Dear \_\_\_(Public Utility Commissioners and Staff…or Consumer Advocate POC)\_\_\_\_\_:

My name is \_(Name)\_\_\_ and I am a resident of \_(State)\_\_\_\_ where I understand you are involved in advocating on behalf of our state’s citizens.  Therefore, I would like to inform you of a critically important issue related to the security of the electric grid upon which all our state’s infrastructure and our population depends.

The Federal Energy Regulatory Commission (FERC) currently has an open docket for disclosure of the identities of utility violators of Critical Infrastructure Protection (CIP) standards. From a grid security perspective, this is one of the most important matters in the past several years. Here is a background article: <https://www.utilitydive.com/news/ferc-nerc-propose-to-publicly-identify-utilities-violating-cybersecurity-s/562205/>

Currently, FERC and its designated Electric Reliability Organization, the North American Electric Reliability Corporation (NERC), withhold the names of electric utilities that violate CIP standards. The stated reason for this practice is to keep confidential information that may aid potential adversaries. However, this practice has also allowed utilities to avoid public scrutiny when they repeatedly violate standards, placing the public at grave risk of blackout. (For more information on this, see the “Reasons Why Transparency is Needed for Grid Security” listed below.)

Under pressure from Congress and the public, FERC is now considering disclosing the names of CIP standard violators, as well as other administrative information on CIP standard audits. Federal officials have repeatedly stated that cybersecurity adversaries have penetrated the U.S. electric grid, so it is clear that that current “secret regulatory system” is not working.

The FERC docket is AD19-18-000.  Filings can be accessed through the FERC eLibrary system using the “General Search” function: <https://www.ferc.gov/docs-filing/elibrary.asp>

Since your office exists to represent the public interest, not the interests of the electric utilities, I would hope that you would be receptive to submitting comments on FERC Docket AD19-18-000 in favor of disclosing the names of utilities who violate NERC Standards.

I am not the only person hoping for this transparency and believing that your office has a stake in this matter.  In the attached statement from FERC Commissioner Cheryl LaFleur, you will see that she states:

*“I believe state regulators, members of the public, and others have a legitimate interest in such violations, and we should seek to achieve as much transparency as we can consistent with protecting legitimate security interests…I hope that we receive a wide range of comments on the White Paper, including any suggestions for alternative processes, which will allow FERC and NERC to move forward on this issue.”*

In addition to the attached statement from Commissioner LaFleur, I have attached the actual FERC/NERC White Paper as well as an "Alternate Proposal" authored by Mr. Michael Mabee.  I believe Mr. Mabee's Alternate Proposal would achieve the type of transparency we need to change corporate culture to become more serious about electric grid security.  I ask that you review these and that your office go on the record one way or another on this critical issue for grid security.  Please do reply to confirm receipt of this email. Thank you.

 Very Respectfully,

Attachments: 1-LaFluer Statement, 2-NERC-FERC-WP, 3-MabeeAlternateProposal

**Four Compelling Reasons Why Transparency is Needed for Grid Security**

These four areas of concern point to systematic, pervasive flaws in the regulation and protection of the electric grid. Critical information is being withheld from the public and conflicting (and misleading) information has been disseminated by NERC, lulling citizens, investors and Congress into a false sense of security.

***Vast Disparities Exist in Electric Grid Incident Reporting:***

* *Physical Attacks:* There were 578 physical attacks against the grid reported to the Department of Energy between January 1, 2010 through May 31, 2019. Yet according the NERC annual reliability reports, there was only one during the same period.
* *Cyber Attacks:* There were 29 cyberattacks against the grid reported to the Department of Energy between January 1, 2010 through May 31, 2019. Yet according the NERC annual reliability reports, there were none during the same period.

***Lack of Enforcement of Already Inadequate Physical Security Standards:***

* *The physical security standard itself—CIP-014-2 (Physical Security)—is inadequate.*There is no requirement that an entity’s risk assessment or physical security plan be reviewed by anyone with physical security knowledge. There is no determination whatsoever as to the effectiveness of any entity’s physical security plan.

* Enforcement of CIP-014-2 (Physical Security) seems nonexistent: In the six years since the Metcalf California substation attack, there have been only 4 citations issued for violations of the physical security standards. And these 4 were for administrative violations.

***Cybersecurity Standards Remain Inadequate:***

* Despite the fact that the malware is what took down the electric gird in the Ukraine in 2015 and 2016, there remains no requirement that malware in the North American electric grid be detected, mitigated and removed.

* The electric industry, including industry lobbyist Edison Electric Institute—whose members include the government of the People’s Republic of China—claim that additional cybersecurity protections would be “unduly burdensome” and “unnecessary.” And The Federal Energy Regulatory Commission bought the argument.

***Systematic and Permanent Coverup of Identities of Regulatory Violators:***

* Since July of 2010, the identity of every violator of Critical Infrastructure Protection (CIP) standards has been withheld from the public, investors and Congress. As of this writing, there have been a total of 253 FERC dockets involving at least 1484 regulatory violators covered up.

* NERC and FERC are attempting to permanently withhold these names of the violators despite the fact that the violations in most cases have been long ago mitigated.