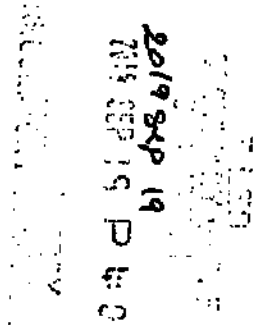
ORIGINAL

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards	)))	**Docket No. AD19-18-000**



Comments on Transparency

Submitted to FERC on September 12, 2019

Preston L. Schleinkofer, a private citizen, respectfully submits comments on FERC Docket No. AD19-18-000, Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards.

My background is as a retired 27 year veteran federal law enforcement officer, and retired 22 year veteran Army National Guard Sergeant First Class. I am also an Officer in Civil Defense Virginia, a 501(c)(3) nonprofit education and training organization. We promote a new American Civil Defense Structure because we have seen, and our extensive research has confirmed, that government has failed the public in too many instances during natural and man-made disasters. I am also a volunteer Officer with the EMP Task Force on National and Homeland Security and a member of the Secure the Grid Coalition. Civil Defense Virginia, the Task Force and the Secure the Grid Coalition are all working daily to inform Americans, politicians, government employees and industry insiders of the huge threats to our national electrical supply system from both natural and man-caused threats from a variety of vectors.

Ever since I began to really dig into the many threats to our national grid in early 2015, I have been flummoxed at the seemingly lackadaisical attitudes of those in congress, government agencies (FERC and DOE), and the power industry, especially their self-regulating agency NERC. My personal research has confirmed that there is a huge and existential threat to our way of life through our national grid system. Ted Koppel identified many threats, more specifically those from cyber attacks, in his 2015 book "*Lights Out*." But, still to this day there hasn't been anyone with authority to make the desperately needed changes and institute requirements that will safeguard our grid and protect the people who make up this wonderful country.

> ***Lights Out***, Page 112: *"In successive State of the Union addresses President Obama has warned of the danger of cyberattacks on our infrastructure. Government is adapting to the "new normal" of daily hacking, and cyber specialists such as Richard Clarke and George Cotter, who held senior government posts, have explained that the Russians and the Chinese are almost certainly inside of the grid, mapping its vulnerabilities. Keith Alexander and Howard Schmidt warn that independent actors will soon have the capability to damage the grid, if they don't have it already."*

Since the above quote was written in *Lights Out* in 2015, the world has seen a huge increase in threats to power grids around the world. There may still be, as the quote above shows, Russian and Chinese bots in our national grid system continuing their mapping of our vulnerabilities. But, is there a requirement for these bots and other malware to be removed? The answer I have found is NO, there is not a requirement. If so, I haven't found it. How about potential foreign threats participating in our electrical power industry trade associations and NERC itself? We know that there are at least three Chinese power companies who have membership in Edison Electric Institute (EEI). How many others besides EEI are corrupted by foreign influence to maintain our vulnerability to outside attacks? How much influence do they have on decisions, policies and reporting from the industry? Would it be wise to continue to accept Chinese companies, who are required by Chinese Counterintelligence law to participate with Chinese Intelligence? With this fact, does it lend more or less credibility to NERC and the self-regulated environment they wish to maintain? Personally, I tend to trust them less given these gross examples of blatant lack of situational awareness with respect to threats to our national grid and our country.

After reading the "White Paper" proposed by the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC), I found it very curious there is so much worry about Critical Energy/Electric Infrastructure Information (CEII) being released to the public and the possibility of certain nefarious actors using this

information to plan attacks and further compromise our grid. The problem with this is the system had already failed to properly conduct a procedure or received a cyber attack, which caused the CIP violation in the first place. FERC won't even receive a CIP NOS for a minimum of 30 days, so isn't this enough time to mitigate the damage that further attacks would supposedly take advantage of? It is obvious the industry works very hard to prevent close scrutiny of industry operations, violations. This doesn't seem to promote transparency or openness to scrutiny from federal and state regulators, investors and the public at large.

I understand completely the need for security of our national electrical grid. In fact, this is the main reason I have gotten involved in trying to bring back a new Civil Defense structure and my participation in both the EMP Task Force on National and Homeland Security, and the Secure the Grid Coalition. With that said, I refuse to give a pass where one is not deserved.

Let's look at this objectively. Since 2010, there have been 255 reported infractions and a total of $35 million in fines. This is minuscule, and represents roughly $7.2 million per violation over nine years. A drop in the bucket compared to the amount of money spent on lobbying our federal and state representatives. In just 2018 alone, FERC spent $147+ million lobbying against stricter standards. Something doesn't add up with this. I could speculate, but will hold it for now, but I am calling for stricter standards and more openness in CIP reporting. The public and investors need to know this information proactively, not whenever the industry decides to let us know, and only what little bit they decide to tell us.

Light brings exposure to a problem and darkness hides actions that should be known by the government, the people, and investors in the companies that provide electrical power to our nation. Currently, there is not enough light and an audit should be conducted by an independent auditing company to reveal the true threats from these 255 CIP violations and the amount of exposure we have voluntarily allowed to foreign entities that may have compromised our entire grid.

This LIGHT on the subject is where we are now. So let's spread some light and see what areas need to be revamped and which are operating the way they should.

It seems from an external view of the relationship NERC has with its membership, that they would tend to be less willing to expose members to scrutiny than would someone with a limited relationship. The "cover" of protecting sensitive information in the CIP NOP, the cover letter and other reporting documents is just not reasonable. Why would the identity and type of infraction and more details about this be sensitive and need to remain hidden from the public and investors? It is cover, nothing more. What information would be given to a nefarious actor from violations in 2012, 2014, or 2015 that would be usable today? Nothing, unless that discrepancy wasn't truly corrected and was still a current vulnerability. If there was a violation, it should be corrected quickly and completely, without any question of being vulnerable to a subsequent attack. In fact, our electrical supply system should be the most robust element of all of our critical infrastructure, as it is the most important of all. If the industry would use the highest protective measures, EMP proof, then we wouldn't have so much to worry about.

I agree with Command Sergeant Major Michael Mabee's well written Alternative Proposal. I support his suggestions pertaining to the full release of information. As an example, his reasons for full disclosure of the information fields from the NOP Spreadsheet has a lot of validity to support why this information should be exposed and included in all reporting for public release. Information should not be held just for the sake of keeping it hidden from the public. Law enforcement and the intelligence community has learned this lesson, now it is the power industry's turn to make changes towards more transparency. This information has a bearing on all of us, and we have a right to know who is doing what and what is being done about it. All areas should be revealed, especially from past violations. I do not believe these suggestions will in any way compromise the industry or its security.

Respectfully submitted by:

Preston Le Roy Schleinkofer

Document Content(s)