ORIGINAL

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY FREGULATORY COMMISSON

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 20, 2019

I, Kenneth D. Chrosniak, 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.

I am presently a retired Army Officer, and former Government Service (GS) employee with 50 years of military and civilian federal service. Additionally, I am active within my community in Carlisle Pennsylvania and totally reliant on a secure and functional electric grid life-sustaining electrical power not only for my family, but also as the Vice President of Cumberland Goodwill EMS ambulance company, and also as an Active Firefighter with the Carlisle Fire and Rescue Company 45 supporting my community.

Establishing and maintaining two-way trust between supporting electric industries in the public which is supported demands that mutual respect must be in place, or discord and distrust will ensue. As a citizen/customer I enter into a compact/contract agreement with the supplying electric power utility to provide reliable electric power 24/7/365. The electric industry provider then has a responsibility to ensure that reliable electric power is provided to the customer to the best of their ability by conforming to established Critical Infrastructure Protection (CIP) standards established by the FERC and NERC, which includes normal to extraordinary measures in order to keep that supply of electric power to home residences and businesses/industry from being compromised by due diligence.

However, it seems now that both the electric grid industry and NERC officials do not feel the need for transparency and accountability when it comes to Grid Security. The past practice of withholding the identities of CIP standards violators does not lend itself in any way to transparency and accountability. I am pleased that FERC and NERC are considering correcting the process by providing the name of the violator, the Reliability Standard(s) violated, and the penalty amount. However, for true accountability and transparency, more information needs to be provided in order to build and maintain trust with the American people. Additional information, as indicated in Michael Mabee's Alternate Proposal, should include:

1. All information fields contained in the present any NERC "searchable NOP spreadsheet" including the name of the entity disclosed in the "Registered Entity" field.
2. Date violation discovered.

X1

3. Duration of violation
4. How violation was discovered (e.g., self-report, audit, etc.)
5. A plain English (non-technical) description of each violation.
6. Aggravating and mitigating factors in penalty assessment
7. Settlement agreement

I fully support Army Command Sergeant Major (Retired) Michael Mabee's "Alternate Proposal" that he submitted to FERC on 3 September 2019. Additionally, I do not believe that in disclosing the recommended information on CIP violators will necessarily result in a national security issue. I am a retired Army National Guard Brigadier General and combat veteran who has served nearly 38 years in the Regular Army, Army Reserve, and Army National Guard in which I have expansive and detailed experience in the handling of highly classified information from numerous command and staff assignments, and also as a Cyber Warfare instructor at the United States Army War College. Therefore, it comes as a surprise to me that whenever a utility company's CIP standard is compromised by either being hacked by a foreign entity/power/aggressor, or faulty vegetation management result again violating mandated CIP standards, why the name of the violator and selected specific information should be withheld from the trusted trusting public/customer. Most of the information involved in the violation may not necessarily reach the realm of sensitive critical information that must be protected from being released to the public. In the first place, the attacker is already quite aware of the vulnerability, that's how the utility was attacked in the first place. Secondly, any type of discussion involving possible proprietary information being released to the public and or competitor utilities should not be worthy of consideration. However, being totally realistic, releasing specific information on the means and methods relating to the violation, and subsequent mitigative efforts, would indeed be critical and sensitive information that should be secured, as information on security and protective actions implemented should maintain confidentiality. However, and most importantly, the date and duration of the violation, process by which it was discovered, resulting penalties, and settlement agreements are certainly not critical information for security purposes.

In closing, it is essential that the customer and the public have a right to know the status of the life-sustaining electrical power utilities of which they are crucially dependent upon. Any violations of CIP standards, past and present, should be open to the public to maintain total transparency and trust, and there are assurances that we have sufficient knowledge that the regulatory system is working.

Bottom-line: ensuring the name of the violator is essential, as both companies and regulators will have the proper incentive to work harder to maintain CIP standard compliance as the security and reliability of all the nations electric grids is critical to the safety of his people, and national security.

Respectfully submitted by:

Kenneth D. Chrosniak

Document Content(s)