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 and Alternative Proposal

Submitted to FERC on October 28, 2019

Jerry R. Ladd and James M. Babcock, owners of CIWRX, Inc. who cumulatively have over 60 years of both publicly traded and privately held Information Technology, Artificial Intelligence, Cyber-security, Computer Consulting and Software as a Service, and enterprise level "C Suite" subject matter expertise mostly, as serial entrepreneurs, respectfully submit comments and an alternate proposal on FERC Docket No. AD19-18-000, Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards. In recognition of the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) Joint White Paper Proposal to seek more transparency in Notice of Penalty (NOP) filings, this alternative Proposal is being presented.

Transparency is critical to the security of the Bulk Electric System (BES) for several reasons. It not only provides a safety-net to the general public, but it is an incentive for companies to comply with the Critical Infrastructure Protection (CIP) standards. This mitigates FERC/NERC risks associated with the legal reasonableness culpability determination in litigation and enforcement actions, as well as vicarious liability or absolute liability between

FERC, its trade associations, the general public, possible future civil liabilities, and or criminal prosecutions. That transparency is absolutely necessary to highlight bad actors, adversaries, hacker intrusions, and (NOP) filings to the critical bulk power system infrastructure in order to prevent FERC liability associated with its pervasiveness of not having full disclosure of those public risks. The public sector should be informed to the fullest extent so they can evaluate the inherent risk associated with the BES failures to be able to manage and mitigate those vulnerabilities to their business enterprises, public communities and general populations. FERC has the responsibility to disclose all information while mitigating risks of additional intrusions, member vulnerabilities, customer inadequacies, software and firmware weaknesses, or failures because of those disclosures or lack there-of. Due to the urgency to resolve this conflicting matter, CIWRX felt it necessary to develop, self-fund and implement, a workable browser and mobile accessible Artificial Intelligence, Software as a Service (SaaS) solution for the private, public and governmental benefit, (FERC/NERC), to protect the Bulk Electric System.

Introduction/Background

In February of 2014, Jerry Ladd as a data scientist/entrepreneur, and James Babcock as a software architect/entrepreneur, began researching and developing a multi-layered security access model and SaaS product platform which could operate in-the-cloud, on premise or any other model-including the ability to have browser and mobile accessibility.

On February 25, 2018 Jerry R. Ladd submitted comments in FERC AD17-9 Cyber Security Incident Reporting Reliability Standards because of concerns related to securing the BES grid. Upon reading all of the respondents' comments, Mr. Ladd realized that there were major impediments to securing the grid. He then advised Mr. Babcock, a business

associate of 25 years, of the criticality and the gaps in the cyber-security, reporting, and securing the grid within NERC/FERC, the CIP, CEII rules and regulations being used to slow walk the trade association's mandated change. Cyber Security Risk Information Sharing Program (CRISP) and self-reporting of the trade associations was becoming very problematic for securing the grid.

Because of that urgency and need to focus all efforts on the task of securing the grid from adversaries, hackers, bad actors and technologically challenged administrative efforts of some in previous administrations, the speed at which intrusions and failures to the grid were occurring was at a velocity absolutely unacceptable and needed to be a priority. Mr. Ladd and Mr. Babcock dissolved all other business relationships and formed CIWRX with the specific Intent to build an artificial intelligence SaaS Product which could be customized to protect the grid as well as other enterprise markets, federal agencies, and DOD departments.

It is understood that there is a reluctance by FERC/NERC and the trade associations to have information shared or disclosed to the public, as the go-to line for the commission seems to be "we have (CEII) objections". 18 C.F.R. § 39.7 (b)(4) and CEII considerations were evaluated carefully by CIWRX before submitting this alternate proposal.

Joint Staff White Paper Proposal

The new proposed Joint Staff Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards proposal to submit a CIP NOP with a public cover letter and a confidential attachment, does not contain enough relevant information to either inform the public of critical security breaches or enough information to change and improve the current notices of penalty pertaining to CIP.

Those revisions are as follows:

1. the name of the violator
2. the reliability standard(s) violated (but not the requirement or sub requirement violated,
3. and the penalty amount

There are eleven CIP Reliability Standards and they are highly complex. They are as follows:

CIP-002-5.1a Cyber Security -BES Cyber Systems Categorization

CIP-003-6 Cyber Security - Sescurity Management Controls

CIP-004-6 Cyber Security – Personnel & Training

CIP-005-5 Cyber Security – Electronic Security Perimeter(s)

CIP-006-6 Cyber Security-Physical Security of BES Cyber Systems

CIP-007-6 Cyber Security-System Security Management

CIP-008-5 Cyber Security-Incident Reporting and Response Planning

CIP-009-6 Cyber Security-Recovery Plans for BES Cyber Systems

CIP-010-2 Cyber Security-Configuration Change Management and Vulnerability Assessments

CIP-011-2 Cyber Security-Information Protection

CIP-014-2 Physical Security

For brevity purposes, a quick perusal of CIP-002-5.1a, Cyber Security-Systems Categorization, which has 37 pages of documentation, all of which are important, relevant and informative to trade association violators, administrators, and bad actors, must have CEII guidelines if the Grid is to be protected. It is a fact that certain fields included in reports to the public could become problematic and jeopardize the security of the Bulk Power System. That being said, there are proactive, programmable methods to optimize those disclosures without giving away the secret sauce and formulas to bad actors. Those methods, algorithms, models

and processes will not, and should not, be discussed in this open comment. A demo of those processes and methods can be viewed upon request by contacting CIWRX[1] .

Determining which information can be disclosed to the public for transparency purposes and which NOP CIP reliability standard fields may have the greatest impact to CEII is better suited for private discussions. One thing is for sure, the current Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards falls short for informing the public for transparency purposes.

FOIA Requested Information/CEII

CEII should not be the excuse for FERC/NERC to withold critical information from the public. Requiring FOIA requests to bottleneck that transparency is a mistake and shows bad faith. Attacks against the GRID from bad actors are extremely sophisticated. Proactive, preventative measures are required to thwart those attacks. Assuming that bad actors are waiting for FERC/NERC CEII information to attack the grid is an absolute mis-calculation. We understand that you make it easy for adversaries by giving them a roadmap for their intrusion, but roadmaps are fine if you have already mitigated the path where the bad actors go.

Blocking FOIA requests to get information on trade associations failures, penalties and instances could be extremely problematic if blocking those requests caused harm and damage. Mitigating risks associated with CEII instances should be paramount, not blocking FOIA requests. Digital Technology has moved way beyond having someone file a legal document to get information on digital attacks to the Bulk Power System. Technology is moving faster than the protective nature of personal agendas. Delaying preventative measures puts the public, and the trade associations as well as FERC/NERC at risk.

[1] Contact jerry.ladd@ciwrx.com 9802 Nicholas Street, Suite 350 Omaha, Nebraska 68114

Alternate Proposal

CIWRX proposes that a new process be used by FERC/NERC on Notices of Penalty (NOP) Pertaining to Violations of Critical Infrastructure Protection (CIP) Reliability Standards. It is in dire need of an upgrade to an advanced technology method to secure the grid while making certain FERC/NERC controllable data is transparent to the public. This process begins with secure data, how it is collected, where it is stored, how it is secured, who has access to it, how it can become useful, helpful, transparent, relative, and how not to allow bad actors to use it (CEII). With artificial intelligence and a strong multi-level FERC/NERC security model, CIWRX has developed a platform, Xlab5000[2], which was architected with the capability and security to be placed, and stored in FedRAMP, if necessary. It is a method that customizes relevant data fields using audited secure data captured and stored in order to do predictive analytics, and artificial intelligence. The SaaS also has features that have strong auditable methods which are necessary to keep the BES/BPS secure from intrusions, while making the private/public information optimally transparent, be it CEII, CIP, NOP or custom fields, programs, enterprises, trade associations, laws, or rules. Using XLab5000 SaaS model with CIWRX's preventative artificial intelligence front end would make it unnecessary for NERC to use a term such as “unidentified registered entity” or “URE ”. There also would be no need to withold the identity of the URE, because the CIP, NOP would not reasonably provide useful information to a person planning an attack on critical infrastructure, as any log of such attack would be circumvented by the installation of the security within the SaaS provided by the architected model of the XLab5000 software. Listing the names and other fields of the CIP violators within the SaaS platform would recognize, not only the self-reporting mechanism which could possibly reduce the CIP Penalty to the trade association, but also the culpability

[2] XLab5000 SaaS Artificial Intelligence Cyber Security Platform Developed by CIWRX

score along with reducing the associators pervasiveness and NERC's and administrators continued tolerance of their actions. The SaaS would show that the violators were being proactive with such attacks and had implemented a solution for future attackers, therefore thwarting bad actor attempts. The SaaS security, coupled with the artificial intelligence predictive measures would be a reasonable preventative measure for any trade association to mitigate attacks and intrusions or failures of security policy. This therefore, would help to satisfy a corrective action within a "reasonableness" argument during lawsuits, litigation and enforcement actions.

Because all entities would be transparent, and the artificial intelligence would determine which information was too dangerous to allow public access, any such dangerous information could be considered with CEII and 18 C.F.R. § 39.7 (b)(4)[3] which would still apply. If the information was too sensitive, or was "classified", it could be moved to FedRAMP if necessary. The artificial intelligence would determine which data needed to be disclosed to the public in order to optimize transparency, while still letting the commission control being vigilant and cognizant of rules, regulations and their business model needs. The number of FOIA requests would diminish as the SaaS became a requirement within NERC/FERC trade associations. The requirement of using such an analytic tool set by the CEII[4] coordinator, would eliminate the time necessary to consult with technical staff and could optimally remove impediments to the public transparency. The Ad-Hoc Reports that are generated by the SaaS can be exported to text and excel spreadsheets, which would help the CEII coordinators' efforts and would optimize information with the Information Security and Systems Assurance Division

[3] Enforcement Reliability Standards

[4] Information related to critical electric infrastructure information generated by or provided to the Commission or other Federal agency other than classified national security information pursuant to section 215A(d) of the Federal Power Act.

(ISSAD), Federal Information Security Management ACT (FISMA), OMB, GAO, Homeland Security, the Data Governance Division (DGD) as well as many other agencies as needed. The SaaS incident database includes a revisable format field as well as an extensive list of fieldchoices formalizedbased on the specific needs of FERC/NERC, the current 11 CIP Reliability standards and the optimization of the artificial intelligence of the SaaS. CIWRX has researched additional fields that would be a good baseline for fields based on CIWRX's understanding of the need of the BES/BPS requirement but FERC/NERC's input can be easily implemented with modifications and enhancements to the SaaS.

We have included customized dashboards with user interfaces that are available, as well as a NO-CODE[5] Integration Functionality feature to develop personalized applications with minimal training or programming experience to help specific trade associations with their unique business rules. The entire SaaS was developed as a CEII protection plan with an artificial intelligence front end. The protection plan can share timely and actionable solutions to other federal agencies while optimizing relevant data, security, and public safety. It lets NERC as the certified ERO control the data and fields going to the personel of owners, operators and users of the critical electric infrastructure with a public/or private option. It can help FERC/NERC to stay in compliance with FOIA, while staying exempt from disclosure with 5 U.S.C. §552(b)(3). That same option is available for violations, compliance, physical attacks, cyber attacks, electromagnetic pulse attacks, severe weather, and scismic events. It has the capability to mind map, optimize, and geo-fence various categories and supply-chain items to secure the critical electric infrastructure and secure the grid.

[5] No-code development platform allows programmers and non-programmers to create application software through graphical user interfaces and configuration instead of traditional computer programming.

Summary

An advanced technology method must be implemented in keeping with the pace at which technological changes are being developed. Cyber security techniques must stay AHEAD of the bad actors who are attacking the grid infrastructure. These attacks are increasing in size and sophistication, unparalleled in the past. A rear view mirror cyber security approach, making corrective actions after an intrusion has taken place and hiding it from the public is no longer an option that the Bulk Electric System, FERC/NERC or the trade associations can risk. It must be mitigated before an event takes place. That process can only be accomplished if both private and public are aware and both know the risks associated with not taking corrective action. Without a forward looking artificial intelligence plan, the current CEII regulation and 18 C.F. R. § 39.7 (b)(4) will be the Achilles heel of the BES failure.

Most Cyber Security companies are great at doing forensic analysis of intrusions and vulnerabilities, but most don't understand artificial intelligence and the need to use "clean", secure data. Malicious triggers imbedded via that data must be protected with CIP Infrastructure protection reliability standards, and those standards must be transparent to the public so they understand the intrusive nature of attacks to the grid and how FERC/NERC is mitigating such threats proactively to "reasonably" protect the public.

The liability of not moving forward with this alternate proposal far outweighs any reason for FERC/NERC or the trade associations to reject it. The future survival of FERC/NERC, the trade associations, the Bulk Power System and the public are depending on a Proactive approach to FERC/NERC Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards. The public deserves to have transparency with Information from FERC/NERC , but a careful protection plan is needed. CIP, NOP, CEII, disclosure within the guidelines of 5 U.S.C § 552(b)(3) is also necessary.

We have taken three years to devise that protective plan.

Therefore, we are submitting it as a comment in Docket No. AD19-18-000

Respectfully submitted,

Jerry R. Ladd

CIWRX

Document Content(s)