

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

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

Comments on Transparency

Submitted to FERC on October 27, 2019

Frank Heindel, 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 private citizen and also as a citizen activist that has pushed for government transparency in South Carolina for over 20 years. I have sent in over 100 FOIA requests during this time to local and state agencies. My experience tells me that our South Carolina state agencies, like Santee Cooper, are not qualified to prevent sophisticated cyber intrusions. I was involved with auditing our state's electronic paperless voting system and have seen state and local agencies redact and refuse to release any type of cybersecurity reports that detail lax security processes and problems the public should be aware of.

In 2012, the South Carolina Department of Revenue had a huge data breach in which my personal information, along with 3.8 million other citizens, was hacked. Although state officials promised to find and punish the hackers, unsurprisingly, the criminals were never found.

I discovered through FOIA that Santee Cooper lied to the public about the rationale for a rate increase as detailed in a September 2, 2012 article in the Charleston Post & Courier entitled "Are you paying too much for power?" If our state agency is not going to be truthful about the rationale for raising rates, why should I expect them to be honest and upfront when they are being attacked from sophisticated nation state hackers?

I have suffered high utility bills due to the unscrupulous and most likely fraudulent actions of Santee Cooper and SCE&G executives since they held back from the public damaging information resulting in a staggering \$9 billion dollars of losses due to their failed nuclear power plans. My point is our state's utilities have not been honest, upfront, and transparent with the South Carolina public about sharing bad news. Therefore, it is crucial for prudent federal oversight to take place that immediately informs and protects citizens from overseas threats. Simply paying a secretive fine to a federal agency will not fix the problem.

I am familiar with the "White Paper" proposed by the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC). It is a very modest small step in the right direction. However, the public will still be in the dark as to what is really happening "behind the curtain". Electric utility executives are focused on personal financial incentives that revolve around profits and have no reason to be more open with the public about cybersecurity breaches – unless the federal government steps in and brings it to the forefront by allowing the public to understand exactly what the foreign attackers are attempting. The public can handle the full truth, regardless of what utility executives might say. And the public deserves the full unvarnished truth without having to wonder if some pertinent information has not been disclosed for the sole reason that it would cast negative light on a particular entity.

A state agency like Santee Cooper is ill equipped to deal with sophisticated nation state hackers. However, if they knew the public would be notified of every security breach and could gauge how Santee Cooper was performing compared to other public utilities across the nation, then their security operations would improve as a result of public scrutiny.

Any citizen knows the system is not transparent and not operating in our best interest when a term like "Unidentified Registered Entity" is being used for a violator that was fined \$2.7 million dollars. It is obvious to me utility executives have far too much power in this process. Shouldn't we all assume the bad actors are well aware of this "Unidentified Registered Entity"?

I agree with retired U.S. Army Command Sergeant Major Michael Mabee as well as the "Alternate Proposal" he submitted to FERC on 3 September 2019. The public needs to see all information fields contained in the present NERC "searchable NOP spreadsheet", obviously to include the actual name of the entity. Also, we need to see the date the violation occurred, the duration of the violation and how it was discovered. We also need a plain English version of what happened and what type of fine was issued. This is just plain common sense. This is basic information that should be readily available without having to send in FOIA requests blindly looking for what electric utilities are wanting to hide from the public.

Please shine a bright light on this issue and err on the side of educating the public before our lights and power go out and we all wish we had acted more prudently in the public's best interest.

Respectfully submitted by:

A handwritten signature in black ink, appearing to read "Frank Heindel". The signature is written in a cursive, slightly slanted style.

Frank Heindel

Document Content(s)

Frank Heindel 10 27 2019 FERC Comments on Transparency.PDF.....1-2