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 3 October 2019

I, Douglas E. Ellsworth, a private citizen, respectfully submit 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 life has coincided with the span of the Cold War. From my elementary school days I recall the “duck and cover” exercises we drilled next to our seats in the classroom, to the video films we watched at school, to the placarded fallout shelters within public buildings. As time wore on into my adulthood, we were able to take some comfort that there was a deterrent that would preclude a surprise atomic attack against our Homeland – that there was a standoff known as “mutually assured destruction” (MAD). While I am not a fan of the concept of MAD these days, it was effective enough to have stayed World War III from occurring.

Today, strategic adversaries are capable of employing different methods which legitimately threaten the lives of the total American populace and our Nation's existence.

Acts of cyber penetration are among the present and continuing dangers of combined-arms warfare threats to our modern society.[1] America's Bulk Power System has been the prime target of cyber intrusions which can, and should, correctly be considered as reconnaissance – intelligence preparation of the battlespace – by adversarial nations, rogue nations, terrorist organizations and even the criminal element.

Today, unlike the Cold War days of yesteryear, there is no effective deterrent to hold at bay our strategic adversaries or rogue nations from executing selected first-strike attack methods which would be potentially sovereignty-ending. The problem is one of attribution – the ability to identify the perpetrator. Our strategic adversaries as well as rogue nations have repeatedly drilled every aspect of anonymous attack methods in military exercises, and have described combined arms warfare in open source military doctrine. This recent history supplies ample indications and warnings worthy of full attention.

Considering the problem of attribution, the only deterrent we can have against a first-strike is to deny the “yield” a would-be attacker would expect to achieve. As a whole, the electric utility industry has not responded sufficiently to this call voluntarily, and therefore it becomes prudent for increased pressure from the FERC and state regulatory bodies.

The current practice of levying fines for cyber security violations against unnamed violators has not produced a desired level of conformity to Critical Infrastructure Protection standards. I believe that naming violators is a requirement to achieve the desired result from having CIP standards. Naming violators is consistent with the oversight process as it applies to industrial sectors other than the electric industry complex, and there is no good reason to withhold the identities from inspection and audit by legislators, by state regulators, by the public, including analysts of the investment community. For this reason I am heartened by the proposals in the Joint Staff White Paper.

---

[1] Combined-arms warfare, in addition to cyber actions, include near-simultaneous coordinated physical attacks against selected keystone substations and exo-atmospheric detonations of fission or fission/fusion devices.

However, that relief within the White Paper is countermanded by a provision in that same document which fundamentally allows the NERC to consider any incident as Critical Energy Infrastructure Information (CEII) and thereby hidden from public access. Moreover, the White Paper continues to provide that the identities of past violators be hidden from public review.

Obviously, achieving a balance between transparency and security concerns is paramount in this matter. It is for these reasons that I endorse and support the program alternative filed by U.S. Army retired Command Sergeant Major Michael Mabee, "Comments and Alternate Proposal," submitted to FERC on 3 September 2019.[2]

The Alternate Proposal of CSM Mabee provides transparency to the public and therefore supplies the incentive to industry to take the due care required by the public interest. Moreover, the Mabee proposal precludes industry's attempts to hide behind an undeserving "security risk" construct.

I am also familiar with industry opposition to the White Paper and the Alternative Proposal of CSM Mabee. It seems as if, once again, there exists a conflict between the interests of the electric power complex and the interests of public welfare. The question that arises is: "To which side does the FERC owe its allegiance?"

Respectfully submitted,

Douglas E. Ellsworth

---

[2] https://elibrary.ferc.gov/idmws/common/downloadOpen.aspdownloadfile=20190903%2D5033%2833768996%29%2Epdf&folder=16766509&fileid=15340441&trial=1

Document Content(s)