Michael Mabee
(516) 808-0883
CivilDefenseBook@gmail.com
www.CivilDefenseBook.com

September 7, 2018

The Honorable Edward J. Markey
United States Senate
255 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Markey:

I am writing to you in response to your letters, dated August 13, 2018, to the Department of Homeland Security (DHS), the Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC) as well as several entities in the electric utility industry. In these letters, you express concern about recent press reports covering cyberattacks on the electric grid and you ask whether the government and the industry are taking the necessary steps to insure the security of our electric grid.

Unfortunately, the answer is no.

Despite all the "yes" answers you are no doubt receiving from the addressees of your letters, America remains extremely vulnerable to a number of threats to our electric grid and we are not taking the necessary steps to protect the national security of the United States in this regard.

My Background:

I am a private citizen with expertise on emergency preparedness, specifically on community preparedness for a long-term power outage. My career includes experience as an urban emergency medical technician and paramedic, a suburban police officer, and in the federal civil service. In the U.S. Army, I served in two wartime deployments to Iraq and two humanitarian missions to Guatemala. I retired from the U.S. Army Reserve in 2006 at the rank of Command Sergeant Major (CSM). I was decorated by both the U.S. Army and the federal government for my actions on 9/11/2001 at the World Trade Center in New York City. In sum, I have a great deal of experience – both overseas and in the U.S. – working in worlds where things went wrong.

I have studied the vulnerabilities of the U.S. electric grid to a variety of threats. My research lead me to write two books about how communities can prepare for and survive a long term power outage. I continue to write extensively on threats to the electric grid and emergency preparedness for blackout. I am affiliated with InfraGard EMP-SIG (Electromagnetic Pulse Special Interest Group)[1] and the Secure the Grid Coalition.[2] These two groups may be excellent resources for your staff

The United States Critical Infrastructures Are Under Attack

On March 15, 2018, The U.S. Department of Homeland Security, US-CERT released an alert entitled "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors."[3] At the same time, it was widely reported in the press that the Trump Administration accused Russia of hacking into the U.S. electric grid.[4]

Significantly, DHS reported that: "Since at least March 2016, government cyber actors—hereafter referred to as "threat actors"—targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors."

Further, DHS reported that: "This campaign comprises two distinct categories of victims: staging and intended targets. The initial victims are peripheral organizations such as trusted third-party suppliers with less secure networks, referred to as 'staging targets' throughout this alert. The threat actors used the staging targets' networks as pivot points and malware repositories when targeting their final intended victims. NCCIC and FBI judge the ultimate objective of the actors is to compromise organizational networks, also referred to as the 'intended target'."

This was hardly news. On July 6, 2017 Bloomberg reported: "Hackers working for a foreign government recently breached at least a dozen U.S. power plants, including the Wolf Creek nuclear facility in Kansas, according to current and former U.S. officials, sparking concerns the attackers were searching for vulnerabilities in the electrical grid."[5]

Also, On March 23, 2018, The U.S. Department of Justice reported that the Iranian Revolutionary Guard hacked numerous institutions including the Federal Energy Regulatory Commission (FERC).[6] This state-sponsored cyber incident was widely reported in the press.[7] According to the Washington Examiner article:

> Justice Department lawyers pointed out during a press conference that the Federal Energy Regulatory Commission "has the details of some of this country's most sensitive infrastructure," said U.S. Attorney Geoffrey Berman. "That is the agency that regulates the interstate transmission of electricity, natural gas and oil."

In a comment to Bloomberg, FERC Commissioner Neil Chatterjee noted on March 23, 2018 that: "cyberattacks have the potential to cause significant, widespread impacts on energy infrastructure. Sophisticated hacking tools are becoming more widely available, and cyber threats are constantly evolving, making such attacks more versatile."[8]

However, what we found in the rulemaking process at FERC in Docket No. RM17-13-000 (Supply Chain Risk Management Reliability Standards) was that the industry through its proxy, the North American Electric Reliability Corporation (NERC), is attempting to take a minimalistic approach to cybersecurity because to do more would be "burdensome" to NERC's constituents. Due to the tremendous pushback from the electric utility industry, FERC's final rule on cybersecurity in this docket was watered-down substantially from what was proposed in the original Notice of Proposed Rulemaking.[9]

The electric grid cannot be trusted to regulate itself on cybersecurity

As you know, the electric grid – which actually comprises thousands of separate public and private sector entities – is self-regulated through a mind numbingly complex relationship between the federal government (FERC), the industry's mouthpiece and purported non-profit regulator, the North American Electric Reliability Corporation (NERC), various regional entities which function as sub-regulators to NERC and, don't forget, public utilities commissions in all 50 states. The regulatory scheme is so complex and convoluted that it literally takes years to get a regulation finalized. For example, after the "Great Northeast Blackout of 2003" (which was caused in part by untrimmed foliage contacting the power lines), it took 10 years to get a tree trimming standard in place.

In the recent FERC cybersecurity rulemaking Docket No. RM17-13-000 (Supply Chain Risk Management Reliability Standards), despite years of active attacks on the bulk power system (and its federal regulator) by state sponsored actors, the North American Electric Reliability Corporation (NERC) argued that the proposed Reliability Standards should apply only to medium and high impact BES Cyber Systems – essentially making most systems "exempt" from the rules and leaving most of the discretion to apply the rules to the industry.

With apologies to Yogi Berra, "it's déjà vu all over again." As we saw from FERC Docket No. RM18-2-000 (Cyber Security Incident Reporting Reliability Standards), there is a "gap" between what the industry reports as a cybersecurity incident and what common sense would say is a cybersecurity incident. The evidence of the industry's inability to regulate itself through "best practices" continues to mount. For example, the following cybersecurity incident was not considered or reported as a as a cybersecurity incident.

On May 30, 2016 cybersecurity expert Chris Vickery reported a massive data breach by Pacific Gas and Electric (PG&E).[10] According to Mr. Vickery:

> "Among other things, it contained details for over 47,000 PG&E computers, virtual machines, servers, and other devices. All of it completely unprotected. No username or password required for viewing. We're talking about IP addresses, operating systems, hostnames, locations, MAC addresses, and more. This would be a treasure trove for any hostile nation-state hacking group. That's not to mention the 120 hashed employee passwords, or the plaintext NTLM, SOAP, and mail passwords."

This breach sounds exceedingly bad. North Korea, Iran or Russia having access to PG&E's systems is a national security concern. What would happen to neighboring parts of the bulk power system if PG&E was suddenly taken down by a cyberattack?

Then on February 28, 2018 NERC issued a "Notice of Penalty regarding Unidentified Registered Entity"[11] in which the NERC-anonymized entity apparently agreed to pay penalties of $2,700,000 for very serious cybersecurity violations. (FERC Docket No. NP18-7-000.) According to NERC, this data breech involved "30,000 asset records, including records associated with Critical Cyber Assets (CCAs). The records included information such as IP addresses and server host names."

According to NERC

> "These violations posed a serious or substantial risk to the reliability of the bulk power system (BPS). The CCAs associated with the data exposure include servers that store user data, systems that control access within URE's control centers and substations, and a supervisory control and data acquisition (SCADA) system that stores critical CCA Information. The data was exposed publicly on the Internet for 70 days. The usernames of the database were also exposed, which included cryptographic information of those usernames and passwords.
>
> Exposure of the username and cryptographic information could aid a malicious attacker in using this information to decode the passwords. This exposed information increases the risk of a malicious attacker gaining both physical and remote access to URE's systems. A malicious attacker could use this information to breach the secure infrastructure and access the internal CCAs by jumping from host to host within the network. Once in the network, the attacker could attempt to login to CCAs, aided by the possession of username and password information."

Notwithstanding NERC's lack of transparency in hiding the identity of the "Unidentified Registered Entity," such a cover-up is against the public interest and should not have been allowed by FERC. But FERC allowed the cover-up to stand and closed the docket without reviewing the case. The PG&E data breach in 2016 and NERC's cover-up of the identity of the "Unidentified Registered Entity" — who by NERC's own admission was involved in a dangerous data breach[12] — is ample proof that a watchful regulator is necessary to protect the bulk power system. And FERC is presently failing in that role.

Disturbingly, there were no "cybersecurity incidents" reported by the industry in 2016.[13]

To identify the "Unidentified Registered Entity," I was forced to file a Freedom of Information Act (FOIA) request with FERC, which was denied and I was forced to appeal. As a result, we finally got confirmation that PG&E was the "Unidentified Registered Entity" and the Wall Street Journal was able to finally report this to the public on August 24, 2018[14] – over 2 years after the cyberbreach took place! It should not have taken a citizen filing a FOIA request to expose a company which was subjected to a regulatory action by the U.S. Government. This secrecy (with no national security purpose – in this case the breach was long over) is contrary to efficient regulation and the public's right to information.

Moreover, not only is the industry (and FERC) actively covering up these violators who endanger the public, but they are covering up the fact that "cybersecurity incidents" are even taking place by defining them in such a way that the cyberattacks being reported by the press do not qualify.

<u>Millions of Americans placed at risk so the industry can avoid "administrative burden"</u>

NERC argued in its filings to FERC's cybersecurity docket that it would be "overly burdensome" to require protections to low impact BES Cyber Systems.[15] NERC was egged on by the industry through largely template comments, for example:

- "CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets."[16]
- "PRPA believes this requirement will place substantial additional administrative burden on entities with low impact assets."[17]
- "SRP believes this requirement will place substantial additional administrative burden on entities with low impact assets."[18]

- "OUC believes this requirement will place substantial additional administrative burden on entities with low impact assets."[19]
- "Santee Cooper believes this requirement will place substantial additional administrative burden on entities with low impact assets."[20]
- "LCRA believes this requirement will place substantial additional administrative burden on entities with low impact assets."[21]
- "XXX believes this requirement will place substantial additional administrative burden on entities with low impact assets."[22] (Note: Apparently, Austin Energy did not carefully proofread the industry's template response before submitting it.)

In fact, there were 172 instances of the word "burden" in industry comments on FERC Docket RM17-13-000. The industry may believe that cybersecurity is a burden, but it is FERC's job to protect the public by protecting the nation's critical infrastructure – and FERC failed to do so by allowing a watered-down cybersecurity rule.

Other Threats to the Bulk Power System and Critical Infrastructure:

On March 28, 2017[23] the Senate Committee on Homeland Security and Governmental Affairs reported this about the critical infrastructure:

> *"The United States depends on its critical infrastructure, particularly the electric power grid, as all critical infrastructure sectors are to some degree dependent on electricity to operate. A successful nuclear electromagnetic pulse (EMP) attack against the United States could cause the death of approximately 90 percent of the American population. Similarly, a geomagnetic disturbance (GMD) could have equally devastating effects on the power grid."* (Page 6.)

And the previous year, the House held a hearing entitled: "Blackout! Are We Prepared to Manage the Aftermath of a Cyberattack or Other Failure Of The Electrical Grid?"[24] In this hearing, the Committee noted that:

> *"The DHS reports that the energy sector is the target of more than 40 percent of all reported cyberattacks. In 2014, the National Security Agency (NSA) reported that the agency had tracked intrusions into industrial control systems by entities with the technical capability 'to take down control systems that operate U.S. power grids, water systems and other critical infrastructure'."* (Page vii. Internal citations omitted.)

On February 12, 2013, President Obama[25] noted:

> "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats."

In 2008, the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack reported about the bulk power system:

> *"Electrical power is necessary to support other critical infrastructures, including supply and distribution of water, food, fuel, communications, transport, financial transactions, emergency services, government services, and all other infrastructures supporting the national economy and welfare. Should significant parts of the electrical power infrastructure be lost for any substantial period of time, the Commission believes that the consequences are likely to be catastrophic, and many people may ultimately die for lack of the basic elements necessary to sustain life in dense urban and suburban communities."* (Page vii.)[26]

In fact, there have been over two decades of congressional hearings, federal reports and studies about the various threats to the U.S. electric grid.[27] Of the numerous hearings on threats to the critical infrastructures, below are a select few in which Congress examined the cyber threats to the grid:

- "Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection." Hearing 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 2003). https://www.gpo.gov/fdsys/pkg/CHRG-108hhrg99793/pdf/CHRG-108hhrg99793.pdf (accessed February 22, 2018).
- "Cyber Security: US Vulnerability and Preparedness." Hearing before the US House, Committee on Science, 109th Congress (September 15, 2005). https://www.gpo.gov/fdsys/pkg/CHRG-109hhrg23332/pdf/CHRG-109hhrg23332.pdf (accessed February 22, 2018).
- "The Cyber Threat to Control Systems: Stronger Regulations Are Necessary To Secure the Electric Grid." Hearing before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. (110th Congress) October 17, 2007. https://www.gpo.gov/fdsys/pkg/CHRG-110hhrg48973/pdf/CHRG-110hhrg48973.pdf (accessed February 22, 2018).
- "Implications of Cyber Vulnerabilities on the Resilience and Security of the Electric Grid." Hearing 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 February 22, 2018).
- "Securing the Modern Electric Grid from Physical and Cyber Attacks." Hearing before the US House, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the Committee on Homeland Security, 111th Congress (July 21, 2009). https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg53425/pdf/CHRG-111hhrg53425.pdf (accessed February 22, 2018).
- "Cyber Security." Hearing before the US Senate, Committee on Energy and Natural Resources, (112th Congress) May 5, 2011. https://www.gpo.gov/fdsys/pkg/CHRG-112shrg67362/pdf/CHRG-112shrg67362.pdf (accessed February 22, 2018).
- "The EMP Threat: Examining the Consequences." Hearing before the Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. Serial No. 112-115. (112th Congress) September 12, 2012. https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg80856/pdf/CHRG-112hhrg80856.pdf (accessed February 22, 2018).
- "Cyber Threats and Security Solutions." Hearing before the US House Committee on Energy and Commerce. (113th Congress) May 21, 2013. https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg82197/pdf/CHRG-113hhrg82197.pdf (accessed February 22, 2018).

- "Blackout! Are We Prepared to Manage the Aftermath of a Cyberattack or Other Failure Of The Electrical Grid?" Hearing before the House Subcommittee on Economic Development, Public Buildings, and Emergency Management. (114th Congress) April 14, 2016. https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg99931/pdf/CHRG-114hhrg99931.pdf (accessed February 22, 2018).

There is no debate that a loss of the electric grid for a long period of time, for any reason, would be catastrophic for the United States. Because we cannot support our present human population without the electric grid, the loss of life would be unimaginable. Here are the undisputed facts:

1. Fact: We know that cyber threats to the U.S. electric grid exist and are increasing.[28]

2. Fact: We know that the electric grid in the Ukraine was attacked and taken down twice by cyberattacks.[29]

3. Fact: We know that cyber-attacks have been known to destroy equipment.[30]

4. Fact: We know that all U.S. critical infrastructures are dependent on the bulk power system.[31]

In addition to the well-documented cyber threat, there is virtually nothing being done to harden the grid from other threats, such as electromagnetic pulse (EMP), geomagnetic disturbance, (GMD), physical attack, pandemic, etc.

Therefore, the threats to the electric grid represent an existential threat to the United States. The federal government is responsible for protecting against threats to national security. It is critical that the federal government insure that the critical infrastructures are adequately protected against known threats. The security of the U.S. electric grid is not a matter of convenience; it is a matter of paramount importance for the federal government.

Conclusion:

Thomas Jefferson famously said: "The first duty of government is the protection of life, not its destruction. Abandon that, and you have abandoned all."

We need immediate federal government action to protect the electric grid from a variety of threats. The present regulatory scheme is not working. We cannot wait years for this inadequate and inefficient regulatory scheme to (possibly) do something while we remain vulnerable.

We need executive and legislative action now.

Respectfully submitted by:

Michael Mabee

[1] InfraGard EMP-SIG (Electromagnetic Pulse Special Interest Group): https://www.empcenter.org/about/ (accessed September 7, 2018).
[2] Secure the Grid Coalition: https://securethegrid.com/about-us/ (accessed September 7, 2018).
[3] US-CERT Alert (TA18-074A) https://www.us-cert.gov/ncas/alerts/TA18-074A (accessed March 15, 2018).
[4] See for example, Gizmodo: "FBI and DHS Warn That Russia Has Been Poking at Our Energy Grid." https://apple.news/AHv5RwYqbSf-EI-yIa355Jw (accessed March 15, 2018); Washington Free Beacon: "Russia Implicated in Ongoing Hack on U.S. Grid." https://apple.news/AGs6ieh6wSP-1tQkUFttREA (accessed March 15, 2018); Slate: "What Does It Mean to Hack an Electrical Grid?" https://apple.news/Au5gy7bTlTDSovpvzg5j79w (accessed March 15, 2018); BuzzFeed News: "The Trump Administration Is Accusing Russia Of Trying To Hack The US Power Grid." https://apple.news/AP5elUw2CQWmAZXgQBXLFKA (accessed March 15, 2018).
[5] Bloomberg. "Russians Are Suspects in Nuclear Site Hackings, Sources Say." July 6, 2017. https://www.bloomberg.com/news/articles/2017-07-07/russians-are-said-to-be-suspects-in-hacks-involving-nuclear-site (accessed March 17, 2018).
[6] U.S. Department of Justice. "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps." March 23, 2018. https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary (accessed March 23, 2018).
[7] Washington Examiner: "Iranian hackers targeted power grid watchdog, Justice Department says." March 23, 2018. https://www.washingtonexaminer.com/policy/energy/iranian-hackers-targeted-power-grid-watchdog-justice-department-says (accessed March 23, 2018).
[8] Bloomberg. "Threat from Cyber Hackers is Growing, U.S. Grid Regulator Says" https://www.bloomberg.com/news/articles/2018-03-23/threat-from-cyber-hackers-is-growing-u-s-grid-regulator-says (accessed March 24, 2018).
[9] Foundation for Resilient Societies. "Petition for Rulemaking to Require an Enhanced Reliability Standard to Detect, Report, Mitigate, and Remove Malware from the Bulk Power System." Filed January 13, 2017. https://www.resilientsocieties.org/uploads/5/4/0/0/54008795/resilient_societies_petition_for_rulemaking_ad17-9.pdf (accessed February 22, 2018).
[10] Vickery, Chris. "Pacific Gas and Electric Database Exposed." https://mackeeper.com/blog/post/231-pacific-gas-and-electric-database-exposed (accessed March 23, 2018).
[11] NERC "Full Notice of Penalty regarding Unidentified Registered Entity FERC Docket No. NP18-_-000." February 28, 2018. http://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_CIP_NOC-2569%20Full%20NOP.pdf (accessed march 23, 2018).
[12] FERC Docket No. NP18-7-000.
[13] FERC Order Number 848. *Cyber Security Incident Reporting Reliability Standards – Final Rule*. https://www.ferc.gov/whats-new/comm-meet/2018/071918/E-1.pdf Page 14. (Accessed September 7, 2018).
[14] Smith, Rebecca. Wall Street Journal. *PG&E Identified as Utility That Lost Control of Confidential Information. As a result of 2016 failure, 30,000 records about PG&E's cyber assets were exposed on the internet.* August 24, 2018. https://www.wsj.com/articles/pg-e-identified-as-utility-that-lost-control-of-confidential-information-1535145850 (accessed September 7, 2018).
[15] Petition Of The North American Electric Reliability Corporation for Approval of Proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 Addressing Supply Chain Cybersecurity Risk Management. September 26, 2017. Page 17.
[16] *Id.* At pg. 499.
[17] *Id.* At pg. 500.
[18] *Id.* At pg. 507.
[19] *Id.* At pg. 531.
[20] *Id.* At pg. 538.
[21] *Id.* At pg. 539.
[22] *Id.* At pg. 501.

[23] Senate Report 115-12. Activities of the Committee on Homeland Security and Governmental Affairs. (115th Congress) March 28, 2017. https://www.gpo.gov/fdsys/pkg/CRPT-115srpt12/pdf/CRPT-115srpt12.pdf (accessed February 22, 2018).
[24] House Hearing before the Subcommittee on Economic Development, Public Buildings, and Emergency Management. *"Blackout! Are We Prepared to Manage the Aftermath of a Cyberattack or Other Failure Of The Electrical Grid?"* (114th Congress) April 14, 2016. https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg99931/pdf/CHRG-114hhrg99931.pdf (accessed February 22, 2018).
[25] Executive Order 13636 *Improving Critical Infrastructure Cybersecurity.* February 12, 2013. https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (accessed February 23, 2018).
[26] Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *"Critical National Infrastructures."* 2008. https://permanent.access.gpo.gov/LPS101707/A2473-EMP_Commission-7MB.pdf (accessed February 23, 2018).
[27] See a comprehensive listing of these federal documents here: https://michaelmabee.info/government-documents-emp-and-grid-security/ (accessed February 22, 2018).
[28] RTO Insider. *Expert Sees 'Extreme Uptick' in Cyber Attacks on Utilities*. https://www.rtoinsider.com/naruc-dragos-cybersecurity-scada-86882/ (accessed February 22, 2018).
[29] Wired magazine. *'Crash Override': The Malware That Took Down a Power Grid.* https://www.wired.com/story/crash-override-malware/ (accessed February 22, 2018).
[30] Wired Magazine. *An Unprecedented Look at Stuxnet, The World's First Digital Weapon*. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (accessed February 22, 2018).
[31] Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *"Critical National Infrastructures."* 2008. https://permanent.access.gpo.gov/LPS101707/A2473-EMP_Commission-7MB.pdf (accessed February 23, 2018). Page vii.