Michael Mabee

Fort Worth, TX 76135
Phone: (516) 808-0883
Email: CivilDefenseBook@gmail.com
Web: https://michaelmabee.info/

October 28, 2021

Chris Inglis
Office of the National Cyber Director
The White House
1600 Pennsylvania Ave NW
Washington, DC 20500

Dear Mr. Inglis,

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. 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.

I am attaching comments I submitted today to the Secretary of Energy Advisory Board which outline what the Administration and the Department of Energy must do to protect the electric grid from the existential cyber threats we face.

"Trickle down grid security" has not worked and we do not have years to secure the grid. We have known about the threats to the electric grid for decades (the cyber threat being chief among them) and the only way we are going to fix this problem is by immediately making the protection of our critical electric infrastructure mandatory. Otherwise, our adversaries may decide at any time of their choosing to fix the problem for us – by shutting off our electric grid.

I hope you will take a moment and consider my comments and proposed solution. I am available to you and your staff to assist in any way I can.

Respectfully,

Michael Mabee

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

Comments of Michael Mabee to the Secretary of Energy Advisory Board, October 28, 2021

I commend the Department of Energy for holding this meeting and I commend the members of the Secretary of Energy Advisory Board for your service to this country.

On June 6, 2021 Secretary of Energy Jennifer Granholm confirmed in a CNN interview that U.S. adversaries have the capability to shut down our power grid.[1]

The U.S. government has been concerned about the cybersecurity of the critical electric infrastructure since at least 2003;[2] the security of the electric grid from physical threats since at least 1981;[3] geomagnetic disturbance (GMD) threats since at least 1990;[4] and electromagnetic pulse (EMP) threats since at least 1972.[5] Moreover, we continue to see the impacts of extreme weather on our critical electric infrastructure every year.[6] 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.

It is unacceptable that after decades of federal reports, studies and congressional hearings on these threats,[7] in 2021 we find that our lights are on at the discretion of our adversaries and mother nature. Tomorrow, somebody may decide to turn them off.

If 9/11 taught us anything, it is that we are not safe from an attack in the United States. The 9/11 Commission famously said: "the most important failure was one of imagination."[8]

We cannot repeat this failure of imagination with our Achilles' heel: the electric grid.

Imagine what a long-term blackout would do to the U.S. Everything we need to support our human population would stop. Food, water, fuel, communications, transportation, the medical system just to name a few of the 16 critical infrastructures – all of which are dependent on the electric grid. Any threat to the electric grid is an existential threat to the United States.

The security of the electric grid against known threats is a true national emergency. The threats are here. They are real and we are out of time.

After decades of self-regulation and pleading for voluntary actions, the U.S. is still vulnerable to all of these threats and now is imminently threatened by both adversaries and nature. To protect our national security from these imminent threats, the U.S. must immediately make protection of the critical electric infrastructure against these known threats *mandatory*.

What the Department of Energy and the Administration must do immediately:

1. Through a Presidential Executive Order and a Department of Energy Emergency Order,[9] protection of the entire electric grid against known threats must be made *mandatory*.

What Congress must do at the Administration's urging:

1. Congress must enact legislation mandating that reasonably prudent actions on cybersecurity, physical security, EMP/GMD protective measures and hardening for severe weather events be taken by all entities, public or private sector, that are part of the critical electric infrastructure. These measures must be certified periodically by the Chief Executive Officer of each such critical electric infrastructure entity.[10]
    a. The Chief Executive Officer of each such critical electric infrastructure entity must be required to certify periodically to the Department of Energy (DOE) and the Department of Homeland Security (DHS) that they have reasonably prudent cybersecurity measures in place that have been reviewed and approved by the Chief Executive Officer of the entity.[11]
    b. The Chief Executive Officer of each such critical electric infrastructure entity must be required to certify periodically to DOE and DHS that they have reasonably prudent physical security measures in place that have been reviewed and approved by the Chief Executive Officer of the entity.
    c. The Chief Executive Officer of each such critical electric infrastructure entity must be required to certify periodically to DOE and DHS that they have reasonably prudent EMP/GMD measures in place that have been reviewed and approved by the Chief Executive Officer of the entity.
    d. The Chief Executive Officer of each such critical electric infrastructure company must be required to certify periodically to DOE and DHS that they have reasonably prudent extreme weather hardening measures in place that have been reviewed and approved by the Chief Executive Officer of the entity.
2. There must be civil and criminal penalties for false certification or failure to submit such certifications.
3. These certifications should be made available to the public as well as state and federal authorities.

Respectfully,

Michael Mabee
Fort Worth, Texas

References from my grid security research:

"How the electric utility industry torpedoed grid security."
https://michaelmabee.info/how-the-electric-utility-industry-torpedoed-grid-security/

"Chinese Transformer Complaint Filed with U.S. Government."
https://michaelmabee.info/chinese-transformer-complaint-filed-with-u-s-government/

"Critical Electric Infrastructure – The Government Must Step Up."
https://michaelmabee.info/critical-electric-infrastructure-the-government-must-step-up/

"Federal Complaint Filed on Texas Grid Collapse."
https://michaelmabee.info/federal-complaint-filed-on-texas-grid-collapse/

"Supply Chain Cybersecurity Complaint Filed with FERC."
https://michaelmabee.info/supply-chain-cybersecurity/

"Loopholes in Grid Physical Security Identified."
https://michaelmabee.info/loopholes-in-grid-physical-security-identified/

"Complaint Filed About Inadequate Electric Grid Physical Security."
https://michaelmabee.info/complaint-filed-electric-grid-physical-security/

"The Role of Transparency in Preventing Regulatory Failures."
https://michaelmabee.info/transparency-regulatory-failures/

"Q: How Did We Became So Vulnerable?"
https://michaelmabee.info/how-did-we-became-so-vulnerable/

End Notes:

[1] CNN. "Energy secretary says adversaries have capability of shutting down US power grid." June 6, 2021. https://www.cnn.com/2021/06/06/politics/us-power-grid-jennifer-granholm-cnntv/index.html

[2] 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

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

[4] See: U.S. Congress, Office of Technology Assessment, "Physical Vulnerability of Electric System to Natural Disasters and Sabotage." OTA-E-453. June 1990. https://bit.ly/2VVHwar (page 13-14), and Department of Energy (DOE). Oak Ridge National Laboratory (ORNL). "Electric Utility Experience Industry with Geomagnetic Disturbances." (GMD) September 1991. http://bit.ly/2CRNE6Q.

[5] See: Defense Civil Preparedness Agency (DCPA). Oak Ridge National Laboratory (ORNL). ORNL-4836. Effects of Electromagnetic Pulse (EMP) on a Power System. December 1972. http://bit.ly/39QXtRP. Also 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.

[6] For example, the Texas grid collapse of 2021 was not a freak occurrence. The same thing happened to the Texas grid in 2011 and 1989 for the same reasons. See: https://michaelmabee.info/federal-complaint-filed-on-texas-grid-collapse/

[7] See: Library of Government Documents on Grid Security at: https://michaelmabee.info/government-documents-emp-and-grid-security/

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

[9] See: "Critical Electric Infrastructure Security" at 16 U.S.C. 824o-1.

[10] 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.

[11] A federal minimum is needed: The National Institute of Science and Technology (NIST) cybersecurity framework can provide this federal minimum. https://www.nist.gov/cyberframework