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

February 23, 2018

Chairman Kevin J. McIntyre
Commissioner Neil Chatterjee
Commissioner Cheryl A. LaFleur
Commissioner Robert F. Powelson
Commissioner Richard Glick
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Comments submitted in FERC Docket RM18–2–000
Cyber Security Incident Reporting Reliability Standards

Dear Chairman McIntyre, Commissioner Chatterjee, Commissioner LaFleur, and Commissioner Powelson, and Commissioner Glick:

Background:

I am a private citizen who has taken it upon himself to study the vulnerabilities of the U.S. electric grid to a variety of threats. My research lead me to write a book about how communities can prepare for and survive a long term power outage.[1] It is a book that never should have had to be written. I'm a regular working American with a regular day-job, but in my spare time I work with several non-profit groups to raise awareness of the existential threats the United States faces vis-à-vis the threats to the electric grid. I continue to write extensively on the subject. It is an occupation I never should have had to have.

On January 13, 2017, the Foundation for Resilient Societies filed a petition for rulemaking[2] with FERC because the electric grid does not have sufficient cybersecurity protection. Not surprisingly, the electric industry objects and seems to try to assure us that everything is fine.

Threats to the Bulk Power System and Critical Infrastructure:

On March 28, 2017[3] 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?"[4] 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[5] 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.)[6]

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.[7] 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.[8]

2. Fact: We know that the electric grid in the Ukraine was attacked and taken down twice by cyberattacks.[9]

3. Fact: We know that cyber-attacks have been known to destroy equipment.[10]

4. Fact: We know that all U.S. critical infrastructures are dependent on the bulk power system.[11]

Therefore, the cyber threat to the bulk power system represents an existential threat to the United States. The federal government – not the electric industry – is responsible for protecting against threats

to national security. Therefore, the electric industry's objections to more stringent regulations are unpersuasive. The bulk power system must, without fail, be protected.

It is critical that the federal government insure that the critical infrastructures are adequately protected against known threats. In this case, the cyber security of the U.S. bulk power system is not a matter of convenience; it is a matter of paramount importance for the federal government.

Conclusion:

I urge you to require NERC to promulgate strict cybersecurity standards and reporting requirements. Thomas Jefferson famously said: "The first duty of government is the protection of life, not its destruction. Abandon that, and you have abandoned all."

FERC's duty here is clear. You must protect life. The threats to the electric grid constitute a national security issue. This is not a matter of a benevolent government being friendly to businesses. This is a matter of national security and the very real threat to millions of Americans' lives.

Respectfully submitted by:

Michael Mabee

---

[1] Mabee, Michael. *The Civil Defense Book: Emergency Preparedness for a Rural or Suburban Community*. ISBN-13: 978-1974320943, first edition published July 4, 2013, second edition published October 17, 2017.

[2] 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).

[3] 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).

[4] 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).

[5] 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).

[6] 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).

[7] See a comprehensive listing of these federal documents here: https://michaelmabee.info/government-documents-emp-and-grid-security/ (accessed February 22, 2018).

[8] RTO Insider. *Expert Sees 'Extreme Uptick' in Cyber Attacks on Utilities*. https://www.rtoinsider.com/naruc-dragos-cybersecurity-scada-86882/ (accessed February 22, 2018).

[9] Wired magazine. *'Crash Override': The Malware That Took Down a Power Grid.* https://www.wired.com/story/crash-override-malware/ (accessed February 22, 2018).

[10] 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).
[11] 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.

Document Content(s)