standards at this time. There are more than 55,000 substations of 100 Kv or higher across North America, and not all those assets can be 100% protected against all threats. I am concerned that a rule-based approach for physical security would not provide the flexibility needed to deal with the widely varying risk profiles and circumstances across the North American grid and would instead create unnecessary and inefficient regulatory burdens and compliance obligations." Letter available at: https://michaelmabee.info/wp-content/uploads/2021/05/NERC-Response-to-Senators-Letter-Reid-2-11-14-v4.pdf
[17] See: https://michaelmabee.info/oe-417-database/
[18] See for example: Smith, Rebecca. Wall Street Journal. "How America Could Go Dark." July 14, 2016. https://www.wsj.com/articles/how-america-could-go-dark-1468423254

Commission (FERC) on January 29, 2020 alleging that grid physical security was inadequate.[19] At the urging of the industry, on June 9, 2020 FERC dismissed the complaint.[20]

- The industry vehemently fought FERC's Notice of Proposed Rulemaking to establish a mandatory standard for Geomagnetic Disturbances.[21] Once forced to write a standard (TPL-007-1) the effectiveness of this industry-written standard is still the subject of considerable debate.[22]
- The industry has consistently fought *against* stronger supply chain cybersecurity standards. The inadequacies of the cybersecurity standards were highlighted in a complaint filed with the Federal Energy Regulatory Commission (FERC) on May 11, 2020 about the need for increased supply chain cybersecurity.[23] At the urging of the industry, on October 2, 2020 FERC dismissed the complaint.[24] A month and a half later, the SolarWinds hack came to light and the regulators – NERC and FERC – were caught flat-footed.
- The irony of the SolarWinds hack is that since 2017, the industry vehemently fought against modifying CIP standards to require detection, mitigation and removal of malware from the electric grid.[25] While fighting this common-sense petition for rulemaking, the head of NERC testified in 2019 that he didn't know whether there was Russian or Chinese equipment or software already installed in the grid.[26] SolarWinds was first detected in 2020 but to this day, thanks to the industry's diligent efforts, there is no requirement that malware be detected, mitigated or removed.
- The Texas grid collapse in February of 2021, which was responsible for over 150 deaths[27] and between $80 billion–$130 billion in economic loss[28], was a repeat offense. Similar outages for identical reasons occurred in 1989 and 2011. The government and the industry have failed to fix the underlying critical electric infrastructure issues that caused all three incidents. Yet the industry urged FERC to take no action to investigate whether the existing standards were followed or if improvements are needed.[29] At the urging of the industry, FERC dismissed a complaint on this issue on May 26, 2021.[30]
- There is currently no mandatory standard for protecting the grid against an electromagnetic pulse (EMP) attack – a standard that the industry opposes and FERC declines to order. The industry enlisted its Electric Power Research Institute (EPRI) to "study" the electromagnetic pulse (EMP)

---

[19] See Exhibit A.
[20] See 171 FERC ¶ 61,205. https://elibrary.ferc.gov/eLibrary/idmws/file_list.asp?document_id=14867700
[21] See FERC Order No. 779, issued May 16, 2013 at 143 FERC ¶ 61,147 https://elibrary.ferc.gov/eLibrary/filelist?document_id=14115712&optimized=false
[22] See FERC Docket RM15-11-000. Multiple experts outside the electric industry argue that the standard is not sufficient to protect the grid from a GMD event.
[23] See Exhibit B.
[24] See 173 FERC ¶ 61,010. https://elibrary.ferc.gov/eLibrary/filelist?accession_num=20201002-3033
[25] See FERC Docket AD17-9-000 Petition for Rulemaking by the Foundation for Resilient Societies in a New Docket: For the Commission to Require an Enhanced Reliability Standard to Detect, Report, Mitigate and Remove Malware from the Bulk Power System.
[26] See February 14, 2019 Senate Committee on Energy and Natural Resources hearing: "Hearing to Consider the Status and Outlook for Cybersecurity Efforts in the Energy Industry" (at 1 hour and 30 minutes). Available at: https://michaelmabee.info/senate-cybersecurity-hearing/
[27] See: https://dshs.texas.gov/news/updates.shtm#wn
[28] See: https://www.dallasfed.org/research/economics/2021/0415.aspx
[29] Attached as Exhibit C is the complaint on the inadequacy of the reliability standards and their failure to prevent the Texas grid collapse of February 2021 filed with FERC on February 28, 2021.
[30] See 175 FERC ¶ 61,163. https://elibrary.ferc.gov/eLibrary/filelist?accession_num=20210526-3061

threat to the electric grid. EPRI disregarded the findings of the Congressional EMP Commission[31] and severely understated the EMP threat. The resulting disingenuous report by EPRI (which was lauded by the industry) has placed the United States in great danger.[32] EPRI's report is contradicted by multiple experts of the Electromagnetic Defense Task Force (EDTF) [33] and by a January 11, 2021 Department of Energy memo.[34] However, the industry continues to propound that the EPRI report is the benchmark report for EMP protection of the critical electric infrastructures. Regardless, there is no movement towards developing an EMP standard to protect the electric grid.

- Edison Electric Institute (EEI) is the trade organization that purports to represent "all U.S. investor-owned electric companies." EEI is a frequent intervenor and commenter in FERC dockets and Congressional hearings related to Critical Infrastructure Protection (CIP) standards and issues. EEI spends millions of dollars annually lobbying the U.S. Congress on matters pertaining to the U.S. critical electric infrastructure. EEI also makes contributions to key members of Congress involved in critical infrastructure security legislation and oversight. EEI counts among its members State Grid Corporation of China, which is a state-owned corporation, owned by the government of the People's Republic of China. EEI also counts as a member Power Assets Holdings, a company based in Hong Kong (which China calls "Hong Kong Special Administrative Region of the People's Republic of China").[35]

The U.S. Government has been concerned about the cybersecurity of the critical electric infrastructure since at least 2003,[36] the security of the electric grid from physical threats since at least 1981[37] and electromagnetic pulse (EMP) threats since at least 1975.[38] In other words, we have been talking about securing our critical electric infrastructure for over four decades from the very threats we still face today.

The electric utility industry has lobbied and fought against grid protection regulations every step of the way. After the Great Northeast Blackout of 2003, Congress passed the Energy Policy Act of 2005 which added Section 215 to the Federal Power Act. However, this moved the needle very little on the security of the critical electric infrastructure. The impact was we moved from "voluntary" self-regulation to "mandatory" self-regulation – but only for a small portion of the whole critical electric infrastructure. Perhaps the problem we face today was best summarized in 2003 in Congressional testimony when the bill was being debated:

---

[31] Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Reports are available here: https://michaelmabee.info/unclassified-emp-commission-reports/

[32] See: https://michaelmabee.info/epri-emp-report/

[33] Electromagnetic Defense Task Force (EDTF) Review of EPRI EMP Report August 23, 2109. http://bit.ly/2OglqYI

[34] Department of Energy. "Physical Characteristics of HEMP Waveform Benchmarks for Use in Assessing Susceptibilities of the Power Grid, Electrical Infrastructures, and Other Critical Infrastructure to HEMP Insults." January 11, 2021. https://bit.ly/3rLmztL

[35] See: https://michaelmabee.info/electric-industry-lobbyists-china-ties-questioned/

[36] See: "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

[37] General Accounting Office (GAO). Federal Electrical Emergency Preparedness Is Inadequate. EMD-81-50. May 12, 1981. http://bit.ly/354ZN4i

[38] See: Defense Civil Preparedness Agency (DCPA). Vulnerability of Regional and Local Electric Power Systems--Nuclear Weapons Effects and Civil Defense Actions. July 1975. http://bit.ly/2QogiVj

> "We must not rely on industry self-regulation. The proposal to move from voluntary self-regulation to mandatory self-regulation misses the point. The difficulty is not the voluntary versus the mandatory. It is the 'self' part. We need clear accountability to public authorities."[39]

While public-private partnerships have their place, the industry has lobbied, promoted and ultimately hornswoggled the federal government into a system of "all carrots and no stick." They laud the public-private partnerships and have fought for decades against regulation and mandatory standards to secure the critical electric infrastructure. Everything they do is calculated to kick the grid security can down the road and commission more "studies." When finally forced to write a mandatory standard, the resulting weak standards should not be surprising. This hands-off approach has not worked and today our national security is jeopardized.

In short, the electric utility industry has had their chance – and for many more years than this regulatory boondoggle should have been allowed to go on. Enough is enough. The present dismal state of our critical electric infrastructure security is *because* the federal government listened to the electric utility industry and applied a light regulatory touch at the urging of industry lobbyists.

The electric utility industry's agenda is not and cannot be the Department of Energy's agenda. The tail has been wagging the regulatory dog for decades on grid security – which is the primary reason we are in a national security crisis today.

Unfortunately, the United States has occasionally been a bad judge of character. A rogues' gallery including Osama bin Laden, Saddam Hussein and Manuel Noriega count themselves as former U.S. allies. Here, we have placed our trust and our national security in the hands of an industry with a checkered past[40]: Samuel Insull, Enron, PG&E's multiple felony convictions, the recent Ohio and Illinois bribery scandals to name only a few. In fact, R Street Institute pointed out[41]:

> "Policymakers should not dismiss these developments as merely the work of a few bad actors, but as the latest evidence of an established behavioral pattern tied to perverse incentives from flawed institutions."

We should not trust the electric utility industry. If after all the industry's efforts and counsel over the past decades, our critical electric infrastructure is not secure, perhaps their agenda is not the same as that of the United States government.

When some of the thousands of entities who own, operate or supply the electric grid do the right things, we should incentivize them. But we must hold those who endanger the critical electric infrastructure

---

[39] Testimony of Mark N. Cooper, Director of Research, Consumer Federation of America. Page 25. "Keeping The Lights On: The Federal Role In Managing The Nation's Electricity." Before the Committee on Governmental Affairs, Oversight of Government Management, the Federal Workforce and the District of Columbia Subcommittee. (108th Congress) September 10, 2003. http://bit.ly/357GCHh

[40] ProPublica. "Four Types of Scandals Utility Companies Get Into With Money From Your Electric Bills." October 10, 2020. https://www.propublica.org/article/four-types-of-scandals-utility-companies-get-into-with-money-from-your-electric-bills

[41] Hartman, Devin and Haugh, Mike. R Street Institute. "Electric Competition: The Antidote For Bad Behavior." September 2020. https://www.rstreet.org/wp-content/uploads/2020/09/Final-No-205-electric-competition-updated.pdf

accountable. And we must ensure that the public, Congress and state regulatory authorities have the transparency necessary to scrutinize the results.

The Department of Energy must show extraordinary leadership in the face of powerful and influential special interests in order to secure the critical electric infrastructure.

Public, Congressional and state scrutiny is needed.

The failure of the industry and the government for decades to secure the critical electric infrastructure from the known threats is punctuated by, at best, confusing and conflicting information provided to the public as well as the downright coverup of misconduct. We need a policy of adequate public information, transparency and accountability.

3. The third challenge is that OE-417 data is inadequate, inaccurate, not updated and conflicts with data from other official sources.

Utility companies and grid operators are required to submit reports on electric disturbance events to the Department of Energy (DOE) on a Form OE-417 ("Electric Emergency Incident and Disturbance Report").

I did an analysis of all the publicly available OE-417 data from 2010 through 2020.[42] First of all, there were 166 different "event types" reported many of which were either duplicates or related. For example, there were at least 24 different "event types" that denoted a physical attack. There were at least 50 "event types" that denoted a disturbance caused by weather. I grouped these 166 "event types" into 15 categories (actually "causes") so that we could get a sense of what has actually threatened the electric grid in the past decade.

All NERC Regions		
Event	#	%
Weather	961	52.6%
Cyber Attack	37	2.0%
Physical Attack	721	39.5%
Fuel Supply Deficiency	74	4.1%
Equipment	15	0.8%
Natural Disaster	14	0.8%
Wildfire	5	0.3%
Generation Interruption	17	
Transmission Interruption	113	
Distribution Interruption	9	
Operations	185	
Islanding	67	
Load Shed	30	
Public Appeal	65	
?	10	
Total OE-417 Reports	**2323**	
Cause Known from OE-417	**1827**	
Cannot Determine Cause	**496**	

There has been a total of 2,323 electric disturbance events filed during the period of January 1, 2010 through December 31, 2020.

Unfortunately, the public OE-417 data is so bad that there were 496 electric disturbance events where I was unable to identify a cause (21% of the reports). These are highlighted in yellow in the chart. I was able to identify a cause in 1,827 electric disturbance events, or 79% of the OE-417 reports filed. (I used this known population of 1,827 for the percentages in the above chart and the study below.)

The results are disturbing to say the least.

[42] Available at: https://michaelmabee.info/oe-417-database/

Weather: As one might suspect, weather was the cause of the majority of the disturbances, 961 events, or 53%. If one believes that weather is getting worse in recent years, then this number should be of great concern.

Physical Attacks: Shockingly, there were 721 physical attacks on the grid, or 40% of the incidents. As previously mentioned, the "physical security standards" for our electric grid are weak in the few areas of the bulk power system where they do apply, but there are no mandatory physical security standards for most of the electric grid.

Fuel Supply Deficiency: There were 74 events, or 4% of the events. related to fuel supply deficiency. The Colonial Pipeline cyberattack raises great concerns for the security of fuel supply to generation plants.

Cyber Attacks: I was also surprised to learn that there have been 37 cyberattacks reported during this period (2% of the reports). What is most disturbing is that during the same period, the North American Electric Reliability Corporation (NERC) annual reliability reports and other government agencies seem to paint completely different pictures.

The data given to the public in the OE-417s is dramatically different than what NERC portrays to the public in their self-serving annual "State of Reliability Reports." [43] Here is what NERC reported during this same period:[44]

- **2020 Report** (page x) "There were no reportable cyber or physical security incidents in 2019." (Note: There was a significant and widely reported cyberattack in the grid in 2019 – which does appear in the OE-417 and was widely reported in the press[45] but disingenuously omitted from NERC's public report.)
- **2019 Report** (page ix): "In 2018, there were no reported cyber or physical security incidents that resulted in an unauthorized control action or loss of load."
- **2018 Report** (page viii): "In 2017, there were no reported cyber or physical security incidents that resulted in a loss of load."
- **2017 Report** (page 3): "In 2016, there were no reported cyber or physical security incidents that resulted in a loss of load."
- **2016 Report** (page v): "In 2015, there were no reported cybersecurity incidents that resulted in loss of load. There was one physical security incident that resulted in a loss of approximately 20 MW of load."
- **2015 Report** (page 7): "[N]o Reportable Cyber Security Incidents or physical security reportable events resulted in loss of load on the BPS in 2014." (Note: Misleading, since the Nogales Station in Arizona was attacked by an IED in 2014. [46])

---

[43] Available at https://www.nerc.com/pa/RAPA/PA/Pages/default.aspx

[44] Note that the report each year is on the previous year, e.g., the 2020 report is for the events of the year 2019.

[45] See, for example: E&E News. "'Cyber event' disrupted U.S. grid networks — DOE" April 30, 2019. https://www.eenews.net/stories/1060242741/ and E&E News. "Report reveals play-by-play of first U.S. grid cyberattack." September 6, 2019. https://www.eenews.net/stories/1061111289. Ironically, NERC posted a "Lessons Learned" document on this cyberattack to the industry, but still told the public "There were no reportable cyber or physical security incidents in 2019."

[46] Holstege, Sean and Randazzo, Ryan, The Republic. *"Sabotage at Nogales station puts focus on threats to grid."* June 13, 2014. https://www.azcentral.com/story/news/arizona/2014/06/12/sabotage-nogales-station-puts-focus-threats-grid/10408053/

- **2014 Report**: No mention of cyber or physical attacks. (Note: Misleading, since the Metcalf Transformer attack took place in 2013.[47])
- **2013 Report**: No mention of cyber or physical attacks.
- **2012 Report**: No mention of cyber or physical attacks.
- **2011 Report**: No mention of cyber or physical attacks.

There is clearly a huge disconnect between what the industry defines as a cybersecurity or physical security incident and what is reported on the OE-417s. The below chart reproduces the public OE-417 entries for the Metcalf physical attack (2013) and the Nogales physical attack (2014):

Date Event Began	Time Event Began	Date of Restoration	Time of Restoration	Area Affected	NERC Region	Alert Criteria	Event Type	Demand Loss (MW)	Number of Customers Affected
4/16/2013	1:47 AM	4/18/2013	3:25 PM	California	WECC		Loss of Part of a High Voltage Substation, Physical Attack	N/A	0
6/11/2014	9:30 AM	6/11/2014	9:31 AM	Nogales, Arizona	WECC		Suspected Physical Attack	N/A	N/A

While this minimal information was reported on the OE-417, NERC did not find Metcalf or Nogales noteworthy enough for their annual reports. These events were significant physical attacks against the grid and NERC chose not to disclose them to the public.

The discrepancies in physical security and cybersecurity reporting can be summarized as follows:

- There were 721 physical attacks against the grid reported on the OE-417's between January 1, 2010 through December 31, 2020, yet according the NERC there was only one during the same period.
- There were 37 cyberattacks against the grid reported on the OE-417's between January 1, 2010 through December 31, 2020, yet according the NERC there were none during the same period.

Meanwhile, federal government reports on cyberattacks against the energy sector during the same periods paint a completely different picture. For example, here's what the United States Government Accountability Office (GAO) had to say in Congressional testimony on October 21, 2015 on cyberattacks[48]:

> "Cyber incidents continue to affect the electric industry. For example, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team noted that the number of reported cyber incidents affecting control systems of companies in the electricity subsector increased from 3 in 2009 to 25 in 2011. The response team reported that the energy sector, which includes the electricity subsector, led all others in fiscal year 2014 with 79 reported incidents. Reported incidents affecting the electricity subsector have had a variety of impacts, including hacks into smart meters to steal power, failure in control systems devices requiring power plants to be shut down, and malicious software disabling safety monitoring systems."

---

[47] Smith, Rebecca. The Wall Street Journal. *"Assault on California Power Station Raises Alarm on Potential for Terrorism."* February 5, 2014. https://www.wsj.com/articles/assault-on-california-power-station-raises-alarm-on-potential-for-terrorism-1391570879

[48] Government Accountability Office. CRITICAL INFRASTRUCTURE PROTECTION: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention. October 21, 2015. http://bit.ly/39kNp3p

And the U.S. Department of Homeland Security reported 59 cyberattacks on the energy sector in FY 2016[49] and 46 cyberattacks in FY 2015.[50] Both the GAO and DHS data conflicts with the OE-417 data which shows only 37 cyberattacks from 2010 through 2020.

Astoundingly, NERC reported to the public that there were no cybersecurity incidents in their annual reliability reports for the same periods.

NERC's definitions apparently don't consider most cyberattacks to be "reportable cyberattacks." The public is confused when the U.S. government reports a substantial number of cyberattacks against the energy subsector and NERC reports no cyberattacks.

While the industry may argue that there are different populations of regulated entities covered by the various reports, clearly, more transparency is needed for the public, investors, Congress and other regulators to understand these discrepancies and make sense of this conflicting information. Regulatory complexity requires even better public information.

Moreover, the requirement that the information be updated is obviously not being followed by the industry, or enforced by DOE, making the information of substantially less value.

For example, attached as Exhibit D is the public OE-417 data for the TRE Region (i.e., ERCOT) for February 2021 – the period covering the Texas grid collapse. One of the OE-417 requirements is that the information is supposed to be updated. Clearly, the information has not been updated. By now we should know the "Demand Loss (MW)" for each entry and the "Number of Customers Affected" but many entries still say "Unknown."

This is not unique to this incident. Attached as Exhibit E is the public OE-417 data (then called the EIA-417) for the Great Northeast Blackout of 2003 in which 45 million people in the U.S. lost power, as well as another 10 million in Canada, the EIA-417 data in 2021 shows "Number of Customers Affected" were 7,369,487. Also, to this day, the "Type of Disturbance" is listed as "Unknown."

The confusing and inaccurate public information needs substantial improvement. If the public data is any indication, then the Department's internal data on electric disturbance events may also be lacking, making analysis of issues in the critical electric infrastructures problematic.

The Department of Energy must improve the quality of the OE-417 data so causes of disturbance events can be meaningfully determined and electric disturbance events analyzed. DOE needs to enforce the reporting requirements to ensure the information is accurate. Substantial penalties should apply where entities fail to report or update required information.

---

[49] National Cybersecurity and Communications Integration Center. "FY 2016 Incidents by Sector." https://www.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf

[50] Idaho National Laboratory. "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector." August 2016. https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf

4. The fourth challenge is the coverup of the names of regulatory violators, which prevents public, Congressional and state scrutiny and shields violators from accountability.

Since July of 2010, the identities of every violator of NERC's Critical Infrastructure Protection (CIP) standards have been withheld from the public, investors, state Public Utility Commissions (PUCs) and Congress. The electric utility industry, through its regulatory mouthpiece NERC – aided and abetted by FERC – are attempting to permanently withhold the names of the violators despite the fact that the violations in almost all cases have been long ago mitigated.

Between July of 2010 and April of 2021 there have been 275 FERC dockets involving over 1,500 "Unidentified Registered Entities" – the industry euphemism for violators whose names are being withheld from the public. In every single case, the identity of the regulatory violator was withheld from the public, Congress and state regulators. This issue is the subject of multiple Freedom of Information Act (FOIA) Requests and a lawsuit against the Federal Energy Regulatory Commission under FOIA.[51] The electric utility industry vehemently opposes the release of the names of violators.

We know for a fact from open sources that the Russians and the Chinese have been in our electric grid for over a decade:

- April 8, 2009 Wall Street Journal: "Electricity Grid in U.S. Penetrated By Spies." [52]
- January 10, 2019 Wall Street Journal: "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It." [53]
- January 29, 2021 Wall Street Journal: "Suspected Russian Hack Extends Far Beyond SolarWinds Software, Investigators Say."[54]

So, if keeping the names of the CIP violators from the public was going to make us safer, wouldn't it have worked by now? A fair conclusion is that "secret regulation" of CIP standards has not worked. It appears from the available evidence that the real reason for the "protection" of the names of the regulatory violators is because the industry does not want to be held accountable for doing more than the minimum on physical and cyber security. There appears to be no legitimate security reason to withhold the names of regulatory violators in perpetuity as is currently the practice.

Notably the electric utility industry has threatened to stop "self-reporting" violations if FERC begins to release the names of CIP violators. The Trade Associations' Motions to Intervene in FERC Docket No. NP19-4-000[55] contains a not so thinly veiled threat:

> "If the Commission begins releasing entity names in addition to the information already made public in the posted Notices of Penalty, then Registered Entities may re-evaluate whether they

[51] Details of the FOIA requests and responses as well as the lawsuit are available here: https://michaelmabee.info/cip-violation-database/

[52] Available at: https://www.wsj.com/articles/SB123914805204099085

[53] Available at: https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

[54] Available at: https://www.wsj.com/articles/suspected-russian-hack-extends-far-beyond-solarwinds-software-investigators-say-11611921601

[55] Available at: https://elibrary.ferc.gov/idmws/file_list.asp?document_id=14756159

> will continue to self-report security information knowing that providing such information to their regulators may be disclosed to the public, including to people seeking to attack their systems. In addition, Registered Entities also may re-evaluate what information is included in their mitigation plans."

This is an extraordinary threat that the entities in the industry represented by the Trade Associations, who are subject to NERC's mandatory reliability standards under federal law,[56] will essentially engage in a regulatory mutiny if the Commission decides to release the names of regulatory violators to the public, as its past orders and regulations require.

The industry is essentially arguing that the names of the regulatory violators constitute "Critical Electric Infrastructure Information" (CEII) and should be withheld from the public permanently (even after the violations are mitigated). This argument is unsupported by FERC regulations and past FERC orders.[57]

There is a public interest in disclosing the names of regulatory violators because:

- Disclosing the names of the violators might lead the public and Congress to assess how well the regulatory system is working.
- This information would inform the public, investors, PUCs and Congress as to whether the current regulatory system can adequately thwart threats to the grid.
- This information could lead the public, investors, PUCs and Congress to conclude that better investment in the critical infrastructures is necessary.

These are public policy questions, not CEII.

Moreover, many companies transcend regulatory lines. Many companies fall under both FERC/NERC and state public utility commission (PUC) jurisdiction and possibly other agencies, such as the Nuclear Regulatory Commission (NRC) and the Securities Exchange Commission (SEC).

- State PUC's need to know the identities of the CIP violators because, among other things, state PUC's often control the funding for mitigation.
- Some of these companies may supply critical DOD and DHS facilities. DOD and DHS need to know if companies they are dependent upon to power facilities critical to national security are violating CIP standards.

---

[56] 16 U.S. Code § 824o(b)(1) (Electric reliability) provides that: "The Commission shall have jurisdiction, within the United States, over the ERO certified by the Commission under subsection (c), any regional entities, and all users, owners and operators of the bulk-power system, including but not limited to the entities described in section 824(f) of this title, for purposes of approving reliability standards established under this section and enforcing compliance with this section. *All users, owners and operators of the bulk-power system shall comply with reliability standards that take effect under this section*." [Emphasis added.]

[57] For further details, see Motion to Intervene in FERC Docket NP19-4-000 available at: https://michaelmabee.info/wp-content/uploads/2019/02/FERC-Docket-NP19-4-Motion-to-Intervene-Mabee.pdf; Reply Comments in FERC Docket NP19-4-000 available at: https://michaelmabee.info/wp-content/uploads/2019/05/Reply-Comments-of-Michael-Mabee-in-NP19-4-000.pdf; Petition for Rulemaking available at: https://michaelmabee.info/wp-content/uploads/2019/02/Petition-for-Rulemaking-Mabee-with-exhibits-1.pdf

- Some of these companies may operate nuclear generation plants and fall under the jurisdiction of the NRC as well as FERC/NERC and a PUC (or more than one PUC). These regulators all need to know if the companies they regulate are in violation of CIP standards.
- Some of these companies are also regulated by the Securities Exchange Commission and have reporting requirements for material events. Since the names of CIP violators are being covered up, investors are unaware of the cybersecurity risks that these publicly traded companies face—and whether the "C Suite" is taking appropriate actions to mitigate (*or at least disclose*) investor risk.

It is hard to imagine how such a Balkanized regulatory system would function in any context, and clearly it is not functioning efficiently in terms of the critical electric infrastructure—one in which the lives of 330 million Americans and our very national security depends.

Until the regulatory system is reformed by Congress, accountability, disclosure and transparency are critical to our national security. There is no possible way for there to be accountability for the thousands of companies involved in the generation, transmission and distribution of electric power in the U.S. except for transparency by DOE, FERC and NERC.

The public, state regulators and investors also have a need to know who violates mandatory CIP standards. Consider the following:

- Who is paying for the CIP violation fines—the ratepayers or the shareholders?
- Who is paying for any mitigation ordered or agreed upon—the ratepayers or the shareholders?
- Most importantly, *who decides who pays*?

The last question is easy: Absent transparency, the regulatory violator decides who pays. This is why it is critical that FERC release the names of the regulatory violators along with sufficient information so that the public ("ratepayers"), investors ("shareholders"), the PUCs (the ones who should be making these decisions) and Congress (the oversight) can see what is happening.

In 2018, PG&E Corp was fined 2.7 million dollars for a cyber breach (which was exposed by one of my Freedom of Information Act requests).[58] PG&E presumably also had to spend an unknown amount (but likely a substantial amount) of money on mitigation. Somebody had to pay for all of this. Because I could find no disclosure of the event or its costs in PG&E's filings with the Securities and Exchange Commission, it is impossible for the public to know whether the shareholders or the ratepayers ate these costs—I am sure both groups would like to know.

Does it make a difference in who should pay if a company is a repeat CIP violator? Does it make a difference in who should pay if the company is negligent?

The *last* one who should be deciding who pays *is the regulatory violator*. This decision should be made by the appropriate regulator (the PUC) with full transparency to the two possible victims: the ratepayers and the shareholders.

---

[58] See report: https://michaelmabee.info/pge-endangered-the-grid/

Ratepayers and investors deserve transparency and accountability. PUCs and Congress deserve sufficient information to effectively regulate and govern. Regulatory violators do not deserve reputational protection by the regulators at the expense of the public interest.

In sum, mandatory CIP standards should protect the U.S. electric grid by holding the electric utility companies and grid operators accountable to protect the portion of the critical electric infrastructure that they own or operate. Instead, the electric utility industry has twisted this regulatory scheme into a sham where companies have no incentive to do more than the minimum. If caught violating a CIP standard, NERC and the Regional Entities will settle the matter privately with the "unidentified registered entities" negotiating a "penalty" that the "unidentified registered entities" are willing to pay and will keep the matter from public view. It looks like a system of back-room settlements and handshake penalties. A great deal for the "unidentified registered entities"—not so much for the American people or the security of the critical electric infrastructure.

Conclusions and Recommendations:

The title of this request for information is "Ensuring the Continued Security of the United States Critical Electric Infrastructure." In order to accomplish this, given the aforementioned four challenges, the U.S. Department of Energy, the Department of Homeland Security and Congress must provide extraordinary leadership. Such federal leadership has been lacking for over four decades.

Recommendations for the U.S. Department of Energy

1. The Department of Energy must use to the fullest extent all federal regulatory authority available to *mandate* and *enforce* critical electric infrastructure protection and seek additional authority from Congress to do so. We need to address the entire infrastructure: Generation, Transmission and Distribution. This is a matter of national security and cannot be left to "self-regulation" at the discretion of special interests, such as the electric utility industry.

2. The Department of Energy must balance industry input and influence with other viewpoints. Public-private partnerships related to the critical electric infrastructure for years have been industry driven and "all carrots and no stick." This has clearly not worked. Critical electric infrastructure owners, operators and suppliers must be held accountable for protecting the electric grid. Critical electric infrastructure protection must be mandatory – not voluntary. Severe penalties and accountability are necessary for violators. Experts from outside the industry and those representing the public interest must have a voice.

3. The Department of Energy must revamp its OE-417 data to make it accurate and useful to the public and other stakeholders. The public should not be getting different and conflicting pictures from DOE, DHS and FERC (through NERC). Reporting on the OE-417 is mandatory. However, DOE needs to *enforce* the accurate reporting of incidents and disturbances and *enforce* updates to the information.

4. The Department of Energy must hold the electric utility industry accountable for failures to secure the critical electric infrastructure. Such accountability includes public, congressional, state and investors having access to the names of violators of Critical Infrastructure Protection (CIP) standards. DOE and FERC cannot continue to let the electric industry hide its dirty laundry from the public and

avoid accountability by continuing to allow a cover-up that has endangered the critical electric infrastructure by allowing violators and the regulatory system to avoid any modicum of accountability.

Recommendation for Congress and the U.S. Department of Homeland Security

With multiple sectors of the U.S. critical infrastructures under current attack[59], immediate and decisive Congressional action is needed:

1. Legislation is needed mandating that reasonably prudent cybersecurity measures be taken by all companies, public or private sector, that are part of the 16 critical infrastructure sectors described in Presidential Policy Directive 21.[60]

    a. The Chief Executive Officer of each such critical infrastructure company must be required to certify periodically to DHS that they have reasonably prudent cybersecurity measures in place that have been reviewed and approved by the Chief Executive Officer of the company.[61]

    b. There must be civil and criminal penalties for false certification or failure to submit such certifications.

    c. These certifications should be made available to the public as well as state and federal authorities.

    d. There must be whistleblower protections for employees of the critical infrastructures who report violations of laws, regulations or standards to their employer, regulators or the government.[62]

Respectfully submitted,

Michael Mabee
Fort Worth, TX
Email: CivilDefenseBook@gmail.com
Phone: (516) 808-0883

Attachments: Exhibits A-F

---

[59] Robert McMillan, Joseph De Avila and Jacob Bunge. Wall Street Journal. "NYC's Subway Operator and Martha's Vineyard Ferry Latest to Report Cyberattacks." June 2, 2021. https://www.wsj.com/articles/ransomware-scourge-continues-as-essential-services-are-hit-11622672685
Attacks on infrastructure are part of a global criminal pivot from stealing data to hobbling operations

[60] See: https://www.cisa.gov/critical-infrastructure-sectors

[61] After the Enron debacle, Congress enacted similar certification requirements for publicly traded companies related to financial and disclosure controls. See sections 302, 404 and 906 of the Sarbanes-Oxley Act of 2002 and it's implementing regulations at 17 CFR §§228-240.

[62] Exhibit F is an example of such a provision contemplated by Senators Grassley and Markey in 2020.

CC: U.S. Senate Committee on Energy and Natural Resources
U.S. House Committee on Energy and Commerce
U.S. Department of Homeland Security - Cybersecurity & Infrastructure Security Agency

Exhibit A

Comments of Michael Mabee
U.S. Department of Energy
Request for Information (RFI) on
Ensuring the Continued Security of the United States Critical Electric Infrastructure

Note: Full copy with Exhibits available at:
https://michaelmabee.info/wp-content/uploads/2020/02/2020-02-19-Mabee.pdf
and
https://michaelmabee.info/wp-content/uploads/2020/02/2019-01-29-FERC-Complaint-Mabee-1.pdf

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Complaint of Michael Mabee	**)**	
Related to Critical Infrastructure	**)**	**Docket No. EL20-21-000**
Reliability Standard	**)**	

Additional Information and Recommendations of Complainant

Submitted to FERC on February 19, 2020

Introduction

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.

In addition to the information and recommendations contained in the original Complaint, filed on January 29, 2020 and docketed by the Commission on February 6, 2020, I wish to submit supplemental information and additional recommendations for the record. In the Complaint, I alleged that: 1) The mandatory physical security standard is inadequate, and 2) Enforcement of the mandatory physical security standard seems nonexistent. Below, I provide further background and detail on the allegations and further recommendations.

CIP-14-2 is Critical to the National Security of the U.S.

Presidential Policy Directive 21 (PPD-21) identifies the energy sector as uniquely critical due to the enabling functions it provides across all 16 critical infrastructure sectors.[1] The bulk power system is the lynchpin: All 16 critical infrastructures – including the rest of the energy sector – depend on the bulk power system. Therefore, any threat to the bulk power system is a threat to U.S. national security.

CIP-14-2 (Physical Security) is the only mandatory physical security standard that protects this key component necessary to the functioning of all 16 critical infrastructures identified in PPD 21.

The threat of physical attack on the electric grid is not theoretical: CIP-14-2 became effective on October 2, 2015. Department of Energy OE-417 data shows that there have been 245 physical attacks on the grid since the standard became effective. (Exhibit A is a listing of the OE-417 reported physical attacks between October 2, 2015 and December 31, 2019.)

[1] Presidential Policy Directive 21 (PPD-21) - Critical Infrastructure Security and Resilience. February 12, 2013. http://bit.ly/2NUr04k (accessed February 16, 2020).

Historically, we have seen spectacular and sophisticated physical attacks against the electric grid such as

- **2013 The Metcalf Sniper Attack.**[2] No arrests have ever been made in one of the most alarming physical attacks against the electric grid. The attack on the PG&E Metcalf substation raised Congressional concern which lead to the Commission directing the North American Electric Reliability Corporation (NERC) to develop a physical security standard. Unfortunately, as I will explain below, the standard is fraught with loopholes and covers very few facilities.
- **2013 The Arkansas grid attacks.**[3] In a period of a few weeks, attacks occurred against a two transmission lines and a substation. The perpetrator was eventually arrested but the attacks demonstrate the extreme vulnerability of transmission lines and substations to physical attack.
- **2014 The Nogales IED attack.**[4] An improvised explosive device (IED) was used in an attempt to blow up a 50,000-gallon diesel fuel tank at a critical transformer substation. The bomb failed to ignite the fuel, but called into larger question the physical security of the grid.
- **2014 The Hydro-Québec attack by airplane.**[5] While the details of the attack are under court seal, the attacker used an airplane to short out two major transmission lines, cutting off power to over 180,000 customers. This incident demonstrated the vulnerability of the grid to an attack by air.

While these four particular attacks took place prior to the effective date of CIP-14-2, it is debatable whether the present standard would have stopped them if they occurred today. In fact, in the case of PG&E's Metcalf station, the following year the Metcalf station was attacked for a second time[6] and

---

[2] Smith, Rebecca. The Wall Street Journal. *"Assault on California Power Station Raises Alarm on Potential for Terrorism."* February 5, 2014. https://www.wsj.com/articles/assault-on-california-power-station-raises-alarm-on-potential-for-terrorism-1391570879 (accessed February 16, 2020).

[3] Pentland, William. Forbes. Weekend Attacks on Arkansas' Electric Grid Leave 10,000 Without Power; 'YOU SHOULD HAVE EXPECTED U.S.' Oct 7, 2013. https://www.forbes.com/sites/williampentland/2013/10/07/weekend-attacks-on-arkansas-electric-grid-leave-10000-without-power-you-should-have-expected-u-s/ (accessed February 16, 2020); Pentland, William. Forbes. Vandals Attack Electric Grid In Arkansas. Sep 26, 2013. https://www.forbes.com/sites/williampentland/2013/09/26/terrorists-attack-electric-grid-in-arkansas/#35a862fd35ef (accessed February 16, 2020); FBI: Attacks on Arkansas Power Grid - Perpetrator Sentenced to 15 Years. August 10, 2015. https://www.fbi.gov/news/stories/attacks-on-arkansas-power-grid (accessed February 16, 2020).

[4] Holstege, Sean. The Republic. Sabotage at Nogales station puts focus on threats to grid. June 12, 2014. https://www.azcentral.com/story/news/arizona/2014/06/12/sabotage-nogales-station-puts-focus-threats-grid/10408053/ (accessed February 16, 2020); Sobczak, Blake and Behr, Peter. E&E News. 'Crude' bomb at Ariz. substation stokes broader security concerns. June 13, 2014. https://www.eenews.net/stories/1060001267 (accessed February 16, 2020).

[5] Freeman, Alan. The Washington Post. Pilot to be sentenced in sabotage that crippled Quebec power grid. November 2, 2018. https://www.washingtonpost.com/world/2018/11/02/pilot-be-sentenced-sabotage-that-crippled-quebec-power-grid/ (accessed February 16, 2020);
Behr, Peter. E&E News. Outage on Quebec power grid traced to airborne attacker. June 17, 2015. https://www.eenews.net/stories/1060020352 (accessed February 16, 2020).

[6] Wald, Matthew L. The New York Times. "California Power Substation Attacked in 2013 Is Struck Again." August 28, 2014. https://www.nytimes.com/2014/08/29/us/california-power-substation-attacked-in-2013-is-hit-again.html (accessed February 16, 2020).

PG&E's credibility was shot when its public statements about its physical security improvements were contradicted by a leaked internal memo.[7]

And the fact remains that *since* the effective date of CIP-14-2, there have been 245 physical attacks on the grid. This simply cannot be ignored.

Moreover, the threat of a coordinated physical attack is not theoretical. There are numerous recent and historic examples of terrorists or "inferior forces" using well-planned sophisticated attacks against multiple targets with great effect. The Tet Offensive on January 30, 1968 was a coordinated surprise attack on over 100 cities and outposts in Vietnam. The attack caught the U.S. totally by surprise and it is widely attributed to turning the tide of the war against the U.S.[8] On September 11, 2001, terrorists attacked the U.S. in a sophisticated, well-coordinated attack against multiple targets.[9] The impacts to the U.S. from the 9/11 attacks were dramatic and society changing.

More recently, on September 14, 2019 two oil production facilities in Saudi Arabia were attacked by drones and missiles causing a substantial temporary loss of Saudi Arabia's oil production.[10] Responsibility for this attack was claimed by Houthi rebels in Yemen, however, the United States and other countries have accused Iran of involvement.[11] Terrorist organizations such as ISIS (a.k.a. "Islamic State") are also known to have deployed weaponized drones.[12]

The U.S. electric grid, built over generations in which domestic terrorism was not a concern, was not designed to thwart physical attacks. That physical security must now be put into place through meaningful mandatory standards. The electric grid is an open target. For example, in 5 minutes using Google Maps, I was able to trace transmission lines from two generating plants to various equipment and substations on the grid. I was able to see the equipment and locations in excellent detail. (Exhibit B is several screen shots from my 5-minute Google Maps "reconnaissance" of part of the grid.) Terrorists can easily map out sections of the grid and locate critical equipment. With drones, they could attack these facilities from several kilometers away.[13]

---

[7] NBC Bay Area "Internal Memo: PG&E Years Away from Substation Security." May 15, 2015 https://www.nbcbayarea.com/on-air/as-seen-on/internal-memo_-pg_e-years-away-from-substation-security_bay-area/69201/ (accessed January 29, 2020).

[8] History Channel. Tet Offensive. October 29, 2009. https://www.history.com/topics/vietnam-war/tet-offensive (accessed February 16, 2020).

[9] The National Commission on Terrorist Attacks Upon the United States. "The 9/11 Commission Report." July 22, 2004. http://bit.ly/3bjibKW (accessed February 16, 2020).

[10] Reid, David. CNBC. Saudi Aramco reveals attack damage at oil production plants. September 20, 2019. https://www.cnbc.com/2019/09/20/oil-drone-attack-damage-revealed-at-saudi-aramco-facility.html (accessed February 16, 2020).

[11] Reuters. U.S. blames Iran for Saudi oil attack, Trump says 'locked and loaded.' September 15, 2019. https://www.reuters.com/article/us-saudi-aramco-attacks/u-s-blames-iran-for-saudi-oil-attack-trump-says-locked-and-loaded-idUSKBN1W00SA (accessed February 16, 2020).

[12] Rassler, Don. United States Military Academy. The Islamic State and Drones: Supply, Scale and Future Threats. https://ctc.usma.edu/app/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf (accessed February 16, 2020).

[13] See: King, Llewellyn. InsideSources. "Drones Pose a New, Deadly Threat to Energy Infrastructure." September 20, 2019. https://www.insidesources.com/drones-pose-a-new-deadly-threat-to-energy-infrastructure/ (accessed February 17, 2020); Bean, Tim. PowerGrid International. "Energy Industry also Faces Threats from Drones." October 9, 2018. https://www.power-grid.com/2018/10/09/energy-industry-also-faces-threats-from-drones/#gref

Finally, CIP-14-2 is riddled with loopholes to the point where it is largely a voluntary standard, not a mandatory standard. The only requirement is that those few facilities who are subject to it have a notebook labeled "Physical Security Plan" with some certain papers of dubious value. It makes no requirement whatsoever that physical security plans of these few facilities be effective or be approved by any regulatory authority. CIP-14-2 leaves out the majority of facilities in the bulk power system. I will discuss this in more detail below.

The current threat landscape requires a full reevaluation of CIP-14-2. FERC needs to understand that it is *the only federal agency* that has the authority to protect the bulk power system from simultaneous physical attacks involving multiple critical facilities that could threaten the 16 critical infrastructures identified in PPD-21.

If FERC fails to direct substantial improvements to CIP-14-2, then it is neglecting the very real danger that an inadequately protected bulk power system poses to the 16 critical infrastructures and is neglecting the Commission's responsibility to the American people.

I hope this is not the case.

Loopholes in the present CIP-14-2 "Applicability" make the standard inadequate.

Unfortunately, CIP-14-2 admittedly expects the population of facilities covered by the standard "will be small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities."[14] And, unbelievably, "the SDT[15] determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard."[16]

Most alarmingly, FERC has admitted that: "Reliability Standard CIP-014-1 does not require responsible entities to assess the criticality of Bulk-Power System facilities based on a simultaneous attack on multiple facilities."[17] Although the issue of simultaneous attacks was raised strenuously in rulemaking, FERC declined to address it:

> Moreover, the March 7 Order "anticipate[d] that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System … [and that the Commission's] preliminary view is that most of these would not be 'critical' as the term is used in [the March 7 Order]." Accordingly, NERC was not required to address in the physical security Reliability Standards scenarios of simultaneous physical attacks involving multiple critical facilities.[18] [Internal footnotes omitted.]

(accessed February 17, 2020); Sobczak, Blake. E&E News. "Feds to energy companies: Beware drones made in China." May 21, 2019. https://www.eenews.net/stories/1060369689 (accessed February 17, 2020).

[14] CIP-14-2 "Guidelines and Technical Basis," page 22.

[15] Standard Drafting Team.

[16] CIP-14-2 "Guidelines and Technical Basis," page 23.

[17] Order Denying Rehearing in Docket RM14-15-001. Page 4 (April 23, 2015).

[18] Order Denying Rehearing in Docket RM14-15-001. Page 5 (April 23, 2015).

There are over 2000 EHV LPTs[19] (Extra High Voltage Large Power Transformers) in the United States and tens of thousands of LPTs. But according to CIP-14-2's applicability, very few of these would meet the criteria for coverage. That is a lot of critical targets for a potential simultaneous terrorist attack which are not covered by the standard.

But it gets worse.

Power generation plants are not covered under CIP-14-2. OE-417 data from the Department of Energy shows that there have been 66 disturbances cause by fuel supply deficiency since 2010.[20] There have also been at least 17 disturbances cause by "generation interruption" during the same period.[21] During times of extreme weather, we have seen the systems in New England, Texas and California strained to the limits. And this is in "normal times."

Then FERC Chairman Cheryl LaFleur testified on September 22, 2014 before the Senate Energy Committee and admitted: "A carefully planned and executed attack on a single or multiple generation plants could cause cascading outages…"[22]

If, as FERC admits, an attack on *one generation plant* could cause a cascading failure, a simultaneous terrorist strike on several generation facilities is a grave danger. If such an attack occurs in conjunction with a "public appeal" to reduce electricity consumption – which have occurred at least 64 times since 2010[23] – or in conjunction with a weather-related event – which have occurred 800 times since 2010,[24] the consequences for an already stressed grid are dire.

Transmission lines are not covered under CIP-14-2. While it may not be feasible to fully secure 240,000 miles of high voltage transmission lines, this does not mean that they should be completely excluded from the CIP standard. There are actions that should be required.

For example, Transmission Owners and Operators should be required to coordinate with all law enforcement agencies through whose jurisdiction the lines pass. They should be required to provide these law enforcement agencies with maps, access points and have a standing "no trespassing" enforcement request. Signage should be required. In critical access areas, gates should be installed to limit vehicular access to authorized vehicles.

Critical military bases and other critical infrastructures may lose power. CIP-14-2's "applicability" will not protect the grid from a coordinated attack on smaller facilities.

---

[19] U.S. Department of Energy "Large Power Transformers and the U.S. Electric Grid." June 2012. https://www.energy.gov/sites/prod/files/Large Power Transformer Study - June 2012_0.pdf (accessed January 29, 2020).

[20] See: https://michaelmabee.info/oe-417-database/ (accessed February 16, 2020).

[21] See: https://michaelmabee.info/oe-417-database/ (accessed February 16, 2020).

[22] Testimony of FERC Chairman Cheryl LaFleur, to U.S. Senate Energy Committee in a letter dated June 4, 2014. https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=86e83c32-636a-40b6-8e5d-c072f2f95a8c (accessed February 16, 2020). Full April 10, 2014 hearing is available at https://www.govinfo.gov/content/pkg/CHRG-113shrg87851/pdf/CHRG-113shrg87851.pdf (accessed February 16, 2020).

[23] See: https://michaelmabee.info/oe-417-database/ (accessed February 16, 2020).

[24] See: https://michaelmabee.info/oe-417-database/ (accessed February 16, 2020).

> "The purpose of Reliability Standard CIP-014 is to protect Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection."[25]

This means that the standard only applies to each individual facility *that if disabled alone* would meet this applicability. Moreover,

> "The Standard Drafting Team (SDT) expects this population will be small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities."[26]

A coordinated attack against uncovered facilities could threaten our key military bases in that area and other critical infrastructures. FERC admits that:

> Reliability Standard CIP-014-1 does not require responsible entities to assess the criticality of Bulk-Power System facilities based on a simultaneous attack on multiple facilities.[27]

CIP-14-2's "applicability" leaves unprotected large swaths of the critical components of the electric grid which are susceptible to a coordinated terrorist attack, including:

- Generation plants
- Transmission lines
- Most transformer stations and substations
- Some control facilities

A standard with an "applicability" to so little of the most critical of our critical infrastructures cannot be deemed "adequate" under any circumstances.

Loopholes in the present CIP-14-2 "Requirements" make the standard inadequate.

The "requirements" of CIP-14-2 are fraught with loopholes to the point where the standard covers few facilities and the loopholes render this largely a voluntary standard, not a mandatory standard. The only ultimate requirement is that those few facilities who are subject to it have a notebook labeled "Physical Security Plan" with some certain papers of dubious value. It makes no requirement whatsoever that physical security plans for these few facilities be effective or approved by any regulatory authority. CIP-14-2 leaves out the majority of facilities in the bulk power system.

Requirement R1. "Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1."

---

[25] CIP-14-2 Guidelines and Technical Basis. Page 22.
[26] CIP-14-2 Guidelines and Technical Basis. Page 22.
[27] Order Denying Rehearing in Docket RM14-15-001. Page 4 (April 23, 2015).

R1 Loophole: The population of covered facilities which would be identified in the "risk assessment" is small. This standard only applies if the loss of the *individual facility alone* could cause a cascading failure. There are no provisions for facilities that in a coordinated attack on multiple facilities could have the same impact. In fact, in the Guidelines and Technical Basis section, NERC explains that: "The Standard Drafting Team (SDT) expects this population will be small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities."

This loophole must be closed. FERC should direct that the standard be modified to include any facilities that alone or in a coordinated attack on multiple facilities, could *contribute* to a critical impact on the operation of the Interconnection in the event the asset is rendered inoperable or damaged.

FERC should also direct that the standard be modified to require Transmission Planners and Reliability Coordinators to model the loss of one or more critical substations on their system with a focus on a simultaneous attack on multiple locations. Such modeling will better inform the industry and regulators on vulnerabilities in the system.

Requirement R2. "Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1." While this sounds good on the surface, several loopholes exist which cast the effectiveness of the requirement in doubt.

R2.2 Loophole #1: Many, if not all, peer Transmission Owners would meet the requirement to be a "verifying entity." This means that peer Transmission Owners could verify each other's risk assessments. This creates an obvious conflict of interest and could incent Transmission Owners to "go easy – they are verifying us next week."

R2.2 Loophole #2: "The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s)."

A Transmission Owner could hire a "verifying entity" just to "verify" that they did a risk assessment and specifically *not make recommendations*. Recommendations should be required. The word "may" should be changed to "shall."

FERC should direct NERC to modify R2 to prohibit reciprocal "verifications" between Transmission Owners to avoid even the appearance of a conflict of interest in the process. Moreover, the requirement should specify that the "verifying entity" ensure that an analysis was conducted on the impact that an attack on multiple facilities would have on the entire interconnection.

R2.3 Loophole: Notwithstanding that in the present standard, recommendations are not "required" and can be easily avoided, there is no regulatory approval required if an entity simply "Document[s] the technical basis for not modifying the identification in accordance with the recommendation." Regulatory approval should be required if a Transmission Owner decides not to modify its identification under Requirement R1.

This should not be burdensome – if a valid reason exists, it should be approved. However, the security of the entire interconnection is at stake in these decisions and therefore, regulators need visibility on the identifications – and protection – of critical facilities.

Requirement R4. "Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2."

R4 Loophole: There is no requirement that anybody with threat evaluation or physical security knowledge or experience even be consulted. There is no requirement for on-site evaluations of these facilities. As this requirement is written, any reasonably literate employee could conduct this threat and vulnerability evaluation from a desk at the corporate office and meet the standard.[28]

FERC should direct NERC to modify Requirement R4 to specify that this evaluation be conducted by a person or entity with threat evaluation and physical security experience and that such evaluation include on-site assessments of each covered facility.

Another loophole in R4 is that there is no provision that subsequent evaluations of the potential threats and vulnerabilities be performed. As written, this "evaluation" is done once. Many such evaluations could now be years old. Given the evolving threats and changes to the geography around a facility, FERC must direct NERC to modify CIP-14-2 to require that such evaluations be done at least annually and include on-site inspections by qualified personnel.

Requirement R5. "Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s)."

R5 Loophole: There is no requirement that the plan be effective in any way and there is no requirement that anybody with physical security experience even be involved in developing the plan. Transmission Owners have the discretion to do a very minimal amount to meet Requirements R5.1 through R5.4. Further, the weaknesses in R1, R2 and R4 are compounded here in physical security plans based on questionable peer reviews and non-expert threat and vulnerability evaluations.

Requirement R6. "Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5."

R6.1 Loophole: This "unaffiliated third party" can still be a peer Transmission Owner who meets the criteria of R6.1 (which most probably do). This means that peer Transmission Owners could verify each other's evaluations (R4) and physical security plans (R5). This creates an obvious conflict of interest and could incent an "unaffiliated third party" to "go easy – they are reviewing us next week."

[28] While the Guidelines and Technical basis has suggestions on resources to consult, they are merely suggestions, not requirements.

Another example. One acceptable "unaffiliated third party" under R6.1 is: "An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification." However, this one member on the review staff may not be the leader or the person writing the "review." There is sufficient "flexibility" to marginalize the role of this "at least one member" of the review staff who has experience, in this largely paper exercise. There is no requirement that this one member who might have some knowledge perform any type of on-site evaluation. In the end, this loophole makes the qualifications and marching orders of the "review staff" – especially peer utilities – suspect.

In fact, the "unaffiliated third party" could fully meet their obligations from their own corporate office by reviewing the "physical security" binder. There is no requirement that they ever set foot on the Transmission Owner's property.

It is worth noting that R6.1 is the only place in the CIP-14-2 that purports to require any modicum of physical security knowledge or expertise in the process. But the loopholes in R6 make it easy for a Transmission Owner to completely marginalize or avoid entirely any chance that the "unaffiliated third party" will recommend that there is further work to be done. The standard, as written, makes this all completely optional.

R6.2 Loophole: "The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5." A Transmission Owner could hire a "unaffiliated third party" reviewer just to "review" that they have a binder labeled "Physical Security" with all of the requisite papers. A Transmission Owner could specifically ask the "reviewer" not make recommendations. Recommendations should be required. Moreover, the review should also consist of on-site visits to the covered facilities.

R6.3 Loophole: Notwithstanding that in the requirement as currently written recommendations are not "required" and can be easily avoided, there is no regulatory approval required if an entity simply "Document[s] the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation."

Regulatory approval should be required if a Transmission Owner decides not to modify its physical security under Requirement R6. If a valid reason exists, it should be approved. However, the security of the entire interconnection is at stake in these decisions and therefore, regulators need visibility on the effectiveness of the physical security plans – and protection – of critical facilities.

Another loophole in R6 is that there is no provision for subsequent "review [of] the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5." As written, this "review" is done once. Many such reviews could now be years old. Given the evolving threats and changes to the geography around a facility, FERC must direct NERC to modify CIP-14-2 to require that such evaluations be done at least annually and include on-site inspections by qualified personnel.

The physical security plan for critical facilities should contain tangible security measures (or reasons they are not required) such as:

- CCTV

- Ballistic barriers
- Gunfire locators
- Fencing or barriers to obscure gunfire targets
- Overhead threat detection
- Overhead threat protection

Finally, physical security plans under Requirement R5 should be *effective* and the effectiveness must be part of the "review" under R6.[29] FERC should direct NERC to modify CIP-14-2 to modify the phrase in R5 to read: "develop and implement a documented and effective physical security plan(s)…" Further, FERC should direct NERC to modify CIP-14-2 to modify R6 to require that the "review" evaluate the effectiveness of the physical security plan developed under R5 and require on-site inspections by the "reviewer." Finally, FERC should direct NERC to modify R6 to prohibit reciprocal "reviews" between Transmission Owners to avoid even the appearance of a conflict of interest in the process.

Loopholes in the present CIP-14-2 "Compliance Monitoring Process" make the standard ineffective.

As previously discussed, an effective CIP-14-2 which protects the bulk power system, and thus the 16 critical infrastructures, is of paramount importance to the national security of the United States. As noted in my Complaint, CIP-14-2 has been cited only 4 times since it became effective.[30]

If the reason that the standard hasn't been cited more often is because every Transmission Owner has a three-ring binder labeled "Physical Security" for the few assets that actually fall under the standard, that is one problem – the standard itself is inadequate.

The enforcement of the standard is another problem. It is important to recall that the electric industry *did not* want this standard. NERC itself opposed a physical Security Standard; then NERC CEO Gerry Cauley stated in a Senate Hearing:

> I do not believe it makes sense to move to mandatory standards at this time. There are more than 55,000 substations of 100 kV or higher across North America, and not all those assets can be 100% protected against all threats. I am concerned that a rule-based approach for physical security would not provide the flexibility needed to deal with the widely varying risk profiles and circumstances across the North American grid and would instead create unnecessary and inefficient regulatory burdens and compliance obligations. [31]

FERC, under immense pressure from Congress, directed NERC to develop a standard anyway. So, the industry went to work writing the physical security standard it didn't want. We shouldn't be surprised at the result – if you force a person, organization or industry to do something they don't want to do,

---

[29] "Red Teams" are one way to test the effectiveness of physical security plans and find additional vulnerabilities that may need attention.

[30] FERC Docket Numbers: NP19-4-000; NP18-14-000 and NP17-29-000 (2 violations).

[31] Senate Hearing: Keeping the Lights On—Are We Doing Enough to Ensure The Reliability and Security of the U.S. Electric Grid? April 10, 2014. https://www.govinfo.gov/content/pkg/CHRG-113shrg87851/pdf/CHRG-113shrg87851.pdf Page 137. (accessed February 16, 2020).

expecting them to rip into the task with zeal is probably a stretch. NERC submitted their proposed standard (known as CIP-014-1[32]) on May 23, 2014.

FERC issued an order on November 20, 2014[33] literally ordering NERC to change one word. (The word was: "widespread" and was used 30 times in the proposed standard. This word—a slight of pen by NERC's attorneys—would have excluded many more facilities from falling under the standard.)

On October 2, 2015, FERC approved the "Physical Security" standard, known as CIP-014-2.

What we know is that according to the Department of Energy OE-417 Electric Emergency Incident and Disturbance Reports there have been 245 physical attacks against the electric grid since the standard became effective.[34] And we know that there have been only 4 citations for violations of the physical security standard.

It does not appear that NERC even wishes to enforce this lame standard. Gerry Cauley's voice may still echo in the hallways of NERC.

FERC must direct NERC to not only develop a standard that provides adequate protection to the bulk power system from physical attacks – specifically the all too real threat of a coordinated attack against multiple facilities – but also to enforce it. NERC shouldn't be simply checking for the for the presence of a three-ring binder – it should be ensuring effective physical security for the bulk power system.

The CIP-14-2 (or successor) standard must be monitored and audited by teams with physical security expertise. NERC and the Regional Entities must employ or contract such experts if they do not already have them. Audits should include on-site visits to covered facilities and must evaluate the effectiveness of physical security plans – not just the existence of a three-ring binder.

Red Teams and Force-on-Force exercises should be regularly conducted so that all Transmission Owners gain this valuable experience and sense of urgency. Getting grid physical security right is a matter of national security.

NERC has just been recertified as the "Electric Reliability Organization" (ERO).[35] NERC's action (or inaction) on the physical security of the bulk power system must be closely monitored by FERC and Congress. What has happened between the date CIP-14-2 became effective and now is unacceptable.

In sum, this present almost voluntary hollow standard must be substantially improved to become truly mandatory and must ensure adequate protection of one of the nation's most valuable – and most vulnerable – assets. The bulk power system.

---

[32] Available at: https://www.nerc.com/pa/Stand/Reliability Standards/CIP-014-1.pdf (accessed February 16, 2020).
[33] Available at: https://www.ferc.gov/whats-new/comm-meet/2014/112014/E-4.pdf (accessed February 16, 2020).
[34] To the extent that anybody wishes to argue that some of these incidents were "mere vandalism," this is hardly comforting. If a couple of 13-year-olds can break in and damage equipment, it does not bode well for our protective posture against terrorists.
[35] 170 FERC ¶ 61,029 "Order on Five-Year Performance Assessment." January 23, 2020.

Conclusion and Recommendations

Publicly available information indicates that: 1) the mandatory physical security standard is inadequate, and 2) enforcement of mandatory physical security standard seems nonexistent. In my Complaint, I recommended that FERC take the following actions:

1. FERC should direct NERC to modify CIP-014-2 (Physical Security) to require that the entity's "Physical Security Plan" be effective and receive regulatory approval. The standard should specify that all "risk assessments" "evaluations" and "security plans" should be reviewed by qualified non-affiliated persons with expertise in physical security.

2. FERC should direct NERC to submit to the Commission for approval a compliance and enforcement plan for physical security that would provide meaningful assurances that the regulators and regulated entities are taking seriously their obligations to protect the bulk power system from physical threats.

3. FERC (in collaboration with DOE, DHS, DOD, and the National Guard) should "Red Team" entities in order to evaluate weaknesses and determine whether their physical security (and cybersecurity) programs are effective. FERC should work with state PUCs to ensure like actions at the state-level.

In the preceding pages, I provided additional specific section-by-section recommendations which all relate back to my original recommendations.

FERC finds itself as the only federal government agency in a position to protect the 16 critical infrastructures and the American people from a dire threat of a coordinated attack on the bulk power system. FERC's actions now could avert a catastrophe. FERC's inaction could enable it.

Respectfully submitted,

Michael Mabee

CC: U.S. Department of Homeland Security
U.S. Department of Defense
U.S. Senate Committee on Energy and Natural Resources
U.S. House Committee on Energy and Commerce

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Complaint under Section 215 of the	**)**	
Energy Policy Act of 2005 related to Critical	**)**	**Docket No.** EL20-21-000
Infrastructure Protection Reliability Standards	**)**	

COMPLAINT

Submitted to FERC on January 29, 2020

Introduction

I am a private citizen who conducts public interest research on the security of the electric grid because I recognize the absolutely 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 filing this complaint under 16 U.S. Code § 824o(d)(5)[1] and 16 U.S. Code § 824o(e)(3)[2] because it appears from publicly available information that: 1) the mandatory physical security standard is inadequate, and 2) enforcement of the mandatory physical security standard seems nonexistent. In summary:

1. *The physical security standard itself—CIP-014-2 (Physical Security)—is inadequate.* There is no requirement that an entity's risk assessment or physical security plan be reviewed by anyone with any physical security expertise. There is no regulator determination whatsoever as to the effectiveness of any entity's physical security plan.

2. *Enforcement of CIP-014-2 (Physical Security) seems nonexistent*. In the almost seven years since the Metcalf California substation attack, there have been only four citations issued for violations of the physical security standards. And these four citations were for administrative violations.

---

[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.]

[2] "On its own motion ***or upon complaint***, the Commission may order compliance with a reliability standard and may impose a penalty against a user or owner or operator of the bulk-power system if the Commission finds, after notice and opportunity for a hearing, that the user or owner or operator of the bulk-power system has engaged or is about to engage in any acts or practices that constitute or will constitute a violation of a reliability standard." [Emphasis added.]

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 correct deficiencies.

Background

Physical security requirements for the electric grid—and their enforcement—are largely non-existent almost 7 years after the Metcalf attack.

At approximately 1:00 a.m. on April 16, 2013, a major PG&E transformer substation in Metcalf California was attacked. The attack was well-planned and sophisticated.[3] One year later, the Metcalf station was struck again when the fence was cut open and, the facility entered and tools were stolen.[4]

Obviously, the physical security situation had not improved much in the intervening year. In fact, PG&E's credibility was shot when its public statements about its physical security improvements were contradicted by a leaked internal memo.[5]

The April 2013 Metcalf attack was not the only physical attack on critical components of the North American electric grid. According the Department of Energy OE-417 reports, there were 578 physical attacks against the grid reported from January 1, 2010 through May 31, 2019.[6]

However, the attack on the Metcalf substation—and the other attacks—shouldn't have been a surprise. On May 12, 1981, the General Accounting Office (GAO) issued a report entitled: "Federal Electrical Emergency Preparedness Is Inadequate." GAO noted in 1981:

> "If saboteurs, terrorists, or an enemy attacked the Nation's electric power system, would the Federal Government be prepared to handle the resulting energy disruptions?
>
> Probably not, because the Department of Energy has failed to prepare required electric emergency preparedness plans. A national plan to cope with the problems caused by a loss of electricity–which would virtually halt communication, transportation, and distribution systems–

[3] Smith, Rebecca. The Wall Street Journal. *"Assault on California Power Station Raises Alarm on Potential for Terrorism."* February 5, 2014. https://www.wsj.com/articles/assault-on-california-power-station-raises-alarm-on-potential-for-terrorism-1391570879 (accessed January 29, 2020).

[4] Wald, Matthew L. The New York Times "California Power Substation Attacked in 2013 Is Struck Again." August 28, 2014. https://www.nytimes.com/2014/08/29/us/california-power-substation-attacked-in-2013-is-hit-again.html (accessed January 29, 2020).

[5] NBC Bay Area "Internal Memo: PG&E Years Away from Substation Security." May 15, 2015 https://www.nbcbayarea.com/on-air/as-seen-on/internal-memo_-pg_e-years-away-from-substation-security_bay-area/69201/ (accessed January 29, 2020).

[6] See report: "Electric Disturbance Events: What is the public allowed to know?" https://michaelmabee.info/electric-disturbance-events/ (accessed January 29, 2020).

> is essential, because utilities and the States cannot be expected to deal with such emergencies on their own."

At least as far back as 1981, GAO was concerned about the physical security of our substations. GAO found:

> "Electric power systems are highly dependable, but are very vulnerable to disruptions from acts of war, sabotage, or terrorism. In the region GAO looked at:
>
> - An attack on just eight substations could disrupt power to the entire region for a long time. (See p. 8.)
> - Damage to just four substations could disrupt power to one city for up to a year. (See p. 8.)
> - Damage to just one substation could leave a key military facility without power. (See p. 8.)"

Further, a year before the Metcalf attack, the National Academies published a report titled: *Terrorism and the Electric Power Delivery System*.[7] The report discussed physical security of high-voltage transformers noting:

> "High-voltage transformers are of particular concern because they are vulnerable to attack, both from within and from outside the substation where they are located. These transformers are very large, difficult to move, custom-built, and difficult to replace. Most are no longer made in the United States, and the delivery time for new ones can run to months or years."

Then, one year *after* the Metcalf attack, the Wall Street Journal ran two alarming stories:

- Assault on California Power Station Raises Alarm on Potential for Terrorism. *April Sniper Attack Knocked Out Substation, Raises Concern for Country's Power Grid.*[8]

- U.S. Risks National Blackout From Small-Scale Attack. *Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage.*[9]

What was done?

After the February 5, 2014 Wall Street Journal article, the Senate sent a letter on February 7, 2014 to the Federal Energy Regulatory Commission (FERC), to ask them what they were doing to protect the grid.[10] And FERC Responded on February 11, 2014 telling the Senate that:

---

[7] Available at: https://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system (accessed January 29, 2020).
[8] Smith, Rebecca. Wall Street Journal. February 5, 2014. Available at: https://www.wsj.com/articles/assault-on-california-power-station-raises-alarm-on-potential-for-terrorism-1391570879 (accessed January 29, 2020).
[9] Smith, Rebecca. Wall Street Journal. March 12, 2014. Available at: https://www.wsj.com/articles/u-s-risks-national-blackout-from-small-scale-attack-1394664965 (accessed January 29, 2020).
[10] Available at: https://www.ferc.gov/industries/electric/indus-act/reliability/chairman-letter-incoming.pdf (accessed January 29, 2020).

> "Since the attack on the Metcalf facility in April 2013, the Commission's staff has taken responsive action together with NERC, other federal and state agencies, and transmission and generation asset owners and operators."[11]

Notwithstanding FERC's assurances to the senate in 2014, the physical security of our critical transformers and facilities appears to remain inadequate in 2020.

Complaint 1. The standard—CIP-014-2 (Physical Security)—is inadequate.

As a result of Metcalf, FERC ordered NERC to develop a physical security standard. NERC submitted their proposed standard (known as CIP-014-1[12]) on May 23, 2014.

FERC issued an order on November 20, 2014[13] literally ordering NERC to change one word. (The word was: "widespread" and was used 30 times in the proposed standard. This word—a slight of pen by NERC's attorneys—would have excluded many facilities from falling under the standard.)

On October 2, 2015, FERC approved the "Physical Security" standard, known as CIP-014-2.[14] Unfortunately, the physical security standard requires very little:

1. Requirement 1: Each Transmission Owner shall perform a risk assessment of its Transmission stations and Transmission substations.
2. Requirement 2: Each Transmission Owner shall have an unaffiliated third party verify the risk assessment *[e.g., a peer grid company would meet the requirement—"Hey, if you verify mine, I'll verify yours"].*
3. Requirement 3: If a Transmission Owner operationally controls an identified Transmission station or Transmission substation, it must notify the Transmission Operator that has operational control of the primary control center.
4. Requirement 4: Each Transmission Owner shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s).
5. Requirement 5: Each Transmission Owner shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s).
6. Requirement 6: Each Transmission Owner shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) under Requirement R5 *[again, a peer grid company would meet the requirement].*

That's it. All the infrastructure owner must do is to have a binder with a bunch of papers labeled "Physical Security Plan" and have any peer utility they choose review the "risk assessment," "evaluation" and "security plan(s)". No need for it to be anybody who knows anything significant about physical security.

---

[11] Available at: https://www.ferc.gov/industries/electric/indus-act/reliability/chairman-letter-feinstein.pdf (accessed January 29, 2020).
[12] Available at: https://www.nerc.com/pa/Stand/Reliability Standards/CIP-014-1.pdf (accessed January 29, 2020).
[13] Available at: https://www.ferc.gov/whats-new/comm-meet/2014/112014/E-4.pdf (accessed January 29, 2020).
[14] Available at: https://www.nerc.com/pa/Stand/Reliability Standards/CIP-014-2.pdf (accessed January 29, 2020).

And there is no requirement as to what the "Physical Security Plan" must include—or even that it be effective. Nobody with regulatory authority even has to even approve it—All you need is somebody to "review" it. What if the "reviewer" happens to say "this plan sucks?" It doesn't matter. The only requirement is that the three-ring binder be "reviewed." (I guess most any papers in a three-ring binder will do.)

That unapproved three-ring binder of papers is what is standing between the United States and a catastrophic widespread power outage caused by a terrorist attack. (Also, it is worthy of note that generation plants are not included in NERC's physical security standard.)

Complaint 2. Enforcement of CIP-014-2 seems nonexistent

One would think that after the public and Congressional interest in the Metcalf attack, FERC and NERC would take a special interest in the enforcement of the physical security standards. Unfortunately, one would be wrong. How many times since Metcalf have utilities been cited for violations of standard CIP-014-2?

Four.

We have had 578 physical attacks to the grid (that have been publicly disclosed) yet, utilities have been cited for violations of the standard only four (4) times in the almost seven (7) years since the Metcalf attack. It would appear that this standard and regulatory scheme are not working. Here are the facts.

- There are close to 1,500 entities regulated by NERC.
- There are over 2000 EHV LPTs[15] (Extra High Voltage Large Power Transformers) in the United States and tens of thousands of LPTs.
- There have been four (4) citations for non-compliance with the physical security standard (CIP-014-2) since Metcalf.

The American people are not stupid. We see these transformers unguarded behind chain-link fences as we drive up the road or walk our dogs.

So, let's take a look at the four times NERC found CIP-014-2 violations:

- In FERC Docket No. NP19-4-000[16] (one Violation—which everybody knows is Duke Energy Corp. [17]), Duke apparently excluded one substation from its risk assessment because they didn't think it met the criteria for inclusion.
- In FERC Docket No. NP18-14-000[18] (one violation), the "Unidentified Registered Entity" failed to do a risk assessment on one substation due to a "management oopsy."

---

[15] U.S. Department of Energy "Large Power Transformers and the U.S. Electric Grid." June 2012. https://www.energy.gov/sites/prod/files/Large Power Transformer Study - June 2012_0.pdf (accessed January 29, 2020).

[16] Available at: https://elibrary.ferc.gov/idmws/file_list.asp?document_id=14739324 (accessed January 29, 2020).

[17] Sobczak, Blake and Behr, Peter. E&E News. "Duke agreed to pay record fine for lax security — sources." February 1, 2019. https://www.eenews.net/stories/1060119265 (accessed January 29, 2020).

[18] Available at: https://elibrary.ferc.gov/idmws/file_list.asp?document_id=14675460 (accessed January 29, 2020).

- And in FERC Docket No. NP17-29-000[19] (two violations), the "Unidentified Registered Entity" failed to include one control center in its 1) risk assessment and 2) security plan (two violations) because an employee who knew what they were doing left the company, leaving nobody else at the company who knew what they were doing.

One will notice that all four of these "violations" are administrative in nature and have nothing to do with whether there is actually meaningful physical security in place.

History of the "Physical Security" standards

CIP-001-1 (Sabotage Reporting)[20] became effective on June 4, 2007. Utilities were cited for its violation 404 times between 6/4/2008 and 5/26/2011. It them morphed into CIP-001-1a (February 2, 2011)[21] and CIP-001-2a (August 2, 2011)[22]—neither of which were EVER cited.

Meanwhile, EOP-004-1 (Disturbance Reporting)[23], which covered "equipment damage" among other things, had violations 16 times between 2009 and 2013.

NERC began to look at merging CIP-001 and EOP-004 "to eliminate redundancies" and on June 20, 2013, FERC approved[24] merging CIP-001-2a (Sabotage Reporting) and EOP-004-1 (Disturbance Reporting) into EOP-004-2 (Event Reporting)[25]. (CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting were then "Retired.") EOP-004-2 covers reporting "damage or destruction of a facility." EOP-004-2 and its successors have never been found to be violated.

Here is the enforcement history of these various standards:

- 404 Citations issued for CIP-001-1 (Sabotage Reporting) between 2008 and 2011
- 16 Citations were issued for EOP-004-1 (Disturbance Reporting) between 2009 and 2013—not all related to damage.

Metcalf happened on April 16, 2013, but then…

- No citations have been issued for EOP-004-2 (effective June 20, 2013)
- No citations have been issued for EOP-004-3 (effective November 19, 2015)
- No citations have been issued for EOP-004-4 (effective January 18, 2018)

And adding in the CIP-014 physical security Standard:

- No violation citations have been issued for CIP-014-1
- Four violation citations have been issued for CIP-014-2

---

[19] Available at: https://elibrary.ferc.gov/idmws/file_list.asp?document_id=14605551 (accessed January 29, 2020).
[20] Available at: https://www.nerc.com/files/CIP-001-1.pdf (accessed January 29, 2020).
[21] Available at: https://www.nerc.com/files/CIP-001-1a.pdf (accessed January 29, 2020).
[22] Available at: https://www.nerc.com/files/CIP-001-2a.pdf (accessed January 29, 2020).
[23] Available at: https://www.nerc.com/files/EOP-004-1.pdf (accessed January 29, 2020).
[24] FERC Order Approving Reliability Standard. 143 FERC ¶ 61,252. https://www.ferc.gov/whats-new/comm-meet/2013/062013/E-8.pdf (accessed January 29, 2020).
[25] Available at: https://www.nerc.com/files/EOP-004-2.pdf (accessed January 29, 2020).

- NP19-4-000 (one violation)
- NP18-14-000 (one violation)
- NP17-29-000 (two violations)

I emphasize: There have been only four (4) NERC Physical Security standard violations cited since the Metcalf attack.

Conclusion and Recommendations

Publicly available information indicates that: 1) the mandatory physical security standard is inadequate, and 2) enforcement of mandatory physical security standard seems nonexistent. I recommend that FERC take the following actions:

1. FERC should direct NERC to modify CIP-014-2 (Physical Security) to require that the entity's "Physical Security Plan" be effective and receive regulatory approval. The standard should specify that all "risk assessments" "evaluations" and "security plans" should be reviewed by qualified non-affiliated persons with expertise in physical security.

2. FERC should direct NERC to submit to the Commission for approval a compliance and enforcement plan for physical security that would provide meaningful assurances that the regulators and regulated entities are taking seriously their obligations to protect the bulk power system from physical threats.

3. FERC (in collaboration with DOE, DHS, DOD, and the National Guard) should "Red Team" entities in order to evaluate weaknesses and determine whether their physical security (and cybersecurity) programs are effective. FERC should work with state PUCs to ensure like actions at the state-level.

Respectfully submitted,

Michael Mabee

Attachment: 18 CFR § 385.206 Compliance Information

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;

- Contained in Complaint

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

- Contained in Complaint

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

- A widespread power outage as a result of the lack of physical security could cause the loss of life and substantial damage to the local or national economy.

(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;

- A widespread power outage as a result of the lack of physical security could cause the loss of life and substantial damage to the local or national economy.

(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 as a result of the lack of physical security could cause the loss of life and substantial damage to the local or national economy.

(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 open FERC docket on CIP-014-2

(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 "Conclusion and Recommendations" 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;

- Records related to the enforcement of CIP-014-2 are in the possession of the Commission and/or the Electric Reliability Organization ("ERO").

(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.

- N/A

(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 Electric Reliability Organization ("ERO") simultaneously with my filing with the Commission.

Respectfully submitted,

Michael Mabee

Exhibit B

Comments of Michael Mabee
U.S. Department of Energy
Request for Information (RFI) on
Ensuring the Continued Security of the United States Critical Electric Infrastructure

Note: Full copy with Exhibits available at:
https://michaelmabee.info/wp-content/uploads/2020/05/2020-05-11-Complaint-Mabeew-exhibits-1.pdf

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	**)**	

COMPLAINT

Submitted to FERC on May 11, 2020

Introduction

I am a private citizen who conducts public interest research on the security of the electric grid because I recognize the absolutely 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 filing this complaint under 16 U.S. Code § 824o(d)(5)[1] and 16 U.S. Code § 824o(e)(3)[2] because:

1) The mandatory Critical Infrastructure Protection (CIP) standard CIP-013-1 (Cyber Security Supply Chain Risk Management) does not comport with Presidential Executive Order 13920: Securing the United States Bulk-Power System[3], and

2) The Federal Energy Regulatory Commission (FERC) has not ensured that mandatory CIP standards "fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework."

---

[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.]

[2] "On its own motion ***or upon complaint***, the Commission may order compliance with a reliability standard and may impose a penalty against a user or owner or operator of the bulk-power system if the Commission finds, after notice and opportunity for a hearing, that the user or owner or operator of the bulk-power system has engaged or is about to engage in any acts or practices that constitute or will constitute a violation of a reliability standard." [Emphasis added.]

[3] Attached hereto as Exhibit A.

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 correct deficiencies.

Background

On July 21, 2016 FERC issued Order No. 829, Revised Critical Infrastructure Protection Reliability Standards.[4] In this order, FERC:

> "directs the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations."

CIP-013-1 was developed by NERC and approved by FERC on October 26, 2018[5] although the implementation date has been delayed.[6] As of this filing, the standard has yet to be implemented – almost 4 years after FERC directed the standard.

Notwithstanding the bureaucratic delays and onerous process to develop a standard, NERC has demonstrated a lack of urgency in protecting the bulk power system. This was clearly evidenced on February 14, 2019 in the Senate Committee on Energy and Natural Resources hearing entitled: "Hearing to Consider the Status and Outlook for Cybersecurity Efforts in the Energy Industry."[7]

Senator Angus King questioned NERC CEO James B. Robb on the supply chain risk management issue:

> **Sen. King:** "Okay let me ask another question. Do any of our utilities have Kaspersky, Huawei, or ZTE equipment in their system?"
>
> **Mr. Robb:** "We issued a NERC alert…"
>
> **Sen. King:** "I didn't ask you if you issued an alert. I asking you do any of our utilities have ZTE, Huawei, or Kaspersky equipment or software in their system?"
>
> **Mr. Robb:** "Not to my knowledge."

---

[4] Available at: https://www.ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf (Accessed May 10, 2020).
[5] See: https://www.govinfo.gov/content/pkg/FR-2018-10-26/pdf/2018-23201.pdf (Accessed May 10, 2020).
[6] See 171 FERC ¶ 61,052, issued April 17, 2020.
[7] Available at: https://www.energy.senate.gov/public/index.cfm/hearings-and-business-meetings?ID=FE0534E7-2FC7-4DB0-BEA6-2634D3821ADD# (accessed October 19, 2019).

Sen. King: "Not to your knowledge. Have you surveyed any of the utilities to determine that?"

Mr. Robb: "Uhhh, I don't believe we have."

Sen. King: "I think that would be a good idea, don't you?"

Mr. Robb: "I'll take that on."

In other words, two and a half years after FERC ordered the Cyber Security Supply Chain Risk Management standard, NERC hadn't even checked to see if there is Russian or Chinese equipment or software installed on the electric grid.

Complaint 1. The mandatory standard CIP-013-1 (Cyber Security - Supply Chain Risk Management) does not comport with Presidential Executive Order 13920.

Against the protest of numerous commenters in the docket, CIP-013-1 fails to cover all systems in the bulk power system. Section 4.2.3.5 of the standard excludes:

> "Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP002-5, or any subsequent version of that Reliability Standard."

In other words, the standard only covers high and medium impact systems and excludes supposed "low impact systems." Unfortunately, the discretion is left to the individual companies in the industry to decide what is "low impact."

On May 4, 2020, the President of the United States declared a national emergency and issued Executive Order 13920: "Securing the United States Bulk-Power System." This action by the President is a vote of no-confidence in the lackadaisical and inadequate actions of FERC and NERC. The Commission and the ERO have not done enough to protect the bulk power system from cyber threats. This indictment of the lack of action on the part of FERC and the ERO must be remedied.

The Executive order requires that the Secretary of Energy:

(i) identify bulk-power system electric equipment designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary that poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the bulk-power system in the United States, poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States, or otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons; and

(ii) develop recommendations on ways to identify, isolate, monitor, or replace such items as soon as practicable, taking into consideration overall risk to the bulk-power system.

This order invalidates the present scheme in CIP-013-1 in which each individual company has the discretion to decide the systems to which it wishes the standard to apply. The president of the United States has ordered the entire bulk power system protected.

Complaint 2. The Federal Energy Regulatory Commission (FERC) has not ensured that mandatory CIP standards fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

On May 21, 2008 Representative James R. Langevin, chairman of the House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, in his opening statement to a hearing on cybersecurity[8] noted:

> *As time passes, I grow particularly concerned by NERC, the self-regulating organization responsible for ensuring the reliability of the bulk power system. Not only do they propose cybersecurity standards that, according to the GAO and NIST, are inadequate for protecting critical national infrastructure, but throughout the committee's investigation they continued to provide misleading statements about their oversight of industry efforts to mitigate the Aurora vulnerability.*
>
> *If NERC doesn't start getting serious about national security, it may be time to find a new electric reliability organization. NERC can begin demonstrating its commitment by incorporating more of the NIST security controls in the next iteration of its reliability standards.*

Emphasis added. That hearing was in 2008. Eleven years later, FERC and NERC had still failed to ensure that the mandatory CIP standards addressed the NIST cybersecurity framework. In September of 2019, the Government Accountability Office (GAO) issued a report[9] finding:

> *The Federal Energy Regulatory Commission (FERC)—the regulator for the interstate transmission of electricity—has approved mandatory grid cybersecurity standards. However, it has not ensured that those standards fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework.*

Emphasis added. GAO include this table with their assessment of how well the current CIP standards address the NIST framework:

---

[8] "Implications of Cyber Vulnerabilities on the Resilience and Security of the Electric Grid." Before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. (110th Congress) May 21, 2008. https://www.gpo.gov/fdsys/pkg/CHRG-110hhrg43177/pdf/CHRG-110hhrg43177.pdf (accessed October 24, 2019). Hearing video available at: https://www.c-span.org/video/?205553-1/security-electric-grid (accessed October 24, 2019).

[9] U.S. Government Accountability Office. "Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid." GAO-19-332: Published: Aug 26, 2019. Publicly Released: Sep 25, 2019. Copy attached hereto as Exhibit B. Also available at: https://www.gao.gov/products/GAO-19-332 (accessed October 22, 2019).

Extent to Which FERC-Approved Cybersecurity Standards Address the National Institute of Standards and Technology Cybersecurity Framework's Identify and Protect Functions

Function	GAO assessment	Category	GAO assessment
Identify	◑	Asset management	◑
		Business environment	○
		Governance	◑
		Risk assessment	◕
		Risk management strategy	○
		Supply chain risk management	◑
Protect	◕	Identity management, authentication, and access control	●
		Awareness and training	◑
		Data security	◑
		Information protection processes and procedures	◕
		Maintenance	◑
		Protective technology	◑

Legend: ●—Fully address. ◕—Substantially address. ◑—Partially address. ◔—Minimally address. ○—Do not address.

Source: GAO analysis of Federal Energy Regulatory Commission (FERC)-approved cybersecurity standards. | GAO-19-332

The President of the United States and Congress are not alone in their criticism of the lack of action by FERC and NERC to protect the bulk power system.

On September 6, 2019, Cybersecurity expert George Cotter submitted an assessment in FERC Docket AD19-18-000 and NP19-4-000 entitled "Security in the North American Grid, The Existential Threat. A White Paper."[10] Mr. Cotter pointed out that:

> "only 1374 of a total of 16,412 BES Transmission Substations qualified for CIP Standards based on Kv power minimums (over 90% excluded) and of the qualifiers, only 550 (40%) were estimated by their utilities to be critical to BES Reliability."

In other words, the vast majority of facilities in the bulk power system are excluded from the CIP standards by their very design.

On May 4, 2020, Cybersecurity expert Joe Weiss pointed out in his blog[11] that:

> "China and Russia have directly attacked the control system vendor supply chains since at least 2010. Many of the systems exploited and affected by adversaries are still used in the U.S. bulk and distribution power systems. Moreover, vendors supplying bulk (and distribution) electric equipment for the U.S. electric system also supplied similar (often the same) bulk and distribution electric equipment to other countries, including China, Iran, Russia, and Pakistan. (I include distribution systems, as it often uses the same equipment as transmission systems, and transmission directly "talks" to distribution – more discussions on distribution follows). Even

[10] Attached hereto as Exhibit C
[11] Attached hereto as Exhibit D

> bulk power equipment manufactured in the U.S. often use servers, processors, software, etc. that come from China which makes assuring supply chain integrity so difficult."

And the supply chain threat is not hypothetical – it has actually happened. In his most recent article,[12] Mr. Weiss points out:

> "So why the EO now? Government and public utility procurement rules often push organizations into buying equipment due to price and without regard to origin or risk. In this case, it resulted in a utility having to procure a very large bulk transmission transformer from China. When the Chinese transformer was delivered to a US utility, the site acceptance testing identified electronics that should NOT have been part of the transformer – hardware backdoors. That transformer now resides at a government installation."

Our electric grid supply chain has already been targeted by state actors, as reported by Mr. Weiss and also by the Wall Street Journal. In a January 10, 2019 article,[13] the WSJ reported:

> "A reconstruction of the hack reveals a glaring vulnerability at the heart of the country's electric system. Rather than strike the utilities head on, the hackers went after the system's unprotected underbelly—hundreds of contractors and subcontractors like All-Ways who had no reason to be on high alert against foreign agents. From these tiny footholds, the hackers worked their way up the supply chain. Some experts believe two dozen or more utilities ultimately were breached."

On May 4, 2020, the President of the United States declared a national emergency and issued Executive Order 13920: "Securing the United States Bulk-Power System." This is a true emergency and the Commission should act on this complaint with a sense of urgency.

Conclusion and Recommendations

The mandatory Critical Infrastructure Protection (CIP) standard CIP-013-1 (Cyber Security - Supply Chain Risk Management) does not comport with Presidential Executive Order 13920: Securing the United States Bulk-Power System.

As noted by Congress in 2008 and the GAO in 2019, the Federal Energy Regulatory Commission (FERC) has not ensured that mandatory CIP standards "fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework."

1. The Commission should direct NERC to Modify CIP-013-1 (Cyber Security - Supply Chain Risk Management) to cover every piece of equipment in the bulk power system with no exceptions including purported "low impact" BES cyber systems. Utilities should not have the discretion to decide what parts of the bulk power system they wish to protect.

---

[12] Attached hereto as Exhibit E.

[13] Smith, Rebecca. The Wall Street Journal. "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It." January 10, 2019. https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112 (accessed May 11, 2020).

2. The Commission should direct NERC to revamp all CIP standards to "fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework."

Respectfully submitted,

Michael Mabee

Attachment: 18 CFR § 385.206 Compliance Information

Exhibit C

Comments of Michael Mabee
U.S. Department of Energy
Request for Information (RFI) on
Ensuring the Continued Security of the United States Critical Electric Infrastructure

Note: Full copy with Exhibits available at:
https://michaelmabee.info/wp-content/uploads/2021/03/FERC-Complaint-Mabee-Final-w-Exhibits.pdf

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Complaint of Michael Mabee	**)**	
Related to Mandatory Reliability Standards	**)**	**Docket No. _____**
in the Texas Grid Collapse of 2021	**)**	

COMPLAINT
Submitted to FERC on February 28, 2021

Introduction

I am a private citizen who conducts public interest research on the security of the electric grid because I recognize the absolutely 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 a resident of Texas and was adversely impacted by the February 15, 2021 Texas grid collapse.

I am filing this complaint under 16 U.S. Code § 824o(d)(5)[1] and 16 U.S. Code § 824o(e)(3)[2] because, the Texas blackout on February 15, 2021 demonstrates that either:

1) The mandatory reliability standards were not followed, or,
2) The mandatory reliability standards were ineffective.

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 correct deficiencies.

---

[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.]

[2] "On its own motion ***or upon complaint***, the Commission may order compliance with a reliability standard and may impose a penalty against a user or owner or operator of the bulk-power system if the Commission finds, after notice and opportunity for a hearing, that the user or owner or operator of the bulk-power system has engaged or is about to engage in any acts or practices that constitute or will constitute a violation of a reliability standard." [Emphasis added.]

Background of Texas Grid Collapse of 2021

On February 11, 2021, the Electric Reliability Council of Texas (ERCOT) issued a press release warning that "Extreme cold weather expected to result in record electric use in ERCOT region."[3] (This press release is attached as Exhibit A.) The press release advised:

> "This statewide weather system is expected to bring Texas the coldest weather we've experienced in decades," said ERCOT President and CEO Bill Magness. "With temperatures rapidly declining, we are already seeing high electric use and anticipating record-breaking demand in the ERCOT region."

On February 14, 2021, ERCOT issued another press release: "Grid operator requests energy conservation for system reliability."[4] (This press release is attached as Exhibit B.) The press release advised:

> "We are experiencing record-breaking electric demand due to the extreme cold temperatures that have gripped Texas," said ERCOT President and CEO Bill Magness. "At the same time, we are dealing with higher-than-normal generation outages due to frozen wind turbines and limited natural gas supplies available to generating units. We are asking Texans to take some simple, safe steps to lower their energy use during this time."

On February 15, 2021, ERCOT issued a third press release: "ERCOT calls for rotating outages as extreme winter weather forces generating units offline - Almost 10,000 MW of generation lost due to sub-freezing conditions."[5] (This press release is attached as Exhibit C.) The press release, in its entirety, advised:

> AUSTIN, TX, Feb. 15, 2021 – The Electric Reliability Council of Texas (ERCOT) entered emergency conditions and initiated rotating outages at 1:25 a.m. today.
>
> About 10,500 MW of customer load was shed at the highest point. This is enough power to serve approximately two million homes.
>
> Extreme weather conditions caused many generating units – across fuel types – to trip offline and become unavailable.
>
> There is now over 30,000 MW of generation forced off the system.
>
> "Every grid operator and every electric company is fighting to restore power right now," said ERCOT President and CEO Bill Magness.
>
> Rotating outages will likely last throughout the morning and could be initiated until this weather emergency ends.

---

[3] Available at: http://www.ercot.com/news/releases/show/224996
[4] Available at: http://www.ercot.com/news/releases/show/225151
[5] Available at: http://www.ercot.com/news/releases/show/225210

Impact on the People of Texas

The reality on the ground in Texas was a little less sterile than "10,500 MW of customer load was shed."[6]

People died. Critical infrastructures were impacted.

Over 4,000,000 customers lost power during two days of subfreezing temperatures. Many lost power for longer. The picture on the right is the temperature at 5:21 a.m. on February 16, 2021 when many of us in Texas had already been without power for over 24 hours. The Houston Chronicle reported[7] that day that:

> Harris County has seen more than 300 carbon monoxide poisoning cases as temperatures bottomed out Monday in Houston and the state's electricity grid failed, sending people scrambling for heat sources. That includes 90 carbon monoxide poisoning calls to the Houston Fire Department and 100 cases in Memorial Hermann's emergency rooms.

Desperate people, who depended on the electric grid, tried any means they could find to keep their families from freezing – sometimes with catastrophic results. According to the article:

> Several people have already died seeking warmth. A woman and an 8-year-old girl died from suspected carbon monoxide poisoning in Sharpstown, while a man and a 7-year-old boy were taken to a nearby hospital in critical condition. Three children and their grandmother died in a Sugar Land house fire after using the fireplace to heat their home.

The Wall Street Journal reported on February 23, 2021 that "Officials are still counting fatalities from hypothermia, carbon monoxide, other factors as some experts warn accurate total might never be known."[8] The article reported:

> The failure of the state's electrical grid during the weeklong cold snap left more than four million Texans without electricity and heat, many for days on end in subfreezing temperatures. Many residents also lost access to water, and 14.6 million were ordered to boil water to make it safe to drink.
>
> …

[6] In fact, Mr. Magness later testified to the Texas State Legislature that 20,000 MW was shed.
[7] Houston Chronicle. "Harris County is slammed with 300+ carbon monoxide cases - and many are kids." March 16, 2021. Available at: https://www.houstonchronicle.com/news/houston-texas/health/article/Memorial-Hermann-sees-60-carbon-monoxide-15954216.php
[8] Wall Street Journal. "Full Death Toll From Texas Storm Could Take Months to Determine." February 23, 2021. Available at: https://www.wsj.com/articles/full-death-toll-from-texas-storm-could-take-months-to-determine-11614107708

> An 11-year-old boy was found frozen in his bed, his family told the Houston Chronicle. A grandmother and three grandchildren died in a house fire as they were trying to stay warm, the Chronicle also reported. At least six deaths occurred near the Abilene area, local media reported, including a patient who couldn't get medical treatment due to a lack of water and three elderly men who were found dead in subfreezing homes.

A copy of this Wall Street Journal article is attached as Exhibit D.

Impact on Texas Critical Infrastructures

Presidential Policy Directive 21 (PPD-21) "Critical Infrastructure Security and Resilience"[9] identifies the 16 critical infrastructures in the U.S. and mandates that:

> The Federal Government shall work with critical infrastructure owners and operators and SLTT [state, local, tribal, and territorial] entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof.

The Texas grid collapse beginning on February 15, 2021 adversely impacted critical infrastructures. Many people may have never heard of PPD-21, but this is what the failure of the critical infrastructures looks like to the people with no power trying to survive in subfreezing temperatures:

Bread isle, Kroger's Fort Worth, TX
February 18, 2021

Water isle, Kroger's Fort Worth, TX
February 18, 2021

[9] Available at: https://fas.org/irp/offdocs/ppd/ppd-21.pdf

Egg case, Kroger's Fort Worth, TX
February 18, 2021

Milk case, Kroger's Fort Worth, TX
February 18, 2021

Here is another example of what critical infrastructure impact looks like to the actual people suffering through it:

QT Gas Station, Lake Worth, TX
February 19, 2021

In addition to the food, agriculture and transportation sectors, the collapse of the water infrastructure has been well covered in press articles.[10] Millions in Texas were under "boil water" orders as the water infrastructure was impacted by the collapse of the grid and many had no water at all. Firefighters watched helplessly as homes burned and they lacked the water to fight the fires.[11]

Some people froze in their homes and those that survived struggled for food and water when the critical infrastructures collapsed along with the Texas electric grid.

This is what the failure of electric reliability standards looks like. People dead, homes destroyed, critical infrastructures failing and the economy severely impacted. [12] (Photo credit: Bexar-Bulverde Volunteer Fire Department.)

Lessons Learned from 2011 and 1989 Texas Blackouts Ignored

In 2021 we find, as Yogi Berra once said, "It's déjà vu all over again." Almost exactly 11 years prior to the collapse of the Texas grid in February of 2021, a very similar thing happened in February 2011. And before that, another similar blackout occurred in December of 1989. While the causes of the 2021 Texas grid collapse are still under investigation, many similarities between the three tragic incidents are apparent.

The Austin American-Statesman reported[13] on February 18, 2021:

---

[10] NBC News. "Texas water shortage adds to power crisis as new winter storm moves in." February 17, 2021. https://www.nbcnews.com/news/us-news/texas-contending-water-nightmare-top-power-crisis-n1258208

[11] New York Times. "A Texas apartment building burned while firefighters scrambled for water." February 19, 2021 https://www.nytimes.com/2021/02/19/us/san-antonio-fire-hydrants-water.html

[12] Foundation for Resilient Societies. "Causes and Costs of ERCOT Load Sheds in February 2021." February 24, 2021 (Preliminary). https://www.resilientsocieties.org/uploads/5/4/0/0/54008795/ercot_load_shed_causes_and_costs_preliminary_feb_25_2021.pdf

[13] Austin American-Statesman / USA Today. "Winter storm blackouts plagued Texas in 2011, too. Recommendations made afterward went unenforced." February 18, 2021. https://www.usatoday.com/story/news/nation/2021/02/18/state-energy-winter-protections-lacking-reports-have-suggested/4490501001/

> Failing power plants, rolling blackouts and a spike in demand as Texas is hijacked by a harsh February winter snowstorm – this was the scenario exactly a decade ago as blackouts rolled through Texas.
>
> A post-mortem at the time – including a key finding that state officials recommended but did not mandate winter protections for generating facilities – has renewed relevance as Texas is roiled by a record storm that has left millions without power for at least three days amid plunging temperatures.
>
> A combination of those 2011 findings, as well as reports from the state grid operators that generators and natural gas pipelines froze during the current calamity and Austin American-Statesman interviews with current and former utility executives and energy experts, ***suggest a light regulatory touch and cavalier operator approach involving winter protections of key industrial assets.***

(Emphasis added.)

While it appears that a lot of lessons were learned from the 2011 Texas blackout. it also appears that few steps were taken to harden the Texas grid against a similar event in the future (i.e., the 2021 Texas blackout).

According to an August 2011 Joint report of the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC)[14]:

> Between February 1 and February 4, a total of 210 individual generating units within the footprint of the Electric Reliability Council of Texas, Inc. (ERCOT), which covers most of Texas, experienced either an outage, a derate, or a failure to start. The loss of generation was severe enough on February 2 to trigger a controlled load shed of 4000 MW, which affected some 3.2 million customers. On February 3, local transmission constraints coupled with the loss of local generation triggered load shedding for another 180,000 customers in the Rio Grande Valley in south Texas.

(A copy of this report is attached as Exhibit E.) It is important to note, that prior to the 2011 Texas blackout, there had been another blackout in 1989 which bears striking similarities to 2011 and 2021. The Joint FERC/NERC report noted:

> The experiences of 1989 are instructive, particularly on the electric side. In that year, as in 2011, cold weather caused many generators to trip, derate, or fail to start. The PUCT investigated the occurrence and issued a number of recommendations aimed at improving winterization on the part of the generators. These recommendations were not mandatory, and over the course of time implementation lapsed. Many of the generators that experienced outages in 1989 failed again in 2011.[15]

---

[14] Federal Energy Regulatory Commission and the North American Electric Reliability Corporation. "Report on Outages and Curtailments During the Southwest Cold Weather Event of February 1-5, 2011." August 2011. https://www.ferc.gov/sites/default/files/2020-05/ReportontheSouthwestColdWeatherEventfromFebruary2011Report.pdf

[15] id. Page 10.

Benjamin Disraeli famously said: "What we learn from history is that we do not learn from history." In the present context, the people of Texas have suffered blackouts in 1989, 2011 and 2021 – all bearing remarkable – and preventable similarities. All having at least something to do with the lack of winterization of equipment and ill-preparedness for extreme cold weather.

In 2011, the regulators were comparing the 2011 blackout to 1989. On April 11, 2011, The Austin American Statesman reported[16]:

> The report from the Public Utility Commission of Texas is clear in its analysis of what went wrong:
>
> "The winter freeze greatly strained the ability of the Texas electric utilities to provide reliable power to their customers. Record and near-record low temperatures were felt throughout the state resulting in a significantly increased demand for electrical power.
>
> "At the same time that demand was increasing, weather-related equipment malfunctions were causing generating units to trip off the line." As a result, it noted, the state suffered widespread rolling blackouts and "near loss of the entire ERCOT electric grid."
>
> ERCOT is still the Electric Reliability Council of Texas. But the PUC report wasn't analyzing the power outages that hit a large swath of Texas when temperatures plunged this past February. The report is dated November 1990 and is referring to the record freeze of late December 1989.
>
> The PUC has a single remaining copy of it in its library north of the Capitol.

The report referred to in the article is Public Utility Commission of Texas report: "Electric Utility Response to the Winter Freeze of December 21 to December 23, 1989."[17] (A copy of this report is attached as Exhibit F.)

The 2011 blackout caused a flurry of investigations, hearings, reports and public outrage. Multiple Hearings, Investigations, Reports — and ultimately inaction.

On February 26, 2021 the Houston Chronicle reported[18]:

> A decade ago, after an Arctic cold spell knocked out power and left millions of Texans shivering in the dark, the Public Utility Commission's enforcement apparatus swung into action. Their aim: punish the companies that had promised but failed to deliver electricity in an emergency.
>
> Specialists contracted by the state agency worked with an enforcement team the utility commission created four years earlier. More recently, it had added lawyers whose only job was

[16] Austin American Statesman. "February power blackouts across Texas echoed 1989 failures, state report shows." April 11, 2011. https://www.statesman.com/article/20110411/NEWS/304119704

[17] Available at: https://lrl.texas.gov/scanned/archive/1990/15303.pdf

[18] Houston Chronicle. "'Muzzled and eviscerated': Critics say Abbott appointees gutted enforcement of Texas grid rules." February 26, 2021. https://www.houstonchronicle.com/politics/texas/article/critics-abbott-power-grid-rules-texas-deadly-storm-15982421.php

> to pursue wrong-doing. The energy companies eventually paid fines and settlements totaling hundreds of thousands of dollars for failing to prepare for the extreme weather.
>
> Two weeks ago, history repeated. Millions of residents were left without power and water in below-freezing temperatures. The damage far exceeded the 2011 storm. Nearly a third of the grid's power plants went offline. Dozens of deaths have been attributed to the event, with a full accounting yet to come.
>
> But the enforcement tools that worked to hold companies accountable for the 2011 failures had been removed under Gov. Greg Abbott's appointees on the utility commission. Hearst Newspapers reported last week that commissioners in November cut ties with the Texas Reliability Entity — the specialists hired — leaving state regulators without an external independent reliability monitor.
>
> Four months before that, the governor's commissioners had also disbanded the Oversight & Enforcement Division. The head attorney was told he no longer had a job; nine other team members were reassigned throughout the utility commission.
>
> Several pending cases were dropped. According to commission records, by the end of 2020 the number of enforcement cases had fallen 40 percent.

The 2011 Joint FERC/NERC report noted:

> On February 14, the Federal Energy Regulatory Commission (FERC) initiated an inquiry into the Southwest outages and service disruptions. The inquiry had two objectives: to identify the causes of the disruptions, and to identify any appropriate actions for preventing a recurrence of the disruptions. FERC stated it was not at that time initiating an investigation into whether there may have been violations of applicable regulations, requirements or standards under FERC's jurisdiction, and that any decisions on whether to initiate enforcement investigations would be made later. Consequently, while this report describes actions which in some cases appear to warrant further investigation, it does not reach any conclusions as to whether violations have occurred.

It seems nobody wants to tell the industry to fix grid security issues in Texas, thus they do not get fixed. This regulatory inaction is causing deaths, impacts to the critical infrastructures, and economic loss — it is unacceptable.

The 2011 Texas blackout was followed by many promises but little action. The Electric Reliability Council of Texas (ERCOT) made many promises, including "ERCOT will be an active participant in the discussion related to the adequate weatherization of generation units."[19]

In 2021, It doesn't seem that this "discussion" was fruitful.

One of the Key Findings in the FERC and NERC Joint 2011 report was:

---

[19] ERCOT "Review of February 2, 2011 Energy Emergency Alert (EEA) Event." February 14, 2011. http://www.ercot.com/content/meetings/board/keydocs/2011/0214/Review_of_February_2,_2011_EEA_Event.pdf

> During the February event, temperatures were considerably lower (15 degrees plus) than average winter temperatures, and represented the longest sustained cold spell in 25 years. Steady winds also accelerated equipment heat loss. However, such a cold spell was not unprecedented. The Southwest also experienced temperatures considerably below average, accompanied by generation outages, in December 1989. Less extreme cold weather events occurred in 2003 and 2010. ***Many generators failed to adequately apply and institutionalize knowledge and recommendations from previous severe winter weather events, especially as to winterization of generation and plant auxiliary equipment.***

(Emphasis added.)

Recommendations related to extreme cold weather and winterization in the FERC and NERC Joint 2011 report have apparently not been heeded. Similar recommendations of the Public Utility Commission of Texas after the 1989 Texas blackout were also not heeded.

The Foundation for Resilient Societies has done a preliminary analysis on the costs of the 2021 blackout versus the cost of mitigation.[20] These data demonstrate that it would have cost substantially less to mitigate the 2021 disaster than the disaster has actually cost us. To paraphrase the old adage, "an ounce of prevention is cheaper than a pound of disaster." And yet we continue in this cycle of inaction and disaster. 1989. 2011. 2021.

Somebody is going to have to pay for this disaster. The taxpayers or the ratepayers. Unfortunately, I am both so I will pay. But perhaps I shouldn't complain. Many people have paid for these disasters in 1989, 2011 and 2021 with their lives.

I implore the Commission: Stop asking and recommending. It is time to direct NERC and Texas RE to take action. Violators of reliability standards must be held accountable and we must make sure that this cycle of blackouts, deaths, critical infrastructure impacts and damage to the economy stops.

---

[20] Foundation for Resilient Societies. "Causes and Costs of ERCOT Load Sheds in February 2021." February 24, 2021 (Preliminary).
https://www.resilientsocieties.org/uploads/5/4/0/0/54008795/ercot_load_shed_causes_and_costs_preliminary_feb_25_2021.pdf

If we were not prepared for a known incoming weather event, are we prepared for other events?

I conducted an analysis of the reported electric disturbance events between 2010 and 2020 from the Department of Energy OE-417 Electric Disturbance Reports.[21] (I have attached a copy of my analysis as Exhibit G.)

All NERC Regions		
Events From 2010-2020	Total	%
Weather	961	52.6%
Cyber Attack	37	2.0%
Physical Attack	721	39.5%
Fuel Supply Deficiency	74	4.1%
Equipment	15	0.8%
Natural Disaster	14	0.8%
Wildfire	5	0.3%
Generation Interruption	17	3.4%
Transmission Interruption	113	22.8%
Distribution Interruption	9	1.8%
Operations	185	37.3%
Islanding	67	13.5%
Load Shed	30	6.0%
Public Appeal	65	13.1%
?	10	2.0%
Total OE-417 Reports	**2323**	
Cause Known from OE-417	**1827**	
Cannot Determine Cause	**496**	

According to my analysis, 52.6% of OE-417 disturbance reports filed nationwide in the last decade are weather related.

Interestingly, 70.9% of the disturbances reported in the Texas RE region are weather related. The Commission needs to ask why this difference exists and whether mandatory reliability standards are either being followed or are effective.

Texas RE Only		
Events From 2010-2020	Total	%
Weather	83	70.9%
Cyber Attack	3	2.6%
Physical Attack	28	23.9%
Fuel Supply Deficiency	3	2.6%
Equipment	0	0.0%
Natural Disaster	0	0.0%
Wildfire	0	0.0%
Generation Interruption	4	7.1%
Transmission Interruption	17	30.4%
Distribution Interruption	2	3.6%
Operations	11	19.6%
Islanding	1	1.8%
Load Shed	0	0.0%
Public Appeal	21	37.5%
?	0	0.0%
Total OE-417 Reports	**173**	
Cause Known from OE-417	**117**	
Cannot Determine Cause	**56**	

If we are not adequately prepared for a weather event that is forecast well in advance, such as the 2021 Texas grid collapse, are we ready for other threats?

Mike Rogers, former chairman of the House Intelligence Committee, recently noted in an article entitled "Why America would not survive a real first strike cyberattack today"[22]:

> The only thing that prevented the Russians from launching a destructive malware attack or inserting malicious code was the Russians themselves. They could have caused a major disruption across our government and private sector networks, changing or deleting data, planting viruses, or simply turning off the networks. Restarting the systems and deleting the offending code alone is not a solution. In 2016, the Ukrainian electricity grid was targeted by the Russians and, until this day, the country is still finding and removing vulnerabilities left behind by Moscow.

[21] See: https://michaelmabee.info/oe-417-database/

[22] Rogers, Mike. "Why America would not survive a real first strike cyberattack today." February 22, 2021. https://thehill.com/opinion/cybersecurity/539826-we-would-not-survive-true-first-strike-cyberattack?rl=1

If we are unable to prepare our electric grid and its dependent critical infrastructures from a cold snap that we see coming over a week away, it begs the question: Are we prepared for a cyberattack?[23] Are we prepared for a coordinated physical attack?[24] Are we prepared for a major geomagnetic disturbance (GMD) event? Are we prepared for an electromagnetic pulse (EMP) attack? Are we prepared for other extreme weather events?

Relief Sought

1. The Federal Energy Regulatory Commission should direct the North American Electric Reliability Corporation (NERC) and its regional entity, Texas Reliability Entity, Inc. (Texas RE) to conduct a comprehensive investigation into whether reliability standards were followed by all entities registered with Texas RE who had any involvement in the Texas grid collapse of February 15, 2021.

2. If the North American Electric Reliability Corporation (NERC) and its regional entity, Texas Reliability Entity, Inc. (Texas RE) determine that violations of reliability standards did not contribute to the Texas grid collapse of February 15, 2021, then the Federal Energy Regulatory Commission should direct the North American Electric Reliability Corporation (NERC) to improve the reliability standards to prevent catastrophic power outages such as this from occurring in the future.

Respectfully submitted,

Michael Mabee

Attachments: 18 CFR § 385.206 Compliance Information
Draft Notice
Exhibits A-G

[23] The Commission dismissed my complaint about inadequate supply chain cyber security CIP standards on October 2, 2020. Docket Number EL20-46-000.
[24] The Commission dismissed my complaint about inadequate physical security CIP standards on June 9, 2020. Docket Number EL20-21-000.

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;

- Contained in Complaint

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

- Contained in Complaint

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

- A widespread power outage in Texas on February 15, 2021 caused the loss of life and substantial damage to the economy.

(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;

- A widespread power outage in Texas on February 15, 2021 caused the loss of life and substantial damage to the economy.

(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 in Texas on February 15, 2021 caused the loss of life and substantial damage to the economy.

(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 Texas Power Outage of 2021.

(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 Electric Reliability Organization ("ERO") and the Texas Reliability Entity, Inc. simultaneously with my filing with the Commission.

Respectfully submitted,

Michael Mabee

Exhibit D

Comments of Michael Mabee
U.S. Department of Energy
Request for Information (RFI) on
Ensuring the Continued Security of the United States Critical Electric Infrastructure

OE-417 Electric Emergency and Disturbance Report - Calendar Year 2021										
Month	**Date Event Began**	**Time Event Began**	**Date of Restoration**	**Time of Restoration**	**Area Affected**	**NERC Region**	**Alert Criteria**	**Event Type**	**Demand Loss (MW)**	**Number of Customers Affected**
February	02/01/2021	11:25 PM	02/02/2021	1:12 AM	Texas: Kleberg County;	TRE	Unexpected Transmission loss within its area, contrary to design, of three or more Bulk Electric System Facilities caused by a common disturbance (excluding successful automatic reclosing).	Transmission Interruption	13	6102
February	02/07/2021	6:57 AM	02/07/2021	7:34 AM	Texas: Cameron County;	TRE	Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. Or suspicious device or activity at its Facility.	Suspicious Activity	0	0
February	02/10/2021	3:00 PM	02/23/2021	3:00 PM	Texas:	TRE	Loss of electric service to more than 50,000 customers for 1 hour or more.	Severe Weather	Unknown	2000000
February	02/12/2021	3:30 PM	02/22/2021	7:30 AM	Texas:	TRE	Fuel supply emergencies that could impact electric power system adequacy or reliability.	Fuel Supply Deficiency	Unknown	Unknown
February	02/13/2021	1:30 PM	02/20/2021	8:00 AM	Texas:	TRE	Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System.	Severe Weather	Unknown	Unknown
February	02/14/2021	8:30 AM	02/19/2021	6:00 PM	Texas:	TRE	Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System.	Severe Weather	7214	Unknown
February	02/14/2021	8:30 AM	02/19/2021	6:00 PM	Texas:	TRE	Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System.	Severe Weather	Unknown	Unknown
February	02/15/2021	1:20 AM	02/18/2021	12:42 AM	Texas: Hidalgo County, Cameron County;	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	Unknown	Unknown
February	02/15/2021	1:20 AM	02/18/2021	12:02 AM	Texas: Harris County;	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	4966	1390000
February	02/15/2021	4:00 PM	02/15/2021	6:34 PM	Texas: Travis County;	TRE	Complete loss of monitoring or control capability at its staffed Bulk Electric System control center for 30 continuous minutes or more.	System Operations	0	0

OE-417 Electric Emergency and Disturbance Report - Calendar Year 2021										
Month	**Date Event Began**	**Time Event Began**	**Date of Restoration**	**Time of Restoration**	**Area Affected**	**NERC Region**	**Alert Criteria**	**Event Type**	**Demand Loss (MW)**	**Number of Customers Affected**
February	02/15/2021	12:00 AM	Unknown	Unknown	Texas:	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	500	Unknown
February	02/15/2021	5:36 AM	Unknown	Unknown	Texas:	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	300	Unknown
February	02/15/2021	1:00 PM	02/20/2021	10:00 AM	Texas:	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	Unknown	175000
February	02/15/2021	1:54 AM	02/17/2021	11:56 PM	Texas:	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	524	Unknown
February	02/15/2021	1:20 AM	02/19/2021	9:00 AM	Texas:	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	7214	Unknown
February	02/15/2021	2:51 AM	02/19/2021	9:00 AM	Texas: Travis County;	TRE	Loss of electric service to more than 50,000 customers for 1 hour or more.	Severe Weather	Unknown	219306
February	02/15/2021	1:54 AM	02/19/2021	9:00 AM	Texas: Travis County;	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	724	Unknown
February	02/15/2021	3:06 AM	Unknown	Unknown	Texas: Bexar County;	TRE	Loss of electric service to more than 50,000 customers for 1 hour or more.	Severe Weather	Unknown	154000
February	02/15/2021	5:27 AM	02/18/2021	8:18 AM	Texas:	TRE	Total generation loss, within one minute of: greater than or equal to 2,000 Megawatts in the Eastern or Western Interconnection or greater than or equal to 1,400 Megawatts in the ERCOT Interconnection.	Severe Weather	Unknown	Unknown
February	02/15/2021	1:23 AM	02/19/2021	5:30 AM	Texas:	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	Unknown	Unknown

OE-417 Electric Emergency and Disturbance Report - Calendar Year 2021										
Month	**Date Event Began**	**Time Event Began**	**Date of Restoration**	**Time of Restoration**	**Area Affected**	**NERC Region**	**Alert Criteria**	**Event Type**	**Demand Loss (MW)**	**Number of Customers Affected**
February	02/15/2021	10:24 AM	02/18/2021	9:52 AM	Texas: Lubbock County;	TRE	Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System.	Severe Weather	116	29942
February	02/15/2021	6:00 PM	02/15/2021	11:55 PM	Texas:	TRE	Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System.	Severe Weather	Unknown	Unknown
February	02/15/2021	5:40 AM	02/16/2021	1:11 PM	Texas:	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	800	Unknown
February	02/15/2021	6:45 AM	Unknown	Unknown	Texas: Arkansas:	TRE	Loss of electric service to more than 50,000 customers for 1 hour or more.	Severe Weather	Unknown	Unknown
February	02/15/2021	7:52 AM	02/17/2021	2:15 PM	Texas: Austin County, Bastrop County, Burleson County, Caldwell County, Colorado County, Fayette County, Gonzales County, Guadalupe County, Hays County, Lee County, Milam County, Travis County, Washington County, Williamson County;	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	107	25000
February	02/15/2021	6:00 PM	02/15/2021	11:59 PM	Texas:	TRE	Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System.	Severe Weather	Unknown	Unknown
February	02/15/2021	1:20 AM	Unknown	Unknown	Texas:	TRE	Loss of electric service to more than 50,000 customers for 1 hour or more.	Severe Weather	360	72000
February	02/15/2021	9:10 AM	Unknown	Unknown	Texas: Randall County;	TRE	Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System.	Severe Weather	0	0
February	02/15/2021	5:36 AM	Unknown	Unknown	Texas:	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	300	Unknown

OE-417 Electric Emergency and Disturbance Report - Calendar Year 2021										
Month	**Date Event Began**	**Time Event Began**	**Date of Restoration**	**Time of Restoration**	**Area Affected**	**NERC Region**	**Alert Criteria**	**Event Type**	**Demand Loss (MW)**	**Number of Customers Affected**
February	02/15/2021	12:00 AM	Unknown	Unknown	Texas:	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	500	Unknown
February	02/16/2021	5:45 PM	02/16/2021	7:15 PM	Texas: Travis County;	TRE	Unplanned evacuation from its Bulk Electric System control center facility for 30 continuous minutes or more.	System Operations	0	0
February	02/16/2021	6:35 PM	02/17/2021	1:00 AM	Texas:	TRE	Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System.	Fuel Supply Deficiency	Unknown	Unknown
February	02/16/2021	11:28 PM	Unknown	Unknown	Texas:	TRE	Unplanned evacuation from its Bulk Electric System control center facility for 30 continuous minutes or more.	System Operations	0	0
February	02/16/2021	7:40 PM	02/17/2021	1:00 AM	Texas:	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	538	Unknown
February	02/16/2021	7:17 AM	02/16/2021	10:08 AM	Texas:	TRE	Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System.	Severe Weather	168	840000
February	02/16/2021	4:26 AM	Unknown	Unknown	Texas:	TRE	Firm load shedding of 100 Megawatts or more implemented under emergency operational policy.	Severe Weather	300	Unknown
February	02/17/2021	6:00 PM	02/17/2021	11:00 PM	Texas:	TRE	Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System.	Severe Weather	Unknown	Unknown
February	02/17/2021	6:38 AM	02/17/2021	8:37 AM	Texas: Travis County;	TRE	Complete loss of monitoring or control capability at its staffed Bulk Electric System control center for 30 continuous minutes or more.	System Operations	0	0
February	02/19/2021	9:00 PM	02/20/2021	1:00 PM	Texas:	TRE	Cyber event that causes interruptions of electrical system operations.	Cyber Event	Unknown	0
February	02/28/2021	12:42 PM	02/28/2021	1:22 PM	Texas:	TRE	Complete loss of monitoring or control capability at its staffed Bulk Electric System control center for 30 continuous minutes or more.	System Operations	0	0

Exhibit E

Comments of Michael Mabee
U.S. Department of Energy
Request for Information (RFI) on
Ensuring the Continued Security of the United States Critical Electric Infrastructure

Table B.2. Major Disturbances and Unusual Occurrences, 2003
(Continued)

Date	NERC Region	Time	Area	Type of Disturbance	Loss (megawatts)	Number of Customers Affected [1]	Restoration Time
August							
8/14/2003	ECAR	Approximately 3:00 p.m.	Geographic areas for MISO Reliability Coordination footprint: Michigan and Ohio	Unknown *	Approx. 18,500 MW, in MISO area: First Energy 7,500 Detroit Edison 9,200 Consumers Energy 1,800	NA	Approximately 8/17/03, 5:00 p.m.
8/14/2003	ECAR	4:09 p.m.	Southeastern Michigan including all of Detroit	Unknown *	11,000	2,100,000	8/16/03, 7:00 a.m.
8/14/2003	ECAR	4:09 p.m.	Southern Lower Michigan and small areas near Flint, Alma, Saginaw, and Lansing Michigan	Unknown *	1,007	101,000	8/16/03, 1:03 p.m.
8/14/2003	ECAR	4:10 p.m.	Northeast, Ohio	Unknown *	7,000	1,203,000	8/16/03, 8:27 p.m.
8/14/2003	NPCC	4:10 p.m.	Southwestern Connecticut and a small portion of Western Massachusetts and Vermont	Unknown *	2,500	NA	8/16/03, 3:45 a.m. Restoration ended; 8/17/03, 7:00 p.m., incident ended
8/14/2003	NPCC	4:10 p.m.	New York State	Unknown *	22,934	unknown	8/18/03, 12:03 a.m.
8/14/2003	NPCC	4:10 p.m.	New York-Buffalo to Albany; Ontario, Canada to Pennsylvania	Unknown *	NA	840,137	8/14/03, 11:48 p.m.
8/14/2003	MAAC	4:10 p.m.	Northern New Jersey Erie, Pennsylvania area	Unknown *	4,100 MW (Northern NJ) and 400 MW, (Erie, PA) area	NA	Approximately 8/15/03, 6:00 a.m.
8/14/2003	NPCC	4:11 p.m.	Entire Con Edison System (five boroughs of NYC and Westchester County)	Unknown *	11,202	3,125,350	8/15/03, 9:03 p.m.

[1] = Estimated Values.

* Information as provided by the respondent. The occurrence is, however, associated with the massive blackout of August 14, 2003. For further information, refer to the Interim Report: Causes of the August 14 Blackout in the United States and Canada, November 2003 at http://www.energy.gov/engine/content.do.

Note: North American Electric Reliability Council region acronyms are defined in the glossary.

Source: Form EIA-417, "Electric Emergency Incident and Disturbance Report."

Exhibit F

Comments of Michael Mabee
U.S. Department of Energy
Request for Information (RFI) on
Ensuring the Continued Security of the United States Critical Electric Infrastructure

organizations, public utility commissions, and public service companies), and businesses that sell motor vehicles through the websites of the Department of Transportation and the Department of Energy, social media, and other methods—

(A) to provide the resource guide under paragraph (1) to interested stakeholders, including relevant consumer groups and transportation-related organizations;

(B) to promote the use of electric vehicles in both government and industry fleets; and

(C) to educate individuals involved in the sale of motor vehicles about the benefits of electric vehicles.

(5) SUBSEQUENT RESOURCE GUIDES.—Not less frequently than every 2 years for the duration of the working group, the working group shall publish an update to the resource guide under paragraph (1), as appropriate based on technological innovation and subsequent information.

(6) ACCESSIBILITY.—The Secretaries shall each maintain the resource guide under paragraph (1) on a designated website, which may be an existing website, of each Secretary relating to electric vehicles.

(d) COORDINATION.—To the maximum extent practicable, the Secretaries and the working group shall carry out this section using all available existing resources, websites, and databases of Federal agencies, such as the Alternative Fuels Data Center, the Energy Efficient Mobility Systems program, and the Clean Cities Coalition Network.

(e) FUNDING.—The Secretaries shall carry out this section using existing funds made available to the Secretaries and not otherwise obligated, of which—

(1) 50 percent shall be from funds made available to the Secretary of Transportation; and

(2) 50 percent shall be from funds made available to the Secretary of Energy.

(f) TERMINATION.—The working group shall terminate on the date on which the third report under subsection (b) is submitted.

SA 1426. Mr. CASEY submitted an amendment intended to be proposed by him to the bill S. 2657, to support innovation in advanced geothermal research and development, and for other purposes; which was ordered to lie on the table; as follows:

In section 2212(a), strike paragraph (1) and insert the following:

(1) HYBRID MICRO-GRID SYSTEM.—The term ''hybrid micro-grid system'' means a micro-grid system that—

(A) comprises generation from both conventional and renewable energy resources; and

(B) may use grid-scale energy storage.

In section 2212(a), strike paragraph (3) and insert the following:

(3) MICRO-GRID SYSTEM.—The term ''micro-grid system'' means a localized grid that operates autonomously, regardless of whether the grid can operate in connection with another grid.

In section 2212, add at the end the following:

(e) MUNICIPAL MICRO-GRID SYSTEMS.—

(1) REPORT.—Not later than 270 days after the date of enactment of this Act, the Secretary shall submit to the Committee on Energy and Natural Resources of the Senate and the Committee on Energy and Commerce of the House of Representatives a report on the benefits of, and barriers to, implementing resilient micro-grid systems that are—

(A)(i) owned or operated by isolated communities or municipal governments; or

(ii) operated on behalf of municipal governments; and

(B) designed to maximize the use of—

(i) energy-generation facilities owned or operated by isolated communities; or

(ii) municipal energy-generation facilities.

(2) GRANTS TO OVERCOME BARRIERS.—The Secretary shall award grants of not more than $500,000 to not fewer than 10 municipal governments or isolated communities each year to assist those municipal governments and isolated communities in overcoming the barriers identified in the report under paragraph (1).

SA 1427. Mr. THUNE submitted an amendment intended to be proposed to amendment SA 1407 submitted by Ms. MURKOWSKI and intended to be proposed to the bill S. 2657, to support innovation in advanced geothermal research and development, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in subtitle H of title I, insert the following:

SEC. 180__. SENSE OF SENATE REGARDING FEDERAL POWER MARKETING ADMINISTRATIONS.

It is the sense of the Senate that—

(1) Federal electric transmission assets under the authority of the Southeastern Power Administration, the Southwestern Power Administration, the Western Area Power Administration, and the Bonneville Power Administration (referred to in this section as the ''Federal power marketing administrations'') should not be sold;

(2) the sale of Federal power marketing administration assets would result in utility rate increases for consumers;

(3) unobligated balances managed by the Federal power marketing administrations are a necessary financial resource that enable the Federal power marketing administrations to meet operation and maintenance needs and applicable purchase power and wheeling requirements;

(4) funds appropriated to the Federal power marketing administrations are repaid by customers of the Federal power marketing administrations; and

(5) the Congressional Budget Office should not score purchase power and wheeling activities carried out by the Federal power marketing administrations.

SA 1428. Mr. GRASSLEY (for himself and Mr. MARKEY) submitted an amendment intended to be proposed to amendment SA 1407 submitted by Ms. MURKOWSKI and intended to be proposed to the bill S. 2657, to support innovation in advanced geothermal research and development, and for other purposes; which was ordered to lie on the table; as follows:

At the end of part I of subtitle B of title II, add the following:

SEC. 220___. WHISTLEBLOWER PROTECTION FOR EMPLOYEES RESPONSIBLE FOR ENSURING THE RELIABILITY, RESILIENCE, AND SECURITY OF THE ELECTRIC GRID.

Section 215A of the Federal Power Act (16 U.S.C. 824o–1) is amended by adding at the end the following:

''(g) WHISTLEBLOWER PROTECTION.—

''(1) DEFINITIONS.—In this subsection:

''(A) ELECTRIC RELIABILITY ORGANIZATION; REGIONAL ENTITY; RELIABILITY STANDARD.—The terms 'Electric Reliability Organization', 'regional entity', and 'reliability standard' have the meanings given the terms in section 215(a).

''(B) ELECTRIC GRID.—The term 'electric grid' means—

''(i) all aspects of the generation, transmission, and distribution of electricity, whether interstate or intrastate; and

''(ii) the supply chain of equipment and software used in the generation, transmission, and distribution of electricity.

''(C) EMPLOYEE.—The term 'employee' means an individual who is an employee, former employee, contractor, subcontractor, grantee, or agent of an employer.

''(D) EMPLOYER.—

''(i) IN GENERAL.—The term 'employer' means an individual or entity in the public or private sector, including any Federal, State, or local government agency, that employs or retains the services of an individual who has access to—

''(I) critical electric infrastructure information or other information relating to critical electric infrastructure; or

''(II) other information relating to the reliability, resilience, or security of the electric grid.

''(ii) INCLUSIONS.—The term 'employer' includes an officer, employee, contractor, subcontractor, grantee, or agent of an individual or entity described in clause (i).

''(2) WHISTLEBLOWER PROTECTION FOR EMPLOYEES.—No employer may discharge, demote, suspend, threaten, blacklist, breach confidentiality, harass, or in any other manner discriminate against an employee with regard to the compensation, terms, conditions, or privileges of employment (including through an act in the ordinary course of the duties of the employee) because the employee or an individual associated with, or acting pursuant to a request of, the employee—

''(A) provided or caused to be provided information that the employee or individual associated with, or acting pursuant to the request of, the employee reasonably believed to evidence a violation of any provision of Federal or State law (including regulations) relating to fire safety or the protection or security of electric infrastructure (including critical electric infrastructure), critical electric infrastructure information, or other information relating to the reliability, resilience, or security of the electric grid, including a reliability standard, such as a Critical Infrastructure Protection standard, if that information is provided to—

''(i) the Commission;

''(ii) the Electric Reliability Organization;

''(iii) a regional entity;

''(iv) a Regional Transmission Organization;

''(v) an Independent System Operator;

''(vi) the Secretary;

''(vii) the Secretary of Homeland Security;

''(viii) the Attorney General;

''(ix) Congress;

''(x) a State regulatory authority or State inspector general;

''(xi) an individual with supervisory authority over the employee, including in communications that are part of the job duties of the employee; or

''(xii) any other individual working for the employer who the employee or associated or requested individual reasonably believes has the authority—

''(I) to investigate, discover, or terminate the misconduct; or

''(II) to take any other action to address the misconduct;

''(B) assisted in an investigation regarding the violation of any provision of Federal or State law described in subparagraph (A) if that assistance is provided to an individual or entity described in clauses (i) through (xii) of that subparagraph;

''(C) has filed or caused to be filed, or plans imminently (with the knowledge of the employer) to file or cause to be filed, a proceeding relating to any violation or alleged

violation of any provision of Federal or State law (including regulations) described in subparagraph (A); or

''(D) testified, participated, or otherwise assisted in an administrative or judicial action taken by the Commission, an Electric Reliability Organization, a regional entity, a State regulatory authority, or a State inspector general relating to an alleged violation of any provision of Federal or State law (including rules and regulations) relating to the protection, security, reliability, or resilience of electric infrastructure (including critical electric infrastructure), critical electric infrastructure information, or other information relating to the reliability, resilience, or security of the electric grid, including a reliability standard, such as a Critical Infrastructure Protection standard.

''(3) ENFORCEMENT ACTIONS.—

''(A) IN GENERAL.—An individual who alleges discharge or another violation of paragraph (2) by any person may seek relief by filing a complaint with the Secretary of Labor by not later than 180 days after the date on which the alleged violation occurs.

''(B) PROCEDURES.—An action under subparagraph (A) shall be governed under the rules and procedures described in section 42121(b) of title 49, United States Code, except that—

''(i) the notification required under paragraph (1) of that section shall be made to the person named in the complaint and to the employer; and

''(ii) with respect to the legal burdens of proof described in that section—

''(I) each reference to 'behavior described in paragraphs (1) through (4) of subsection (a)' contained in paragraph (2)(B) of that section shall be considered to be a reference to behavior described in subparagraphs (A) through (D) of paragraph (2) of this subsection; and

''(II) any reference to a 'violation of subsection (a)' contained in that section shall be considered to be a reference to a violation of paragraph (2) of this section.

''(C) ACTION BY SECRETARY.—

''(i) DEADLINE.—The Secretary of Labor shall act on a complaint filed under subparagraph (A) by the date that is 180 days after the date on which the complaint is filed.

''(ii) FAILURE TO ACT.—If the Secretary of Labor fails to act on a complaint filed by an individual who alleges discharge or another violation of paragraph (2), absent a sufficient demonstration that the failure to act is due to the bad faith of the individual, the individual who alleged the violation may file an action at law or equity for de novo review in a Federal district court of competent jurisdiction, in accordance with subparagraph (D).

''(D) ACTIONS FOR DE NOVO REVIEW.—

''(i) JURISDICTION.—The jurisdiction of a Federal district court over an action filed under subparagraph (C)(ii) shall be determined without regard to the amount in controversy.

''(ii) PROCEDURE.—

''(I) IN GENERAL.—An action under this subparagraph shall be governed under the rules and procedures described in section 42121(b) of title 49, United States Code, except that the notification required under paragraph (1) of that section shall be made to—

''(aa) the person named in the complaint; and

''(bb) the employer.

''(II) BURDENS OF PROOF.—An action under this subparagraph shall be governed by the legal burdens of proof described in section 42121(b) of title 49, United States Code, except that—

''(aa) each reference to 'behavior described in paragraphs (1) through (4) of subsection (a)' contained in paragraph (2)(B) of that section shall be considered to be a reference to behavior described in subparagraphs (A) through (D) of paragraph (2) of this subsection; and

''(bb) any reference to a 'violation of subsection (a)' contained in that section shall be considered to be a reference to a violation of paragraph (2) of this section.

''(iii) STATUTE OF LIMITATIONS.—An action under this subparagraph shall be commenced by not later than 180 days after the date on which—

''(I) the alleged violation occurs; or

''(II) the applicable employee became aware of the violation.

''(iv) JURY TRIAL.—A party to an action under this subparagraph shall be entitled to trial by jury.

''(4) NONENFORCEABILITY OF CERTAIN PROVISIONS WAIVING RIGHTS AND REMEDIES OR REQUIRING ARBITRATION OF DISPUTES.—

''(A) WAIVER OF RIGHTS AND REMEDIES.—The rights and remedies provided under this subsection may not be waived by any agreement, policy, form, or condition of employment, including by a predispute arbitration agreement.

''(B) PREDISPUTE ARBITRATION AGREEMENTS.—No predispute arbitration agreement shall be valid or enforceable if the agreement requires arbitration of a dispute arising under this subsection.''.

SA 1429. Mr. HEINRICH (for himself and Mr. GARDNER) submitted an amendment intended to be proposed to amendment SA 1407 submitted by Ms. MURKOWSKI and intended to be proposed to the bill S. 2657, to support innovation in advanced geothermal research and development, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE IV—AMENDMENTS TO THE INTERNAL REVENUE CODE OF 1986

SEC. 4001. ENERGY CREDIT FOR ENERGY STORAGE TECHNOLOGIES.

(a) IN GENERAL.—Subclause (II) of section 48(a)(2)(A)(i) of the Internal Revenue Code of 1986 is amended by striking ''paragraph (3)(A)(i)'' and inserting ''clause (i) or (viii) of paragraph (3)(A)''.

(b) ENERGY STORAGE TECHNOLOGIES.—Subparagraph (A) of section 48(a)(3) of the Internal Revenue Code of 1986 is amended by striking ''or'' at the end of clause (vi), by adding ''or'' at the end of clause (vii), and by adding at the end the following new clause:

''(viii) equipment which receives, stores, and delivers energy using batteries, compressed air, pumped hydropower, hydrogen storage (including hydrolysis), thermal energy storage, regenerative fuel cells, flywheels, capacitors, superconducting magnets, or other technologies identified by the Secretary in consultation with the Secretary of Energy, and which has a capacity of not less than 5 kilowatt hours,''.

(c) PHASEOUT OF CREDIT.—Paragraph (6) of section 48(a) of the Internal Revenue Code of 1986 is amended—

(1) by striking ''ENERGY'' in the heading and inserting ''AND ENERGY STORAGE''; and

(2) by striking ''paragraph (3)(A)(i)'' both places it appears and inserting ''clause (i) or (viii) of paragraph (3)(A)''.

(d) EFFECTIVE DATE.—The amendments made by this section shall apply to property placed in service after December 31, 2019.

SEC. 4002. RESIDENTIAL ENERGY EFFICIENT PROPERTY CREDIT FOR BATTERY STORAGE TECHNOLOGY.

(a) IN GENERAL.—Subsection (a) of section 25D of the Internal Revenue Code of 1986 is amended by striking ''and'' at the end of paragraph (4), by inserting ''and'' after the comma at the end of paragraph (5), and by adding at the end the following new paragraph:

''(6) the qualified battery storage technology expenditures,''.

(b) QUALIFIED BATTERY STORAGE TECHNOLOGY EXPENDITURE.—Subsection (d) of section 25D of the Internal Revenue Code of 1986 is amended by adding at the end the following new paragraph:

''(6) QUALIFIED BATTERY STORAGE TECHNOLOGY EXPENDITURE.—The term 'qualified battery storage technology expenditure' means an expenditure for battery storage technology which—

''(A) is installed on or in connection with a dwelling unit located in the United States and used as a residence by the taxpayer, and

''(B) has a capacity of not less than 3 kilowatt hours.''.

(c) EFFECTIVE DATE.—The amendments made by this section shall apply to expenditures paid or incurred in taxable years beginning after December 31, 2019.

SA 1430. Ms. CANTWELL submitted an amendment intended to be proposed to amendment SA 1407 submitted by Ms. MURKOWSKI and intended to be proposed to the bill S. 2657, to support innovation in advanced geothermal research and development, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle H of title I, add the following:

SEC. 18____. METHANE LEAK DETECTION AND MITIGATION.

(a) IN GENERAL.—Subtitle F of title IX of the Energy Policy Act of 2005 (42 U.S.C. 16291 et seq.) (as amended by section 1405(a)) is amended by adding at the end the following:

''SEC. 969B. METHANE LEAK DETECTION AND MITIGATION.

''(a) IN GENERAL.—The Secretary, in consultation with the Administrator of the Environmental Protection Agency and the heads of other appropriate Federal agencies, shall carry out a program of methane leak detection and mitigation research, development, demonstration, and commercial application for technologies and methods that significantly reduce methane emissions (referred to in this section as the 'program').

''(b) REQUIREMENTS.—In carrying out the program, the Secretary shall—

''(1) develop cooperative agreements with State or local governments or private entities to provide technical assistance—

''(A) to prevent or respond to methane leaks, including detection, mitigation, and identification of methane leaks throughout the natural gas infrastructure (including natural gas storage, pipelines, and natural gas production sites); and

''(B) to protect public health in the event of a major methane leak;

''(2) promote demonstration and adoption of effective methane emissions reduction technologies in the private sector;

''(3) in coordination with representatives from private industry, State and local governments, and institutions of higher education, create a publicly accessible resource for best practices in the design, construction, maintenance, performance, monitoring, and incident response for—

''(A) pipeline systems;

''(B) wells;

''(C) compressor stations;

''(D) storage facilities; and

''(E) other vulnerable infrastructure;

''(4) identify high-risk characteristics of pipelines, wells, and materials, geologic risk factors, or other key factors that increase the likelihood of methane leaks; and