



## CENTER FOR SECURITY POLICY

Frank J. Gaffney, Jr., President & CEO

29 May 2018

Chairman Kevin J. McIntyre  
Commissioner Neil Chatterjee  
Commissioner Cheryl A. LaFleur  
Commissioner Robert F. Powelson  
Commissioner Richard Glick  
Federal Energy Regulatory Commission  
888 First Street, NE  
Washington, DC 20426

### **Comments submitted in FERC Docket NP18-7-000 on a Notice of Penalty for an Unidentified Registered Entity**

Dear Chairman McIntyre, Commissioner Chatterjee, Commissioner LaFleur, Commissioner Powelson, and Commissioner Glick:

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.

Among the most critical of those challenges are the various, looming threats to America’s electric grid. Consequently, from the time of the Commission on the Electromagnetic Pulse (EMP) Threat’s first report to Congress in 2004 to the present day, the Center – like many other leaders in the national security arena – have been warning that the grid’s lack of resilience poses a potentially existential danger to our country.

As you know, this vulnerability can be exploited by enemies using a variety of techniques including physical sabotage, electromagnetic attack, or cyberattack. Given that the very survival of our nation depends upon the protection of grid assets against these forms of attack, there is great public interest in doing so.

During the comment period for Docket RM18-2-000 on Cyber Incident Reporting, our organization argued that it is necessary that the Federal Energy Regulatory Commission (“FERC” or “the Commission”) order NERC to set an enhanced standard for malware detection, reporting, mitigation, and removal. This commonsense recommendation – which was vehemently opposed by others on the docket, including many in the electric utility industry who claimed such a standard would be “unduly burdensome” and “unnecessary” – was apparently unpersuasive to FERC since no such enhanced standard has been established to date.

Even though FERC has the authority under Section 215(d)(5) of the Federal Power Act to order a proposed reliability standard to address the yawning gaps in the current NERC cybersecurity policy, it “declined to propose” additional Reliability Standard measures, to the potentially severe detriment to our national security and the safety of hundreds of millions of Americans.

During our organization’s comments for Docket RM18-2-000, we listed ample evidence from the public domain pointing to the rapidly increasing risk of malware present in information technology (IT) and operational technology (OT) associated with electric grid infrastructure, posing a grave and immediate danger to the American people who depend on this infrastructure for daily life. Even since the time of our previous comments in February 2018, more has been learned about the incredible effectiveness of Russian SVR (Foreign Intelligence) and Russian Ministry of Defense (MOD)/GRU (Military Intelligence) actors’ reconnaissance of U.S. grid IT systems; surreptitious penetration of those systems; modification of software and firmware; and ability clandestinely to withdraw without a trace.

As recently as March of this year, the U.S. Department of Justice reported that your own Commission was the target of a massive cyber operation orchestrated by the Islamic Republic of Iran to steal information from governments and private companies worldwide.

Meanwhile, as you well know, at the same time as these adversaries of our nation were busy penetrating the cyber systems of our government and private energy industry, one of our nation’s largest utilities unwittingly allowed a massive 590-day data breach, including 680,000 log entries, violating Security Management standards specified in CIP 003-3 Requirement R4 (*implement a program to identify, classify and protect information associated with CCA assets*) and Requirement R5 (*implement a program for controlling access to CCA information*) and putting the National Security installations on the West Coast of America at risk – to say nothing of major urban areas and private corporations working in Silicon Valley. This very same utility suffered one of the most renowned and frightening physical attacks on its infrastructure in April 2013. And a year later, in 2014, it failed to keep thieves from stealing assets within the previously targeted substation, possibly encouraged by the utility’s suggestion that the previous penetration of their infrastructure was mere “vandalism.”

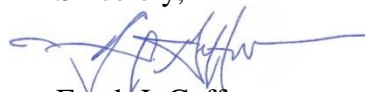
Incredibly, despite the Western Electricity Coordinating Council concluding that the cyber security violation posed a severe risk to the Bulk Electric system (“BES”) and the assessment of a \$2.7M penalty, your commission seems disinclined to identify this utility and its offending contractor, contrary to the clear interests of its customers and investors and the public at large. As such, not only does FERC deny the opportunity for “lessons learned” to be shared among other utilities, it signals to the owners and operators of our nation’s most critical infrastructure that the “business as usual” culture of lackadaisical security can remain in place for our adversaries to exploit.

With Docket NP18-7-000 and its Notice of Penalty for an Unidentified Registered Entity, FERC has the opportunity to be transparent about this dangerous cyber security breach, and publicly identify the currently “Unidentified Responsible Entity” and “Unidentified Contractor-Vendor.” As an agency of the Federal Government, FERC has the power to request a joint investigation

with other Federal Agencies to help both determine adversarial access to the utility's system and to inform future cyber security policies of the U.S. Government and private industry.

The Center for Security Policy once again calls on you to exercise your authority to require clearly necessary enhancements of the U.S. electric grid's resiliency to cyber and other forms of man-induced and naturally occurring threats. To do otherwise is to be complicit in the reckless perpetuation of grave dangers to the public safety and national security.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Frank J. Gaffney', with a long horizontal flourish extending to the right.

Frank J. Gaffney  
President and CEO

cc: Hon. Rick Perry, Secretary of Energy

Document Content(s)

FrankGaffney-FERC-DocketNP18-7-000.PDF.....1-3