UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NERC Full Notice of Penalty regarding	**)**	
[Redacted in Public Version of NOP]	**)**	**Docket No. NP19-4-000**
	)	

MOTION TO INTERVENE

Submitted to FERC on _____Date_____

I, Frank J. Gaffney, a private citizen, request the Commission's leave to intervene in the above captioned docket, pursuant to 18 C.F.R. § 39.7(e)(4).

After serving in the Reagan administration in various positions, including acting as the Assistant Secretary of Defense for International Security Policy, I founded the Center for Security Policy – a not-for-profit, non-partisan educational corporation which strives to provide timely, informed analyses and recommendations concerning critical foreign and defense policy challenges. Our organization considers one of the most important portions of our security portfolio is encouraging policy to protect our nation's *most* critical infrastructure – the U.S. electric grid.

A year ago, I joined many other national security minded individuals and organizations to petition your agency to improve mandatory reporting of cyber security incidents among the owners and operators of our nation's electric grid. This petition was in relation to Docket Nos. RM18-2-000 and AD17-9-000: Cyber Security Incident Reporting Reliability Standards.

The Office of Information and Regulatory Affairs provides the following abstract to describe Docket Nos. RM18-2-000 and AD17-9-000:

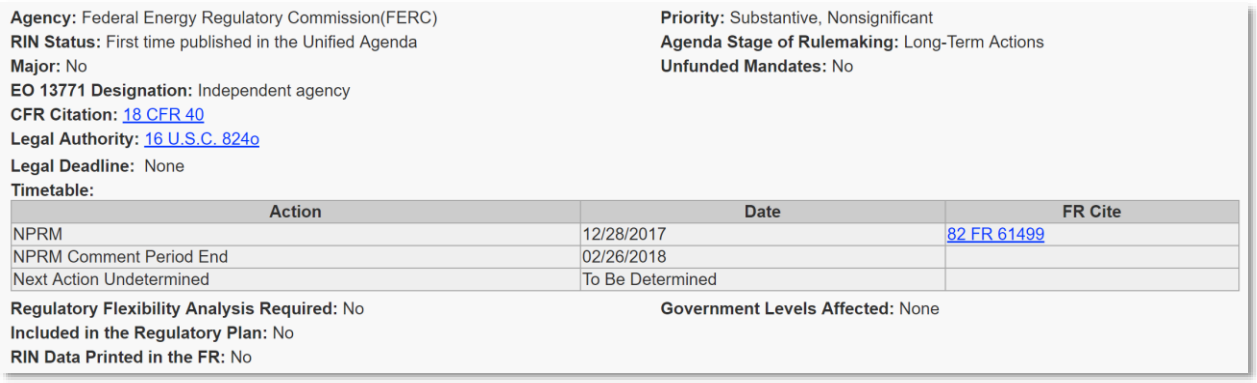
> The Commission proposed to direct the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization, to develop and submit modifications to the NERC Reliability Standards to improve mandatory reporting of Cyber Security Incidents, including reporting of incidents that might facilitate subsequent efforts to better understand and respond to cyberattacks that could harm the reliable operation of the bulk electric system. Specifically, current NERC Reliability Standards only require reporting of cyber incidents that result in actual cyber incidents that compromise the electric grid. NERC's Annual Reports for several years have shown zero reported incidents under this reporting standard. To obtain more granular and useful information, the Commission proposed to require NERC to improve the reporting so that it includes "attempts" to compromise the electric grid, even when no actual harm occurred (Docket Nos. RM18-2-000 and AD17-9-000).

My comments on the docket cited scores of evidence pointing toward the real and present danger that our nation's adversaries have penetrated the cyber defenses in our energy sector and I requested that FERC order NERC to set an enhanced standard for malware detection, reporting, mitigation, and removal. I also reminded your agency that it has the authority under Section 215(d)(5) of the Federal Power Act to order such a reliability standard to address the yawning gaps in the current NERC cybersecurity policy and that such action would shore up both grid security and national security writ

large since it could help facilitate multi-direction information sharing between U.S. intelligence agencies, cybersecurity vendors, and electric utility companies and also help both the Executive and Legislative branches of government conduct proper strategic planning to deal with adversaries targeting the nation's electric grid.

Notably, out of the numerous (27) sets of comments on these dockets, less than half (11) disagreed with the value of an enhanced cyber security standard, but all of them were members of the electric utility industry you regulate. Rather, the overwhelming sentiment among those industry insiders was that an enhanced cybersecurity standard would be too "burdensome." In fact, in the 240 pages worth of compiled comments for Docket Nos. RM18-2-000 and AD17-9-000, the word "burden" appeared 56 times and the phrase "unduly burden" appeared 6 times.

From my research into the results of this debate, it appears that your agency required NERC to set a reliability standard for cybersecurity incident reporting but the below screenshot from The Office of Information and Regulatory Affairs demonstrates to the public that your next action on this matter is "to be determined."



Agency: Federal Energy Regulatory Commission(FERC)
RIN Status: First time published in the Unified Agenda
Major: No
EO 13771 Designation: Independent agency
CFR Citation: 18 CFR 40
Legal Authority: 16 U.S.C. 824o
Legal Deadline: None
Priority: Substantive, Nonsignificant
Agenda Stage of Rulemaking: Long-Term Actions
Unfunded Mandates: No
Timetable:

Action	Date	FR Cite
NPRM	12/28/2017	82 FR 61499
NPRM Comment Period End	02/26/2018	
Next Action Undetermined	To Be Determined	

Regulatory Flexibility Analysis Required: No
Included in the Regulatory Plan: No
RIN Data Printed in the FR: No
Government Levels Affected: None

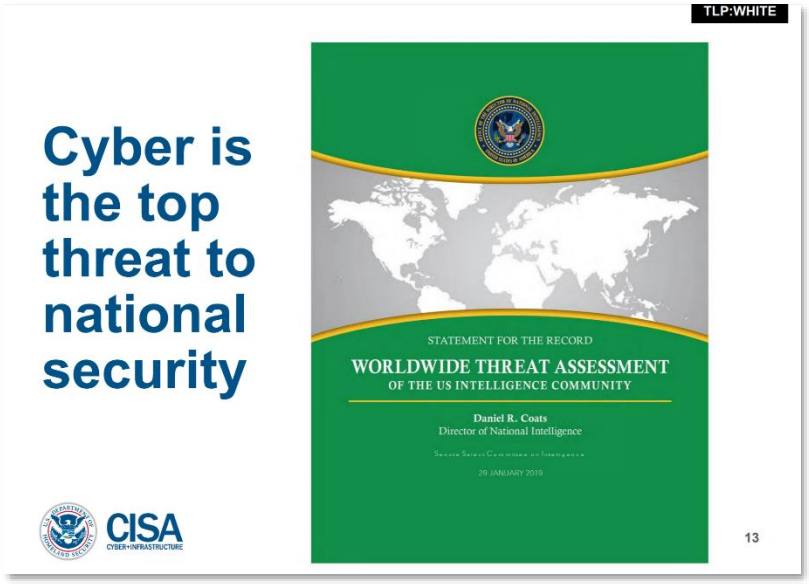
What is also "to be determined" is just how long our nation will go before it suffers a debilitating cyber attack on the grid and its other life sustaining infrastructure.

The public recognizes that even after the "Great Northeast Blackout (which took place on 14 August 2003 and was caused by inadequate vegetation management practices that led to tree contact), it took NERC and your agency until March 21, 2013 - nearly a decade - to establish and approve a final rule for "Transmission Vegetation Management" (FAC-003-2). The American public cannot afford such a slow process when it comes cybersecurity and the U.S. electric grid.

In a hearing before the 114th Congress' Subcommittee on Economic Development, Public Buildings, and Emergency Management entitled "Blackout! Are We Prepared to Manage the Aftermath of a Cyberattack or Other Failure Of The Electrical Grid?" (April 14, 2016) the committee noted that:

> *"The DHS reports that the energy sector is the target of more than 40 percent of all reported cyberattacks. In 2014, the National Security Agency (NSA) reported that the agency had tracked intrusions into industrial control systems by entities with the technical capability 'to take down control systems that operate U.S. power grids, water systems and other critical infrastructure'."* (Page vii. Internal citations omitted.)

Meanwhile, the cybersecurity threats to our nation's electric industry have continued to grow. For example, in an awareness briefing titled "Chinese Cyber Activity Targeting Managed Service Providers" hosted twice in February 2019 by the US Department of Homeland Security's Cyber and Infrastructure Security Agency (CISA), the CISA warned American IT companies that the Chinese government has been successfully utilizing a method of wholesale cyber espionage by targeting the cybersecurity and IT service providers for numerous industries. These briefings highlighted the findings of the Office of the Director of National Intelligence (ODNI) in its 29 January 2019 Worldwide Threat Assessment. As can be seen in the accompanying DHS CISA slide, this ODNI assessment – like every annual assessment since 2013 – named "Cyber" as the #1 threat to our National Security.



This ODNI Threat Assessment went on to state that "China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure." It also stated that "China has the ability to launch cyberattacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States." This report builds upon more than a decade of open source media revelations and U.S. Government warnings that Russian malware is already present in the U.S. electric grid.

These revelations undoubtedly informed an important hearing by the U.S. Senate Committee on Energy and Natural Resources on 14 February 2019: "Hearing to Consider the Status and Outlook for Cybersecurity Efforts in the Energy Industry." Senator Angus King of Maine asked a number of cybersecurity-related questions to NERC's CEO and President James B. Robb and Mr. Robb's responses leave the public doubtful of NERC's seriousness to address cybersecurity threats. Below is an example exchange from this hearing:

> Sen. King: "Okay let me ask another question. Do any of our utilities have Kaspersky, Huawei, or ZTE equipment in their system?"
>
> Mr. Robb: "We issued a NERC alert."
>
> Sen. King: "I didn't ask you if you issued an alert. I asking you do any of our utilities have ZTE, Huawei, or Kaspersky equipment or software in their system?"
>
> Mr. Robb: "Not to my knowledge."
>
> Sen. King: "Not to your knowledge. Have you surveyed any of the utilities to determine that? "

Mr. Robb: “Uhhh, I don’t believe we have.”

Sen. King: “I think that would be a good idea don’t you?”

Mr. Robb: “I’ll take that on.”

This hearing, and NERC’s CEO’s testimony, raises an important question to the public. Just how long will it take NERC and your agency to set a reliability standard for cybersecurity incident reporting if NERC has not yet even taken the steps to survey its utilities to determine the existence of ZTE, Huawei, or Kaspersky equipment or software, despite numerous intelligence community and homeland security related warnings?

A related question is whether or not NERC’s current practice of hiding and redacting identities and other identifying information about Critical Infrastructure Protection (CIP) standards violators is an overwhelming contributor to the lack of urgency within the industry to fix cybersecurity vulnerabilities. This lack of urgency was noted by Senator King during the Valentine’s Day hearing and is observed by the general public. NERC “issuing an alert” on a cyber security threat is much different than NERC transparently holding accountable those that fail to uphold CIP reliability standards, as such “alerts” don’t get the attention of the C-Suites in these companies.

Members of my staff have attended numerous cybersecurity-related briefings and workshops attended by members of the electric utility industry and have observed that the operational technicians and cybersecurity experts working for these utilities routinely bemoan what they describe as an overall lack of interest in the topic of cybersecurity among the corporate elite in the industry. We believe this is precisely because the C-suite has little concern that its company’s identity will be made public to customers or shareholders if they violate cybersecurity protocols.

We believe NERC is improperly using the Critical Energy/Electric Infrastructure Information (CEII) rule to hide the identities of entities that violate CIP reliability standards – even when there is no arguable security need to withhold this information. Your agency holds the key to reversing this practice and the resulting lackadaisical treatment of critical infrastructure protection among NERC’s utilities.

For example, the public has observed that the Securities and Exchange Commission does not hide the identities of companies and individuals subject to regulatory actions under U.S. securities laws; that when the Food and Drug Administration recalls food due to public safety concerns it does not redact the names of the food brands; and when an aircraft crashes the National Transportation Safety Board doesn’t try to hide the name of the aviation company or aircraft manufacturer.

The risks of unhealthy food, irresponsible investment, or unsafe aircraft travel pale in comparison to the risk to the American public of a prolonged or widespread blackout caused by a cyberattack, or any other breach of CIP reliability standards. The public realizes this and also realizes that your agency has the authority under the Federal Power Act to protect the public interest by enforcing the same types of disclosure practiced in every other aspect of regulation in our free society.

Therefore, I request that 1) the Commission review this Notice of Penalty (NOP) to ensure that it is in the public interest, and 2) that the name of the entities(s), the unredacted Notice of Penalty and the unredacted settlement agreement be released in the public docket. I also request that FERC consider

the serious reality that NERC has been redacting the names of the companies violating CIP reliability standards since July 6, 2010 – for more than 8 years – and whether these redactions are still necessary and this practice is helpful to the overall security of the American public.

I also believe that the precedence of your agency allowing NERC to hide the names of CIP reliability standard violators has the potential to lead regulators at the state and municipal level doing the same thing for the utilities they oversee. For these reasons I am sending a copy of this intervention to executives of the Federal government as well as the Executive Committee, National Association of Regulatory Utility Commissioners so this important topic can be considered by policymakers at all levels of government.

Ultimately, I believe it is clear that that NERC's secrecy has not made their associated companies more vigilant and that the American public deserves to know if their own electric utilities are not taking cybersecurity seriously.

Sincerely,

Frank J. Gaffney
Executive Chairman
Center for Security Policy

Copy to:
National Security Advisor, National Security Council, Executive Office of the President
National Infrastructure Advisory Council
Secretary of Energy
Secretary of Homeland Security
Executive Committee, National Association of Regulatory Utility Commissioners