20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

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 26 September 2019

I, Frank J. Gaffney, 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.

Background:

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 and programs requied to enhance the resiliency of the Nation's *most* critical infrastructure – the U.S. electric grid.

More than a year ago, I joined many other national security-minded individuals and organizations to petition your Commission 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.

On 28 March of this year, I submitted a motion to intervene in Docket No. NP19-4-000 with this stated purpose:

> "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 Angus King during a hearing on 14 February 2019 and is observed consistently 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. We ask that the identity of standard violators be made public by FERC."

That intervention provided FERC with scores of examples of the real, present and growing cybersecurity threats to the electric grid and evidence of the lack of sense of urgency on the part of the electric power industry – especially among the corporate leadership – about fixing cybersecurity vulnerabilities. I summarized the view of a broad coalition of national security experts by stating: "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."

Given this background, I am somewhat encouraged to see the "White Paper" proposed by the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC). If, in fact, these organizations are *truly* seeking more transparency in Notice of Penalty (NOP) filings, I commend them. Such public transparency is critical to the security of the bulk power system as it provides an incentive for companies to comply with mandatory Critical Infrastructure Protection (CIP) standards. It also provides the means for public, investor, congressional and state scrutiny and evaluation of the violators and the regulatory system. However, the White Paper does not inspire confidence that such transparency actually *is* the goal.

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

Concerns with the Proposed White Paper

I am concerned that the current White Paper proposal provides only a limited amount of transparency that does not give Congress, investors, other regulators, or the public sufficient information to determine whether or not these companies are complying with their obligations to protect the critical infrastructure upon which all of our lives depend. I also believe that the White Paper proposal does not provide sufficient information on CIP violations and violators to determine with certainty whether the regulatory system is, in fact, working for the public interest. For example, the White Paper provides caveats that will enable NERC to treat almost anything as Critical Energy Infrastructure Information (CEII) and it also closes the door on any public scrutiny of past CIP violators whose identities have thus far been obscured.

Support for an "Alternate Proposal"

I am familiar with the research, analysis and public dissemination of information about CIP violators conducted by retired U.S. Army Command Sergeant Major (CSM) Michael Mabee and believe that he is well-qualified to propose an alternate approach that would satisfy the public interest in relation to both the workings of the regulatory system and the compliance of the industry to CIP standards. I am satisifed that CSM Mabee is working for the public interest and is not a self-interested party that could personally profit from this advocacy for transparency.

I carefully reviewed the Comments and Alternate Proposal[1] submitted by CSM Mabee to FERC on September 3, 2019 and I believe that both his comments and his Alternate Proposal are sufficiently thorough and warranted

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

to achieve what is my primary interest and that of the Command Sergeant Major and the public at large: the type of true transparency that will focus corporate leadership on the security of the electric grid.

I am also familiar with the vehement opposition of industry members and industry lobbying organizations to the transparency currently proposed by FERC and NERC in the White Paper and by CSM Mabee in his Alternate Proposal. I believe that FERC and NERC must be very careful to avoid allowing this effort toward transparency to be subverted by industry and lobbying organizations claiming that the type of disclosure suggested in the Command Sergeant Major's comments and Alternate Proposal would present security risks to their assets or personnel. I believe CSM Mabee convincingly explains why this "security risk" argument is without merit and how transparency actually *increases* the security of the electric grid by helping change corporate culture. I have found that a number of notable experts in the field of cybersecurity share my conviction and his that the danger to the national security of allowing the grid's present vulnerabilities to cyber and other electromagnetic threats greatly exceeds any risks that might be imputed to the sort of transparency recommended by the Alternate Proposal.

Insights on Transparency from Renowned Cybersecurity Experts

One such cybersecurity expert is the former Chief Information Officer of the U.S. National Security Agency (NSA), George Cotter. This world-class authority filed comments[2] on this Docket on September 6, 2019 that underscore the importance of CSM Mabee's alternate proposal. He stated:

> "Unless the alternative proposed by Mike Mabee is fully accepted, the FERC/NERC White Paper, if codified in FERC Regulations, would make minimal information publicly available on CIP violations (only

[2] https://elibrary.ferc.gov/idmws/common/downloadOpen.asp?downloadfile=20190912%2D0014%2833795044%29%2Epdf&folder=16845269&fileid=15355490&trial=1

> Utility Name, CIP Standard but not 'Requirements", Penalty Amount) while formalizing and significantly extending NERC and FERC actions of the past nine years in denying the public ***and other Federal Authorities*** all other details of violations."

On the predictable opposition from the utilities about "security risks," Mr. Cotter wrote, "From a security perspective, more denial of violations will be counter-productive." He expanded this thought with a statement that demonstrates that he, too, is deeply concerned that the FERC/NERC White Paper is not intended to promote genuine transparency:

> "There are no security benefits that will accrue to the BPS by further denial of access to violations of CIP Standards. NERC E-ISAC is aware of this entire threat evolution. *NERC should be held criminally liable should these capabilities ever be used against this nation.* Instead, NERC jointly sponsors this industry-biased White Paper thinly disguised as protective of the BPS, in reality intended to further insulate utilities from liability lawsuits, state PUCs, CIP compliance actions, and, of course, other Federal examination." (Emphasis added.)

Another internationally renowned cyber security expert, Joseph M. Weiss, also commented on this Docket September 20, 2019.[3] While he acknowledged two concerns: 1) "the [possibility of] disclosure of entity names and CIP standards being violated, and an adversary correlating this database with the DOE OE-417 reports and ICS-CERT reports" and 2) "that utilities will begin to share *less* information on cyber incidents for fear of being 'named and shamed,'" Mr. Weiss concluded that these concerns were outweighed by the overall costs of *not* mandating transparency. As he put it:

[3] https://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=15361912

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

> "In sum, I see the need for a significant increase in the type of transparency required to change corporate culture. In the last decade, withholding the names of the CIP violators has not thwarted state actors and criminals from their cyberattacks. Since industry culture is part of the problem, more transparency in future Notices of Penalty (NOPs) must be part of the solution."

Furthermore, on September 18, 2019, David Jonas Bardin filed comments "on relation of this Docket to two cultures: 'compliance' and 'best practices.'"[4] Mr. Bardin keenly observed another element of transparency pertaining to the FERC/NERC current practice of obscuring the identifies of CIP violators – whether or not those entities have been following the guidance of the Securities Exchange Commission (SEC) to "disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences."

Indeed, according to SEC's Statement and Guidance on Public Company Cybersecurity Disclosures on February 26, 2018[5], the SEC "believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack." Due to the fact that FERC/NERC have been hiding the identities of CIP violators, I find it highly doubtful that those who have invested in the electric utility industry are aware of the cybersecurity (or physical security) risks associated with CIP violations on the part of those public companies in which they have invested.

[4] https://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=15358420
[5] https://www.sec.gov/rules/interp/2018/33-10459.pdf

This underscores yet another dimension of this need for transparency and yet another reason why the industry might vigorously oppose transparency in relation to Notices of Penalty for CIP violations: public disclosure would force corporate leadership in offending companies to have to decide whether or not their offense was a material risk to investors and whether or not they must disclose that risk if such disclosure had not already taken place. Such transparency-induced accountability will assuredly effect the sort of changes in the electric industry's corporate culture required to achieve, at last, needed upgrades in infrastructure security.

To its credit, the FERC has invited comments on this White Paper that go beyond the narrow question of transparency. Notably, in her August 27, 2019 "Statement on FERC/NERC Staff White Paper on CIP Standards Notices of Penalties,"[6] FERC Commissioner Cheryl A. LaFleur welcomed "any suggestions for alternative processes which will allow FERC and NERC to move forward on this issue." In response to this request, I would strongly recommend – in addition to moving toward transparency for CIP violators as recommended by CSM Mabee's Alternate Proposal – that a thorough examination should take place surrounding whether NERC CIP is an effective regime in the first place.

Insights on the Insufficiency of NERC CIPs

A case in point is the related problem with transparency concerning the grid's physical security. In recent writings on his website, Command Sergeant Major Michael Mabee has pointed out the deficiencies of NERC CIPs in relation to the resilience of the electric grid's infrastructure to sabotage. In an article entitled, "Physical Security: The Electric Grid's Dirty Little Secret"[7] (posted on April 25, 2019), CSM Mabee lays out the deficiencies with CIP-014-2 ("Physical Security") and the seeming, utter failure to enforce CIP-014-2. And his article entitled

[6] https://elibrary.ferc.gov/idmws/common/downloadOpen.asp?downloadfile=20190827%2D4001%2833760378%29%2Epdf&folder=16765903&fileid=15335449&trial=1

[7] https://michaelmabee.info/physical-security-dirty-little-secret/

'Electric Disturbance Events: What is the Public Allowed to Know?"[8] (posted on August 5, 2019) explores thoroughly the evident, massive gap between what the electric power industry reports to the Department of Energy through the OE-417 reports and the number of entities that have been cited for violating CIP-014-2. For example, the Command Sergeant Major's research shows that, since January 1, 2010, there have been 578 physical attacks on the grid reported to DOE by the industry. Yet, during the period of time following perhaps the most well-known – and potentially most catastrophic example – of *physical* sabotage of the grid (i.e., the April 16, 2013 attack on a major PG&E transformer substation in Metcalf California), NERC has cited violations of standard CIP-014-2 only *four* times.

While these articles are written for CSM Mabee's online blog and, hence have a somewhat informal style, the extensive research and rigorous analysis presented by these two articles are of such value in documenting the lack of transparency and the apparently attendant lack of focus on physical security in the NERC CIP regime that I have attached a copy of each to these comments. (See "Exhibit A" and "Exhibit B.")

CSM Mabee's research also suggests that, during the same period, the industry has not been transparent to the public about its lack of physical security. For example, in an article titled "Metcalf Attack: NBC Reports on PG&E Security Memo"[9] posted on April 5, 2016, CSM Mabee points out:

> "An internal Pacific Gas & Electric Corporation memo obtained by NBC Bay Area shows the company is years away from promised security upgrades at its electrical substations.
>
> The company made promises to bolster security at critical facilities after a dramatic automatic-weapons attack on its Metcalf substation in South San Jose more than two years ago. Since then, the company claimed that it has increased security at key substations and that more changes are coming soon. The director of corporate security said publicly that PG&E has "high level security" at critical facilities.
>
> This new information casts doubt on those prior statements and raises concerns about the company's ability to provide security for the California electrical grid. The memo was provided to the Investigative Unit by PG&E insiders who wanted this information out.
>
> Last August, Stephanie Douglas, the director of the Corporate Security Division (CSD), wrote to PG&E president Chris Johns that "the physical security infrastructure of PG&E has plenty of work to be done."
>
> "In reality," she wrote, "PG&E is years away from a healthy and robust physical security posture."
>
> Just 12 days before that, Douglas told the Investigative Unit a very different story.
>
> "For our critical facilities right now we have high level security there—yes," she said.
>
> In April 2013, snipers attacked the Metcalf substation in South San Jose. The attack caused millions in damages and could have blacked out much of Silicon Valley."

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

Cybersecurity experts too are troubled by the ineffectiveness of NERC CIP. George Cotter's September 6th comments stated the following about CIP:

> "The electric grid, generation, distribution and nuclear utilities, have been subject to deep technical reconnaissance since at least 2008 by the Russian Federation, including direct unexplained coupling of those incursions since at least 2014, to attacks on the US Election System. CIP Standards have been ineffective in preventing, or even revealing, those incursions."

> "Over 90% of BPS sub-stations have been excluded by utilities from categorization for CIP cyber assets. Many in large utilities (e.g., TVA) function simultaneously in Distribution networks or otherwise are the principal linkage to Distribution assets, including those supporting National Security facilities. To its discredit, NERC fought off a FERC proposal to consider National Security dependencies in CIP 14-02."

> "An industry that greatly fears federal and state regulation is being regulated to near absurdity by a increasingly costly CIP program that fails to protect them from foreign adversary states."

George Cotter's filing also included his July 10, 2018 White Paper titled "Security in the North American Grid – The Existential Threat" which summarized the history of the development of CIP Standards and provided numerous specific observations of the shortcomings of CIP from the cybersecurity perspective, perhaps most succinctly in this excerpt:

> ***Comment:*** CIP Standards are hardly more than a "feel-good" placebo for regulators and other overseers. CIP Standards are simply ignored in the hundreds of media reports on Grid attacks; in the technical feedback from security firms and the NCCIC/US CERT alerts and advisories. CIP Standards have had no value in protecting the Grid from foreign adversaries; they certainly have been no impediment to the SVR or GRU since they turned to the Grid as a major malware target in 2012. The major reasons the Grid has been an easy Russian target are (1) how few cyber assets are covered under CIP Standards, (2) the exclusion of communications and network linkages despite extensive Internet connectivity by utilities, (3), the absence of hard technical requirements in standards, and (4) the extremely weak compliance system in use.

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

In fact, the "Appendix II" of Mr. Cotter's White Paper [titled "Critical Infrastructure Protection (CIP) Standards"] is so comprehensive and the scanned version currently available on the FERC docket is of such poor visual quality, that I have attached a higher-resolution version of that document to this filing as "Exhibit C."

Transitioning from NERC CIPs to NIST SP 800-53 for Cybersecurity

One of George Cotter's most important insights in his White Paper concerns the difference between NERC CIP and another alternative: the National Institute of Standards and Technology (NIST) cybersecurity standards. For example, he made the following observation:

> "Between 2005 and 2008, there were substantial discussions between FERC and NERC and tangentially, with congressional staffs on the intent of the EPA [Energy Power Act]. Congressional staffs urged the industry and FERC to adopt NIST standards, then applicable to Federal agencies."

> "CIP Standards are, by design, a pro forma, high level set of security objectives intended to influence, not proscribe, selection of cyber protection systems by utilities. Unlike the extremely detailed standards in NIST SP 800-53, preferred by Congress in passage of the EPA of 2005, NERC CIP Standards have not served as an acquisition technical check-list for utilities. Compliance reviews are therefore hardly much more than very subjective, tabletop assessments, so general in fact, that little or no commercial support activity for CIPs has been fielded by major security technology firms. And CIP is barely mentioned by major IT suppliers."

George Cotter is not the only internationally renowned cybersecurity expert to argue that the NERC CIPs are insufficient and that they should be replaced by NIST. Joseph Weiss' filed comments on this docket outlined seven shortcomings of NERC CIP:

> - There have been utilities who have been fined for doing MORE than what the NERC CIPs require;
> - NERC CIPs require disclosure only on "critical assets;"
> - NERC CIP auditors have an incentive to find problems but generally do not understand the implications to the reliability of the electric grid;
> - Many NERC CIP violations are "paper" issues that have nothing to do with the actual protection of electric grid assets;
> - The most important devices for the reliability of the electric grid are not even in scope for the NERC CIP and Supply Chain such as process sensors, actuators, drives, as well as serial communications, etc.;
> - Known security issues such as connecting SCADA and control systems directly to the Internet are allowed so this real violation that is not even considered a violation; and
> - NERC CIP002 is the requirement for defining critical assets and violations of this are what NERC references as the"$1 million per day fine", but since the establishment of NERC CIP, there haven't been any violations of this requirement cited by NERC.

In relation to the topic of NIST, Mr. Joseph Weiss' comments closely mirrored those of George Cotter:

> NERC CIP needs to be replaced by NIST SP800-53. It is already mandatory for the federal utilities such as the Tennessee Valley Authority (TVA), Bonneville Power Administration (BPA), and the Western Area Power Administration (WAPA). NIST SP800-53 does not allow the utilities to a priori ignore any system or device. No other industry or organization gets to decide what to address and what to ignore without even looking. There is a problem when a Human Resources organization in a small retail organization is held to a higher cyber security approach than the most important electric systems in this country. NIST SP800-53 requires an assessment as to whether the system or device is low, medium, or high priority. This is the only way to have confidence that subtle threats that can cascade to bigger ones and unintended consequences are addressed.

Similarly, on September 26, 2019, the U.S. Government Accountability Office (GAO) published a report titled "Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid."[10] In this document, the GAO explained:

> "The Federal Energy Regulatory Commission (FERC)—the regulator for the interstate transmission of electricity—has approved mandatory grid cybersecurity standards. However, it has not ensured that those standards fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework. (See table below for an excerpt of GAO's analysis of two of the five framework functions.) Without a full consideration of the framework, there is increased risk that grid entities will not fully implement leading cybersecurity practices." [table omitted]

[10] https://www.gao.gov/mobile/products/GAO-19-332

The GAO continued with the following recommendations to FERC:

> 1. Consider adopting changes to its approved cybersecurity standards to more fully address the NIST Cybersecurity Framework.
>
> 2. Evaluate the potential risk of a coordinated cyberattack on geographically distributed targets and, based on the results of that evaluation, determine if changes are needed in the threshold for mandatory compliance with requirements in the full set of cybersecurity standards.

Given the knowledge, credibility, and reputation of Mr. Weiss and Mr. Cotter and the considerable weight of the GAO's analysis and recommendations, I believe FERC should initiate a rapid transition process to replace NERC CIP with NIST SP800-53.

Additional Recommendations for All Hazards Critical Infrastructure Protection

I believe that FERC should consider additional suggestions made by cybersecurity experts in their comments on this docket. For example, I concur with Joseph Weiss' recommendation that a **Cyber Incident Playbook** be developed to help with control system incident investigations. I also concur with George Cotter's "**minimum steps to protect National Security facilities and start the CIP transition**" which I have reproduced here since their importance cannot be overstated:

> - Isolate and repair the vulnerabilities of the nine Centers that effectively control power flows in the Grid. Identify potential "Islanding" linked to loss of each. Upgrade and harden the Reliability Entities that manage Grid operations.
> - Link their associated critical nodes in a secure, multi-level Indications and Warning network into National Intelligence Centers/Cyber Command operations.
> - Power feeds to Critical National Security and Nuclear Facilities dependent on commercial power must be isolated and protected. States hosting such facilities must stand up, train and exercise selected National Guard/Military Reserve units as "First Responders" to Grid incursions.
> - Derive new top-level Critical Infrastructure Protection standards (consistent with NIST standards) from lessons-learned from the foregoing."

In addition to these urgent cybersecurity actions suggested by Mr. Cotter, I suggest that FERC address physical and electromagnetic spectrum vulnerabilities (such as high altitude electromagnetic pulse – HEMP and

intentional electromagnetic interference – IEMI) at the "nine Centers" and for the power feeds to Critical National Security and Nuclear Facilities he mentions. Two consecutive studies[11] [12] of the U.S. Air Force's Electromagnetic Defense Task Force (EDTF) point out that if there were anywhere in this nation besides our nuclear deterrent assets where Mil-Spec EMP protection should be most rapidly applied, it would be at and in support of the nuclear power generation sites (i.e., the "feeds" mentioned by Mr. Cotter.) The same can be said of these "nine Centers."

Given the value of the USAF EDTF's contribution to the national discourse on critical infrastructure protection from electromagnetic spectrum threats, FERC should assume that it can draw from experts within DoD to address other threats, such as physical sabotage. Since the Department of Defense is completely reliant on the same electric infrastructure as the rest of the population, FERC should invite DoD to assemble a group of subject matter experts (SMEs) to help create both a "red team" concept for FERC to be able to "inspect" what it "expects" of NERC in physical infrastructure compliance enforcement and also to brainstorm methods by which DoD installations can be sufficiently informed of the need for their commanders and contracting personnel to closely collaborate with the utilities upon which they depend in matters pertaining to security.

For example, if military commanders (active, guard and reserve) sufficiently appreciated the vulnerabilities of the electric infrastructure supporting their installations and were invited "to the table" to collaborate, they could begin the process of establishing the type of civil/military relationships that will be necessary for our nation to adequately defend its critical infrastructure from physical attack and possibly other vectors such as cyberattack and electromagnetic attack. As part of this initiative, FERC should prioritize its overhaul of the

[11] https://media.defense.gov/2018/Nov/28/2002067172/-1/-1/0/LP_0002_DEMAIO_ELECTROMAGNETIC_DEFENSE_TASK_FORCE.PDF

[12] https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/LP_0004_ELECTROMAGNETIC_DEFENSE_TASK_FORCE_2_2019.PDF

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

critical infrastructure protection regime with an all-hazards-focused crash program focused FIRST and FOREMOST on hardening these "nine Centers" and "the power feeds to Critical National Security and Nuclear Facilities."

Conclusion

I believe that this docket is among the most important of any that FERC has initiated in its history. I know that many of the comments made by security experts on this docket have been informed by decades worth of experience and reflect the authors' dedication to the protection of our nation's most critical infrastructure.

I also believe that many comments made on this docket will expose for the American people the reality that the owners and operators of this most critical infrastructure have been, by and large, "off the hook" for adequately protecting it from cyberattacks and physical attacks because of an insufficient protection regime developed and operated by NERC – one that, in practice, has provided "top cover" for the industry to cultivate and maintain a corporate culture apathetic about security.

I am grateful that Commissioner LeFleur invited "any suggestions for alternative processes," creating an opportunity for this discussion to both include and transcend the matter of transparency. I believe that if FERC were to adopt Command Sergeant Major Michael Mabee's "Alternate Proposal," it would greatly enhance the transparency that is so profoundly needed and make an instant and immeasurable impact on the corporate culture of the electric power industry.

In my professional judgment, this docket and the comments it has engendered offer an ample basis for FERC to go beyond simply adopting Mr. Mabee's "Alternate Proposal." I strongly suggest that FERC adopt the additional

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

proposals made by other experts such as Mr. Cotter and Mr. Weiss, combined with my own suggestions above to achieve a redesign of the protection regime enabling it to address *all* hazards.

No other entity in the Federal Government wields the power and authority of Federal Energy Regulatory Commission when it comes to requiring the protection of our nation's most critical infrastructure. I pray that the FERC Commissioners and staff will translate this responsibility into action in light of the present and growing threats to our electric grid and, by so doing, provide proof that they truly serve the *public* interest, rather than the special interest of the electric power industry.

Sincerely,

Frank J. Gaffney
Executive Chairman
Center for Security Policy

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

Exhibit A

Physical Security: The Electric Grid's Dirty Little Secret

Posted on April 25, 2019 by Michael Mabee

Physical security requirements for the electric grid—and their enforcement—are largely non-existent 6 years after the Metcalf attack

At approximately 1:00 a.m. on April 16, 2013, a major PG&E transformer substation in Metcalf California was attacked. The attack was well-planned and sophisticated. One year later, the Metcalf station was struck again when the fence was cut open and, the facility entered and tools were stolen.

Protected by a chain-link fence and crossed fingers…

Obviously, the physical security situation had not improved much in the intervening year. In fact, PG&E's credibility was shot when its public statements about its physical security improvements were contradicted by a leaked internal memo.

The April 2013 Metcalf attack was not the only physical attack on critical components of the North American electric grid:

- On June 11, 2014 there was an attack by Improvised Explosive Device (IED) on the Nogales Station in Arizona.
- On December 4, 2014, Hydro-Québec suffered a power outage (and narrowly avoided a province-wide blackout) when a pilot attacked the grid by airplane interrupting the flow of electricity to the United States.
- On September 25, 2016 there was a rifle attack on the Buckskin Substation in Utah.

However, the attack on the Metcalf substation—and the other attacks—shouldn't have been a surprise. A year before the Metcalf attack, the National Academies published a report titled: *Terrorism and the Electric Power Delivery System*. The report discussed physical security of high-voltage transformers noting:

> High-voltage transformers are of particular concern because they are vulnerable to attack, both from within and from outside the substation where they are located. These transformers are very large, difficult to move, custom-built, and difficult to replace. Most are no longer made in the United States, and the delivery time for new ones can run to months or years.

Then, one year after the Metcalf attack, the Wall Street Journal ran two alarming stories:

> Assault on California Power Station Raises Alarm on Potential for Terrorism. *April Sniper Attack Knocked Out Substation, Raises Concern for Country's Power Grid*
>
> *Smith, Rebecca. Wall Street Journal. February 5, 2014*

> U.S. Risks National Blackout From Small-Scale Attack. *Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage*
>
> *Smith, Rebecca. Wall Street Journal. March 12, 2014*

Huge physical security vulnerabilities were identified—so what was done?

(Spoiler Alert: The answer is "Goose Egg")

One would think that action would be taken. At first, a lot of paper flew. After the February 5, 2014 Wall Street Journal article, the Senate sent a letter on February 7, 2014 to the Federal Energy Regulatory Commission (FERC), to ask them what they were doing to protect the grid. And FERC Responded telling the Senate that:

> "Since the attack on the Metcalf facility in April 2013, the Commission's staff has taken responsive action together with NERC, other federal and state agencies, and transmission and generation asset owners and operators."

So we are okay. right? Action has been taken?

Nope.

The physical security of our critical transformers and facilities remains a complete mess in 2019.

Problem #1: The standard—CIP-014-2 (Physical Security)—is a joke.

Protected by a chain-link fence and crossed fingers…

As a result of Metcalf, FERC ordered NERC to develop a physical security standard. Yes, that's right—the industry is self-regulated and writes their own standards. NERC submitted their proposed standard (known as CIP-014-1) on May 23, 2014.

FERC issued an order on November 20, 2014 literally ordering NERC to change one word. (The word was: "widespread" and was used 30 times in the proposed standard. This word—a slight of pen by NERC's attorneys—would have excluded many facilities from falling under the standard.)

On October 2, 2015, FERC approved the "Physical Security" standard, known as CIP-014-2. What does the physical security standard require? Well, it requires very little:

1. Requirement 1: Each Transmission Owner shall perform a risk assessments of its Transmission stations and Transmission substations.
2. Requirement 2: Each Transmission Owner shall have an unaffiliated third party verify the risk assessment *[e.g., a peer grid company would meet the requirement—"Hey, I'll show you mine if you show me yours"].*
3. Requirement 3: If a Transmission Owner operationally controls an identified Transmission station or Transmission substation, it must notify the Transmission Operator that has operational control of the primary control center.
4. Requirement 4: Each Transmission Owner shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s).
5. Requirement 5: Each Transmission Owner shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s).
6. Requirement 6: Each Transmission Owner shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s)

under Requirement R5 *[e.g., a peer grid company would meet the requirement—"Hey, I'll show you mine if you show me yours"].*

That's it. All you have to do is have a binder with a bunch of papers labeled "Physical Security Plan" and have anybody you choose review your "risk assessment," "evaluation" and "security plan(s)". No need for it to be anybody who knows anything about physical security.

And there is no requirement as to what the "Physical Security Plan" must include—or even that it be effective. Nobody with regulatory authority even has to even approve it—All you need is somebody to "review" it. What if the "reviewer" happens to say "this plan sucks?" It doesn't matter. The only requirement is that the three ring-binder be "reviewed." Check! I guess most any papers in a three-ring binder will do!

That unapproved three-ring binder of papers is what is standing between your family and a widespread power outage caused by a terrorist attack.

Oh, did you notice that generation plants (that's where electricity is made) are not included in NERC's physical security standard? Commissioner Cheryl LaFleur even testified before Congress that an attack on a single generation plant can cause a cascading outage.

Moreover, in her May 20, 2014 re-nomination hearing, Congress asked Commissioner LaFleur: "will the physical security standard recently passed by NERC adequately protect the public from electric grid outage caused by terrorist attack?" Her written answer:

> NERC's petition to approve the physical security standard was filed with the Commission for review on May 23, 2014. It would be inappropriate for me to judge the merits before interested parties have an opportunity to submit comments to the Commission, so that we can consider all relevant arguments. I assure you that I will carefully consider the proposal and all filed comments to ensure that NERC's filing does adequately protect the public.

A bureaucratic non-answer. Now after almost 9 years of Commissioner LaFleur's "leadership"—and six years after the Metcalf attack—the public is not "adequately" protected.

(But let us not get "into the weeds" on physical security, as this can be truly upsetting, especially for those dependent on reliable electricity—intensive care patients in

hospitals, those dependent on kidney dialysis, diabetics needing insulin refrigeration, etc. FERC has told us "responsive action" has been taken and that's all we need to know.)

Problem #2: Enforcement of CIP-014-2 seems nonexistent

Okay. Even if the physical security standard is bull shit, it is better than nothing right? If all of the companies at least are doing this, it makes us a little safer, right? As long as NERC is enforcing this standard, we are at least a little safer, right?

NERC must be all over this in its audits of the utilities, right?

So, how many times since Metcalf have utilities been cited for violations of standard CIP-014-2?

Four.

That's right. I'm not golfing. I mean "four" as in the numeral. We have had several physical attacks (that the public knows about) yet, the standard has only been cited four (4) times in the six (6) years since the Metcalf attack. What does that mean?

It means one of three things:

1. Either the electric utility industry totally got its "sierra" together after Metcalf and all of our transformers are secure and NERC can find no violations. (Note: That would also require that they are actually assessing *the effectiveness* of the plans, which the standard does not require but this would assume that NERC and all 1,500 regulated entities are going way above and beyond the call of the standard that they wrote.)
2. Or all the companies have a three-ringed binder marked "Physical Security Plan."
3. Or NERC and the Regional Entities are pulling a "Sergeant Schultz" and just not looking. ("I see nothing…I know nothing!")

NERC and the Regional Entities on a CIP Audit?

Unless what is actually happening is #1 – then this standard and regulatory scheme are not working. Here are the facts.

- There are 1,500 entities regulated by NERC.
- There are likely over 2000 EHV LPTs (Extra High Voltage Large Power Transformers) in the United States and tens of thousands of LPTs.
- There have been 4 citations for non-compliance with the BS physical security "standards" since Metcalf.
- The American people are not stupid. We see these transformers unguarded behind the chain-link fence as we drive up the road or walk our dogs.

So how seriously does NERC take physical security? Not very judging by their lack of effort to update their website.

Click for Larger View

Here is a screenshot of NERC's website on "Physical Security" taken on April 20, 2019. It is talking about CIP-014-1. This standard has been outdated since October 2, 2015.

NERC's physical security website has not been updated in 3 and 1/2 years. What

does that tell us? I guess #1 was a long shot anyway.

So let's take a look at the 4 times NERC found CIP-014-2 violations:

- In NP19-4-000 (one Violation—which everybody knows is Duke Energy Corp.), Duke apparently excluded one substation from its risk assessment because they didn't think it met the criteria for inclusion.
- In NP18-14-000 (one violation), the "Unidentified Registered Entity" failed to do a risk assessment on one substation due to a "management oopsy."
- And in NP17-29-000 (two violations), the "Unidentified Registered Entity" failed to include one control center in it's 1) risk assessment and 2) security plan (two violations) because an employee who knew what they were doing left the company, leaving nobody else who knew what they were doing.

You will notice that all 4 of these "violations" are administrative in nature and have nothing to do with whether there is actually meaningful physical security in place.

That's it for NERC Physical Security enforcement since Metcalf!

A more detailed history of "Physical Security" standards

At the risk of getting a bit geeky, a recitation of the history of the physical security and sabotage reporting standards is instructive.

CIP-001-1 (Sabotage Reporting) became effective on June 4, 2007. It was cited 404 times between 6/4/2008 and 5/26/2011. It them morphed into CIP-001-1a (February 2, 2011) and CIP-001-2a (August 2, 2011)—neither of which were EVER cited.

Meanwhile, EOP-004-1 (Disturbance Reporting), which covered "equipment damage" among other things, was cited 16 times between 2009 and 2013.

NERC began to look at merging CIP-001 and EOP-004 "to eliminate redundancies" and on June 20, 2013, FERC approved merging CIP-001-2a (Sabotage Reporting) and EOP-004-1 (Disturbance Reporting) into EOP-004-2 (Event Reporting). (CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting were then "Retired.") EOP-004-2 covers reporting "damage or destruction of a facility." EOP-004-2 and its successors have never been cited.

So here is the enforcement history of these various standards:

- 404 Citations issued for CIP-001-1 (Sabotage Reporting) between 2008 and 2011

- 16 Citations were issued for EOP-004-1 (Disturbance Reporting) between 2009 and 2013—not all related to damage.

Metcalf happened on April 16, 2013, but then…

- No citations have been issued for EOP-004-2 (effective June 20, 2013)
- No citations have been issued for EOP-004-3 (effective November 19, 2015)
- No citations have been issued for EOP-004-4 (effective January 18, 2018)

And adding in the CIP-014 physical security Standard:

- No citations have been issued for CIP-014-1
- 4 citations have been issued for CIP-014-2
  - NP19-4-000 (one Violation)
  - NP18-14-000 (one violation)
  - NP17-29-000 (two violations)

There are Solutions

The Department of Energy as well as many commercial companies offer various solutions to defeat ballistic, explosive and electromagnetic threats. Here are just a few, These are not endorsements, simply evidence that physical security solutions exist:

- Idaho National Laboratory – Armor The Grid
- Metalex – How to Protect the Grid with Stronger Security Fencing
- Siemens – Bullet Resistant Power Transformers
- BTI – Ballistics Transformer Protection
- ArmorCore – Used For Securing Nation's Grid
- Durasystems – Barriers
- Southern States LLC – Physically Securing Substations

The military has been doing physical security of critical facilities longer than anybody. Since the military is dependent on the civilian electric grid, DoD has a dog in the fight and expertise but no actual authority to do anything. Similarly, DHS and DOE have expertise and resources—and also have a stake in grid security—but no direct authority. (Although DOE does have authority in an emergency under the FAST Act—and arguably this is an emergency.) FERC is the key player here.

I wonder what we would find if FERC got a physical security "Red Team" together? What if FERC hired some retired Army Green Berets, Navy SEALs and Marine Raiders to check these three-ring binders?

Conclusion

Physical security for the electric grid still appears largely non-existent 6 years after Metcalf attack. The standard is weak and the enforcement seems absent.

There is little public evidence that anything substantial has been done since Metcalf to secure our critical transformers and control centers. The standard doesn't require anything other than a peer-reviewed risk assessment, evaluation and a three-ring binder labeled "Physical Security Plan" (which needs not be approved by anyone who knows what they are doing—just "reviewed" by somebody the utility chooses).

The first step is that FERC needs to coordinate with DoD, DOE and DHS to "Red Team" the electric utilities on physical security. (The same "Red Team" concept would work for cybersecurity, EMP and GMD hardening as well.) We should help the willing to fix themselves and we should "Black Hat" regulate the repeat CIP standard violators. NERC should not be involved. This needs to be a government verification that the industry's self-regulation of a critical infrastructure is working.

Anything less than immediate action by FERC to evaluate the physical security of the electric grid—Including NERC's "regulation" of the standard—is unacceptable.

###

References:

Senate Metcalf Letter Dated February 7, 2014, Regarding Physical Attack on Metcalf Substation

- Click for PDF copy of February 7, 2014 letter from Senate to FERC
- Click for PDF copy of February 11, 2014 letter from FERC to Senate
- Click for February 12, 2014 Statement of Acting Chairman Cheryl A. LaFleur

Metcalf Substation Attack, California (4/16/2013)

- **Assault on California Power Station Raises Alarm on Potential for Terrorism**
- **VIDEO: Metcalf Sniper Attack – Wall Street Journal**
- **Metcalf Attack: NBC Reports on PG&E Security Memo**
- **Snipers Coordinated an Attack on the Power Grid, but Why?**
- **Sophisticated but low-tech power grid attack baffles authorities**

- Sniper attack on California power grid may have been 'an insider,' DHS says

Hydro-Québec Grid Attack (12/4/2014)

- Pilot to be sentenced in sabotage that crippled Quebec power grid
- Pilot gets 7 years in prison for attacking Hydro-Québec network
- 'Pilot to the stars' nearly crippled entire Hydro-Québec network

Noglaes Station Attack (6/11/2014)

- Arizona substation attacked with bomb
- Sabotage at Nogales station puts focus on threats to grid
- Concern widens over sabotage at Nogales power station

Buckskin Substation Attack, Utah (9/5/2015)

- Power company offers rare $50K reward for information on vandalism
- Substation attack is new evidence of grid vulnerability
- Sniper attack on Utah substation highlights grid vulnerability

Please help support Michael Mabee's public interest research and grid protection work. Thanks!

NEWS

Duke Redux – A Repeat Cybersecurity Violator Exposed!

UPDATED: CIP Violation Database and FOIAs

FERC White Paper: An Alternate Proposal Submitted

Duke Energy Notice of Penalty Docket Shut Down!

EDTF Discredits False EPRI EMP Report

Exhibit B

Michael Mabee

Author of The Civil Defense Book™

Electric Disturbance Events: What is the public allowed to know?

Posted on August 5, 2019 by Michael Mabee

Electric Disturbance Events are reported to the Department of Energy, but huge gaps exist in the publicly available information

Utility companies and grid operators are required to submit reports on electric disturbance events to the Department of Energy (DOE). The publicly available information from these reports is incomplete and confusing when compared to reports submitted by the North American Electric Reliability Corporation (NERC). These discrepancies must be fixed.

First, a brief primer on the "Form OE-417" and electric disturbance reporting.

In 1974, Congress passed the Federal Energy Administration Act which created a new government agency to oversee energy in response to the oil embargo of 1973. A few years later, the Federal Energy Administration became the Department of Energy (DOE). One of the many things that DOE does is collect information on "electric disturbance events." DOE collects this information on what is known as a Form OE-417 ("Electric Emergency Incident and Disturbance Report"). Only a small amount of this information is available to the public and is difficult to find and even more difficult to read and analyze.

What does this information look like? The publicly available information on electric disturbance events is in the form of a spreadsheet which is neither user friendly nor frequently updated. As of August 4, 2019 data was only available through the end of May.

Here is an example of what it looks like to us. On May 27, 2019 tornadoes and thunderstorms hit the Dayton Ohio area causing destruction and over 68,000 customers lost power. Here is what the publicly available OE-417 entry looks like:

Data	Date Event Began	Time Event Began	Date of Restoration	Time of Restoration	Area Affected	NERC Region	Alert Criteria	Event Type	Demand Loss (MW)	Number of Customers Affected
May	5/27/2019	10:07 PM	05/28/2019	3:00 AM	Ohio: Montgomery County, Darke County, Mercer County, Miami County, Greene County;	RF	Loss of electric service to more than 50,000 customers for 1 hour or more.	Severe Weather/Transmission Interruption	347	70000

Click for Larger View

DOE keeps archives of these spreadsheets on their website back to 2000. The form has changed a bit over the years and has changed names from the EIA-417 to the present OE-417.

Here's another example. Remember the Great Northeast Blackout of 2003? It was a cascading failure that began with untrimmed foliage in Ohio, add in some computer error, a touch of human error and the result is 55 million people without power – 45 million in the U.S. and 10 million in Canada. Here is what the OE-417 entries look like:

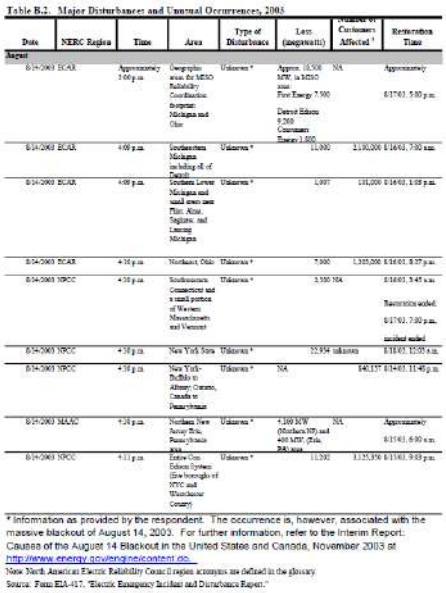


Table B.2. Major Disturbances and Unusual Occurrences, 2003

Date	NERC Region	Time	Area	Type of Disturbance	Loss (megawatts)	Number of Customers Affected *	Restoration Time
August							
8/14/2003 ECAR		Approximately 3:00 p.m.	Geographic area for MISO Reliability Coordination footprint: Michigan and Ohio	Unknown *	Approx. 18,500 MW, in MISO area: FirstEnergy 7,500 Detroit Edison 6,500 Consumers Energy 1,800	NA	Approximately 8/17/03, 5:00 p.m.
8/14/2003 ECAR		4:05 p.m.	Southeastern Michigan including all of Detroit	Unknown *	11,000	2,100,000	8/16/03, 7:00 a.m.
8/14/2003 ECAR		4:08 p.m.	Northern Lower Michigan and small area near Flint, Alma, Saginaw, and Lansing, Michigan	Unknown *	1,997	191,000	8/16/03, 1:05 p.m.
8/14/2003 ECAR		4:10 p.m.	Northeast, Ohio	Unknown *	7,000	1,203,000	8/16/03, 8:37 p.m.
8/14/2003 NPCC		4:10 p.m.	Southwestern Connecticut and a small portion of Western Massachusetts and Vermont	Unknown *	2,500 MA		8/16/03, 5:45 a.m. Restoration ended 8/17/03, 7:00 p.m. incident ended
8/14/2003 NPCC		4:10 p.m.	New York State	Unknown *	22,914 unknown		8/18/03, 12:00 a.m.
8/14/2003 NPCC		4:10 p.m.	New York-Ontario to Albany, Ontario, Canada to Pennsylvania	Unknown *	NA		8/17/03, 11:40 p.m.
8/14/2003 MAAC		4:24 p.m.	Northern New Jersey, Erie, Pennsylvania area	Unknown *	4,100 MW (Northern NY) and 400 MW (Erie, PA) area	NA	Approximately 8/17/03, 6:00 a.m.
8/14/2003 NPCC		4:11 p.m.	Entire Con Edison System (five boroughs of NYC and Westchester County)	Unknown *	11,200	3,135,950	8/13/03, 9:53 p.m.

* Information as provided by the respondent. The occurrence is, however, associated with the massive blackout of August 14, 2003. For further information, refer to the Interim Report: Causes of the August 14 Blackout in the United States and Canada, November 2003 at http://www.energy.gov/engineiccontent.cfm.

New North American Electric Reliability Council region acronyms are defined in the glossary.

Source: Form EIA-417, "Electric Emergency Incident and Disturbance Report."

Click for Larger View

In this case. there were multiple reporting entities involved and so there are multiple reports. It is interesting that the "Number of Customers Affected" in these reports comes nowhere near the 55 million that ultimately were without power during this extraordinary blackout.

Very few people have ever heard of the OE-417 or this reporting requirement. We have a false sense of security about the reliability of the electric grid. We also have a false sense of security that our government is on top of the threats to the electric grid.

Part of what puts us in danger is the general public's lack of knowledge of the threats and our government's lack of public information – and in fact their coverup of critical information that the public needs. If the public really knew what was going on, there would be an outcry to fix the broken regulatory scheme that endangers the electric grid and all of our lives.

But I digress. Let's get back to the exciting world of the OE-417 and how electric disturbance events are reported.

What electric disturbance events must be reported?

Depending on the type of event (or "alert criteria"), there are three different time requirements for reporting:

1. An "Emergency Alert" must be reported within 1 hour
2. A "Normal Report" must be filed within 6 hours
3. A "System Report" must be filed within one business day.

In addition, updates are required if there are significant changes to the initial report and a final report must be filed within 72 hours. There are 24 alert criteria listed on the Form

OE-417 and the instructions. (8 for an "Emergency Alert"; 4 for a "Normal Report" and 12 for a "System Report.")

For example, here is how cyber attacks would be reported:

- A "cyber event that causes interruptions of electrical system operations" would have to be reported within 1 hour.
- A "cyber event that could potentially impact electric power system adequacy or reliability" would have to be reported in 6 hours.

For physical attacks:

- A "physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations" would have to be reported in 1 hour.
- A "physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems" would have to be reported in 6 hours.
- A physical attack resulting in "damage or destruction of its Facility that results from actual or suspected intentional human action" would have to be reported within 1 business day.

What do the OE-417's tell us about threats to the grid?

I did an analysis of all the publicly available OE-417 data from 2010 through May of 2019. (I started in 2010 because that is when the NERC CIP Coverup began.) First of all, there were 166 different "event types" reported many of which were either duplicates or related. For example, there were at least 24 different "event types" that denoted a physical attack. There were at least 50 "event types" that denoted a disturbance caused by weather. I grouped these 166 "event types" into 15 categories (actually "causes") so that we could get a sense of what has actually threatened the electric grid in the past 8 1/2 years.

Event	#
Weather	749
Cyber Attack	29
Physical Attack	578
Fuel Supply Deficiency	61
Equipment	15
Natural Disaster	10
Wildfire	5
Generation Interruption	16
Transmission Interruption	46
Distribution Interruption	6
Operations	80
Islanding	67
Load Shed	30
Public Appeal	64
?	10
Total Reports	**1766**
Cause Known from OE-417	**1447**

Click for Larger View

There have been a total of 1766 electric disturbance events filed during the period of January 1, 2010

through May 31, 2019.

Unfortunately, the public OE-417 data is so bad that there were 251 electric disturbance events where I was unable to identify a cause (14% of the reports). These are highlighted in yellow in the chart. Also, there were 68 generation, transmission and distribution interruptions I was not able to distill down further into what caused the "interruptions." Therefore, there were a total of 319 electric disturbance events (18%) where I couldn't identify the cause. I was able to identify a cause in 1447 electric disturbance events, or 82% of the OE-417 reports filed. (I used this 1447 known population for the study below.)

The results are disturbing to say the least.

Weather: As you might suspect, weather was the cause of the majority of the disturbances, 749 events, or 52%. If you believe that weather is getting worse in recent years, then this number should concern you greatly.

Physical Attacks: Shockingly, there were 578 physical attacks on the grid, or 40% of the incidents. As I have reported, the "physical security standards" for our electric grid are a sham and enforcement is almost non-existent. (Read: "Physical Security: The Electric Grid's Dirty Little Secret.")

Fuel Supply Deficiency: If you live in New England, pay attention. There were 61 events, or 4% of the events. related to fuel supply deficiency. With the retirement of coal and nuclear plants, this is only going to get worse. Remember: We all love solar and wind but it is not reliable (i.e., the sun doesn't shine and the wind doesn't blow 24 hours a day). You can run coal and nuclear 24/7. Just sayin'. Gas fired plants are great, but they require a pipeline. If the pipeline is attacked or explodes, oh well. Maybe Americans will decide to reduce their electricity usage? (Naw, didn't think so.) Fuel security and supply are issues we need to deal with.

Cyber Attacks: I was also surprised to learn that there have been 29 cyber attacks reported during this period (2% of the reports). What is most disturbing is that during the same period, the North American Electric Reliability Corporation (NERC) annual reliability reports seem to paint a completely different picture.

OE-417 vs. NERC Reliability Reports

Here is what NERC reported in their annual reports during this same period (note that the report each year is on the previous year, e.g., the 2019 report is for the events of the

year 2018):

- **2019 Report** (page ix): "In 2018, there were no reported cyber or physical security incidents that resulted in an unauthorized control action or loss of load."
- **2018 Report** (page viii): "In 2017, there were no reported cyber or physical security incidents that resulted in a loss of load."
- **2017 Report** (page 3): "In 2016, there were no reported cyber or physical security incidents that resulted in a loss of load." (Odd, since the Buckskin Utah transformer attack took place in 2016.)
- **2016 Report** (page v): "In 2015, there were no reported cybersecurity incidents that resulted in loss of load. There was one physical security incident that resulted in a loss of approximately 20 MW of load."
- **2015 Report** (page 7): "[N]o Reportable Cyber Security Incidents or physical security reportable events resulted in loss of load on the BPS in 2014." (Odd, since the Nogales Station in Arizona was attacked by an IED in 2014.)
- **2014 Report**: No mention of cyber or physical attacks. (Odd, since the Metcalf Transformer attack took place in 2013.)
- **2013 Report**: No mention of cyber or physical attacks.
- **2012 Report**: No mention of cyber or physical attacks.
- **2011 Report**: No mention of cyber or physical attacks.

There is clearly a huge disconnect between what the industry defines as a cybersecurity or physical security incident and what is reported on the OE-417s. Below are the OE-417 entries for the Metcalf attack (2013), the Nogales attack (2014) and the Buckskin attack (2016).

Date Event Began	Time Event Began	Date of Restoration	Time of Restoration	Area Affected	NERC Region	Alert Criteria	Event Type	Demand Loss (MW)	Number of Customers Affected
4/16/2013	1:47 AM	4/18/2013	3:25 PM	California	WECC		Loss of Part of a High Voltage Substation, Physical Attack	N/A	0
6/11/2014	9:30 AM	6/11/2014	9:31 AM	Nogales, Arizona	WECC		Suspected Physical Attack	N/A	N/A
9/25/2016	12:49 PM	9/25/2016	6:20 PM	Utah: Kane County, Garfield County; Arizona: Coconino County, Mohave County	WECC	Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems	Vandalism	20	10000

Click for Larger View

While this minimal information was reported on the OE-417, NERC did not find any of it noteworthy enough for their annual reports. These three events were significant physical attacks against the grid. (Read more HERE.)

And on cyberattacks, here's what the United States Government Accountability Office (GAO) had to say in Congressional testimony on October 21, 2015:

> "Cyber incidents continue to affect the electric industry. For example, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team noted that the number of reported cyber incidents affecting control systems of companies in the electricity subsector increased from 3 in 2009 to 25 in 2011. The response team reported that the energy sector, which includes the electricity subsector, led all others in fiscal year 2014 with 79 reported incidents. Reported incidents affecting the electricity subsector have had a variety of impacts, including hacks into smart meters to steal power, failure in control systems devices requiring power plants to be shut down, and malicious software disabling safety monitoring systems."

But NERC reported no cybersecurity incidents in their annual reliability reports for the same periods! Are you kidding me? In what possible world is this level of misinformation acceptable?

> Does it bother anybody else that NERC has completely ignored these events, while the OE-417 – a form you may never have heard of before reading this article – contains such scant information?
>
> Does it bother anybody else that there were 578 physical attacks against the grid reported on the OE-417's between 2010 and the present, yet according the NERC there was only one during the same period?
>
> Does it bother anybody else that there were 29 cyberattacks against the grid reported on the OE-417's between 2010 and the present, yet according the NERC there were none during the same period?
>
> Does it bother anybody else that DHS has a completely different number of cyber incidents than DOE, who has a completely different number than NERC?

It is clear to me that the public and Congress are not getting enough information on threats to the grid and what is reported on the OE-417s and what NERC wants us to believe are not the same.

Does the public – and Congress – have a right to know? Do we have a right to better information?

Conclusion

The American people and Congress are not getting enough information to see 1) what is going on and 2) whether the regulatory regime is effective. First. NERC is withholding the names of CIP violators (so we do not know if there are egregious or repeat violators and can't hold anybody accountable). Second, we see the flawed OE-417 information where we can't even see what the cause of 18% of the reported disturbances. Finally, we see that there is an unexplained disparity between the OE-417 reports and the NERC annual reliability reports. These deficiencies must be corrected.

I have the following recommendations for the Department of Energy (DOE):

1. Each OE-417 needs to list a root cause for each disturbance reported.
2. The "Number of Customers Affected" block on the OE-417 does not always seem accurate.
3. The OE-417s and the NERC Reliability Reports do not seem to tell then same story. Since DOE owns the OE-417, can we force NERC to address the OE-417 data in their annual reliability reports?

I have the following recommendations for the Federal Energy Regulatory Commission (FERC):

1. The OE-417s and the NERC Reliability Reports do not seem to tell the same story. Since you are NERC's regulator, can you force NERC to address the OE-417 data in their annual reliability reports?
2. We need transparency and disclosure of the names of CIP violators in order to give incentive to the industry to fix the longstanding physical and cybersecurity weaknesses which plague our electric grid.

I have the following recommendations for the North American Electric Reliability Corporation (NERC):

1. You are not the industry's champion – you are their regulator. Buy a back hat and regulate.
2. You must start disclosing the names of the CIP violators once the violations are mitigated. This will provide the industry with incentive to try harder on cyber and physical security. They are not trying hard enough.
3. You must discuss and analyze the OE-417 data in your annual reliability reports.

I have the following recommendation to Congress:

1. The public and Congress needs reliable and accurate data on the threats to the electric grid. We are not getting it and this must be fixed.
2. We must not allow the industry to protect CIP violators – we need to hold the industry accountable for physical security and cybersecurity.

###

Please help support Michael Mabee's public interest research and grid protection work. Thanks!

NEWS

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

Appendix II - Critical Infrastructure Protection (CIP) Standards

Limitations

In addition to structural weaknesses,[1] CIP Standards contain exclusions and specific metrics that further limit their coverage:

1. CIP Standards apply only to individual BES utilities and selected other "Registered Entities", e.g., "balancing authorities". Some supernumerary functionaries have "reliability authorities" but do not bring cyber assets exclusive to the function.

2. Cyber assets covered by CIP must satisfy a 15 minute "BES" impact rule to be categorized as BES Cyber Assets.

3. Metrics and other rules exclude an extensive set of generation and transmission facilities. The degree of coverage is a critical CIP issue; yet other than a slip-up during CIP v4 negotiations, NERC and FERC carefully hide these numbers from the public.[2]

4. Categorization of Cyber Assets excludes all communications systems and networks, one of four major exclusions from CIP 002-5. Internet connectivity is a major Grid vulnerability; it is also a significant factor in Supply Chain vulnerabilities.

5. With end-to-end modernization, operational technologies (OT) and information technologies (IT) in both Transmission and Distribution Systems are exploding, most with neither security protection nor overriding CIP Standards to ensure protection.

6. CIP Standards prevent utilities from holding their vendors responsible for penetration of the vendors' product Supply Chain, the major attack vector for sophisticated cyber adversaries.

7. CIP Standards do not specifically address "data flows", "data formats", "communications protocols", "encryption", "data aggregations", "analytic processes", "control algorithms" and a myriad of other generic application areas critical to protection of the BES. (NERC will always claim that interpretive decomposition of CIP Standards suffices, making obscurity the major challenge for compliance reviewers.)

8. CIP Standards do not, as yet, require utilities to remove ***known malware*** from their systems.

CIP Coverage.

In negotiations on CIP v4, FERC asked for information on assets coverage for Reliability Regions. Data sent

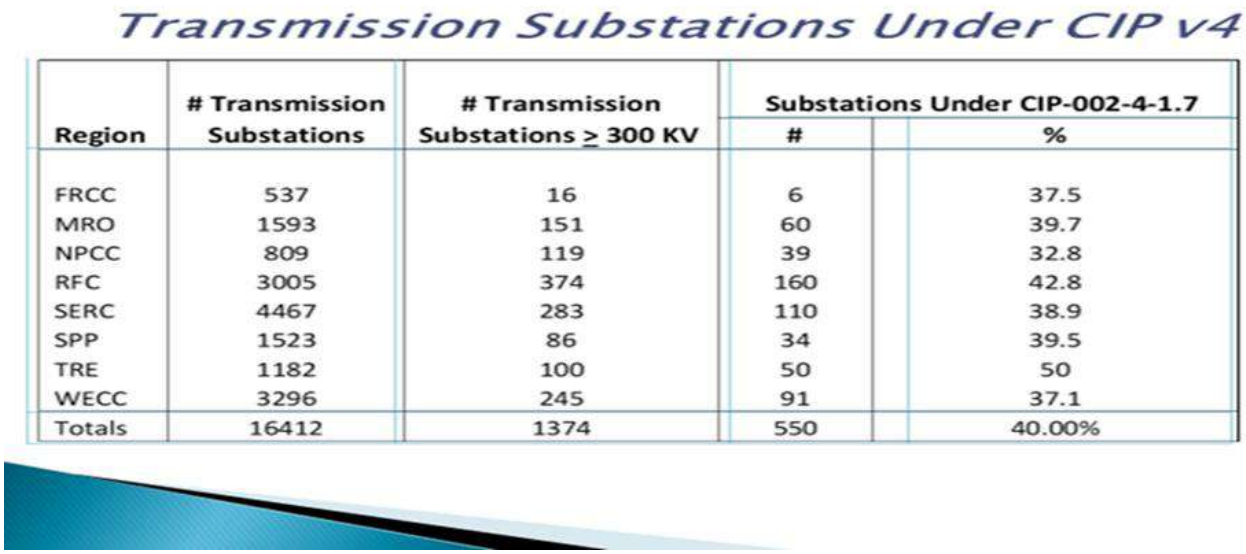
---

[1] For any in-depth examination of the limitations of CIP Standards, a good starting point is the NERC report on "Remote Access required by FERC Order No. 822: Remote Access Study Report, Docket No. RM15-14-___ " June 30, 2017. While NERC concludes that CIP Standards are effective in Risk Management, a good "RED TEAM" examination of this study would conclude just the opposite, flaws and huge omissions by boundary conditions put on the study would demonstrate the futility of extremely weak BES Standards protecting just the BES, let alone Distribution Utilities and Nuclear sites totally dependent on the BES for power.

[2] See table and comments in CIP Coverage. FERC has been challenged in several filings to task NERC for current statistics on assets within or outside CIP Standards but to no avail. Nonetheless, the display from CIP v4 development is believed to reflect current coverage in CIP v5/v6/v7.

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

publicly by NERC is summarized in the following table. CIP v4 was never implemented; however, nothing in follow-on CIP v5 developments would substantially change these facts; viz, substantial inconsistencies across utilities, extremely high percentage of assets exempt from coverage.



Region	# Transmission Substations	# Transmission Substations ≥ 300 KV	Substations Under CIP-002-4-1.7	
			#	%
FRCC	537	16	6	37.5
MRO	1593	151	60	39.7
NPCC	809	119	39	32.8
RFC	3005	374	160	42.8
SERC	4467	283	110	38.9
SPP	1523	86	34	39.5
TRE	1182	100	50	50
WECC	3296	245	91	37.1
Totals	16412	1374	550	40.00%

We can see that only 1374 of a total of 16,412 BES Transmission Substations qualified for CIP Standards based on Kv power minimums (over 90% excluded) and of the qualifiers, only 550 (40%) were estimated by their utilities to be critical to BES Reliability. These judgments were validated by their Reliability Region, i.e., the Compliance Authority and by NERC. NERC will protest that this display does not reflect CIP v5 coverage, but rest assured, they will not voluntarily provide the current coverage statistics.

Critical Infrastructure Protection Standards

CIP	*Title*	*Definition*
002-5.1a	BES Cyber System Categorization	Low, Medium, High
003-5	Security Management Controls	Cybersecurity policies
004-5	Personnel and Training	Security awareness, risk assessment, access management
005-5	Electronic Security Perimeter(s)	Discrete Electronic Access Points
006-5	Physical Security BES Cyber Sys.	Physical security plan
007-5	Systems Security Management	Technical, operational and procedural steps
008-5	Incident Reporting, Response	Incident reporting -1 hour of recognition
009-5	Recovery Plans BES Cyber System	Response for stability, operability, reliability
010-1	Configuration Change Management	Monitoring, vulnerability assessment
011–1	Information Protection	Consolidation of information protection
014-1	Physical Protection	Security of Enterprise Security Perimeters

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

CIP Standards as they exist today are summarized in the above table. They are a subset of Reliability Standards, a much larger and more technical aggregation that were developed by the industry over the last 40 years and are kept current with the major changes in the field. [3] Further, CIP Standards invoke a number of metrics from Reliability Standards and are often linked to the latter in the referenced publication. NERC Standards Development Teams (SDTs) are responsible for development. A typical CIP Standard construct consists of a purpose, applicable "Responsible Entities", requirements that must be satisfied for CIP Cyber Systems to be covered, Violation Risk Factors, Violation Severity Levels (VSLs) to be evaluated for non-compliance, and frequently amplifying narrative. The key CIP Standard is CIP-002.5.1a since it governs categorization of BES Cyber Systems and therefore the applicability of all follow-on CIP Standards to systems so categorized.

CIP-002-5.1a

This "gateway" standard's purpose is to identify and categorize BES Cyber Systems and their associated BES Cyber Assets. Responsible functional entities include Balancing Authorities, certain Distribution Authorities based on BES linkages, Generation Operators, Generation Owners, Interchange Authorities, Reliability Coordinator, Transmission Operator, Transmission Owner. Also defined are Facilities (types) under these authorities and BES Cyber Systems, Cyber Assets covered by Cyber Systems and Control and Monitoring and methodology permitting the flexibility the Utility has in its groupings of Cyber Assets (individually or within a Cyber System).

Attachment 1 to this CIP provides the criteria for judging whether a Cyber System (and its associated Cyber Assets) is categorized as Low, Medium or High Impact. Highlighted assets covered by that criteria are Electronic Access Control and Monitoring Systems (EACMS), Physical Access Control Systems (PACs), and Protected Cyber Assets (PCAs). (***These Assets are the subject of a major disagreement between the Industry, NERC, and FERC over FERC's insistence that they be included in CIP modifications for Supply Chain vulnerabilities[4].)***

Requirement R1 details the assets to be reviewed by the "Responsible Entity" and identified as a medium or high impact asset IAW the criterial in Attachment 1. It further states: "***Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).***"

Requirement R2 calls for a critical review of the set identifications of R1, at least every 15 months and approval of a CIP Senior manager of such decisions.

Note: The following are exclusions from CIP Cyber System Categorization:

"4.2.3. Exemptions: The following are exempt from Standard CIP-002-5.1a:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

---

[3] NERC Reliability Standards for the Bulk Electric Systems of North America, Updated January 3, 2018

[4] Docket No. RM17-13-000 COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.[5]"

Violation Severity Levels (VSLs)

This standard includes VSLs for each of the Requirements, specified as Lower, Moderate, High or Severe. Each details the omissions or flaws revealed by the compliance audit. Penalties is any, are not shown; left to the judgment of the CEA presumably. Note that these CIP Standards all relate to the Impact on the BES and over time, FERC has agreed to local determination by the compliance auditor, overseen by Regional Entities and ultimately by NERC. The Reliability Assessment Initiative[6] has significantly altered the CIP Standards effectiveness in the process.

Compliance

The Regional Entity serves as the Compliance Enforcement Authority (CEA) nominally the Regional Reliability authority or his agent. Compliance evidence is retained by the CEA a minimum of 3 years unless a longer period is specified by the CEA. The Compliance Monitoring and Assessment Processes can involve any or all of the following: Compliance Audit, Self-Certification, Spot Checking, Compliance Investigation, Self-Reporting or Complaint.

Other CIP Standards

The remaining CIP standards follow the same structure as outlined above for CIP 002-5.1a, over 300 pages in the latest Reliability Standards update.[7] With rare exceptions, the standards eschew technical content in favor of process-oriented guidance. The need for "plans" is dominant, plans take utilities to later decisions on details of the protective mechanisms that ultimately must be acquired, installed, maintained.

Grid-wide Security vs. Individual Utility's Endpoint Security

Introduction

Since total protection for the Grid depends on the sum of protection for all the facilities labeled "Electronic Secure Perimeter", it is fair to assess each such facility as an ***"end point".*** The security industry frequently characterizes their guidance in terms of either the enterprise, or the users ***"endpoint",*** the latter a physical or virtual location with boundary conditions that allow for specific protection advice. For "Grid"

[5] Section 4.2.1 identifies one or more facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

[6] The Reliability Assessment Initiative (RAI), a cornerstone of the Compliance process, keys the latter totally to BES Risk Management; permitting self-analysis, and non-public reporting, ostensibly to encourage utilities to open collaboration with CEAs. The RAI has made compliance non-threatening but FERC continues to question NERC efforts to make Compliance totally non-public.

[7] NERC Reliability Standards for the Bulk Electric Systems of North America, Updated January 3, 2018

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

security, we must understand that the Grid involves three major, semi-independent segments overseen by independent authorities, the Bulk Electric System (BES), the NRC nuclear generation facilities, and state-controlled distribution facilities. Neither FERC nor NERC (the Industry Reliability Organization) deny this fundamental segregation and can focus cybersecurity oversight only on the BES and its reliability in supporting the entire national electric system.

However, cybersecurity standards or processes do not apply to the Grid as a whole; instead apply to individual utilities engaged primarily in operation of the Bulk Electric System. Grid-wide situational awareness depends almost totally on the interaction of eight BES "Reliability" regions that monitor system operational technologies (OT) to keep the transmission backbone of the Grid functioning, including supporting power generation systems. CIP v5/v6/v7 cybersecurity standards apply separately (and not interactively) to over 1400 "Responsible Entities",i.e., it's accumulated facilities. Each such physical facility is defined as an ***"electronic security perimeter*** or **ESP**, an "***Endpoint***". Thus Grid-wide operational cybersecurity rests on the premise that the sum of the Endpoint parts secures the overall BES and that a secured BES protects nuclear sites and massive distribution facilities.

> ***Comment***: Would any other major nation-wide enterprise, for example a national security organization, a financial conglomerate, a national healthcare provider, trust its enterprise-wide security totally to individual endpoints? Enterprise-wide security is the major reason why public cloud firms are creating national (and global) VPNs, ***coupling*** secured virtualized data centers, i.e., securing individual endpoints is simply insufficient to protect the entire, networked enterprise.

Discussion

As directed in Federal law, mainly the 2005 amendment to the Federal Power Act, and subsequent embodiment of Critical Infrastructure Protection standards developed by NERC and implemented by FERC, survivability of the entire national electric system therefore depends on the resiliency of the BES to attack, which in turn depends on the security of most of its core 1400 CIP-protected Endpoints. And those endpoints must survive without benefit of an enterprise-wide operational cybersecurity program; i.e., a 24/7 attack detection/warning/alerting system linking them together.

So the critical question for survival of the nation's electric system is "Does EndPoint Security for perimeterized utilities protect the BES and therefore assure reliable electrical supply to nuclear sites, and the mass of Distribution Systems serving fifty states and their urban centers?" Forrester, a major Research firm, rates assessments of the performance of 14 top-rated EndPoint Security Companies on three fundamental product/services capabilities - Prevention, Detection, and Remediation. How well are these functions embodied in CIP v5/v6 standards, becomes the major issue:

- **Prevention.** Do CIP standards require endpoint systems that prevent malware and exploits from executing; does the suite create an environment where malware cannot, for example, load into memory or stop an exploit from taking advantage of a running process? Do endpoint systems implemented under CIP standards reduce the attack surface through system hardening and applications control?

- **Detection**. Do CIP standards ensure that endpoint systems detect malicious activity, post-execution, (knowing attackers will inevitably bypass prevention controls)? For example, do endpoint suites monitor running memory, internal networks, and applications to prevent malware from achieving its goals? Do endpoint systems monitor both process behavior and user behavior to create a context for

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

complete analysis? Do CIP Standards require a SIEM (Security Incident and Event Monitoring) capability that links all facility security protections to feed comprehensive security management?

- **Remediation.** Do CIP standards result in endpoint security suites that identify and contain malicious endpoint activity or a potential vulnerability? Are endpoint suites capable of launching automated remediation (without significant admin involvement) such as: execution/file quarantining, configuration roll-back? Do they implement blocking actions for process and user behavior?

Assessment

The concept for CIP v5/v6/v7 Standards is one of "Risk/Management", with Cyber Assets grouped into Cyber Systems in estimating low, medium or high impact loss on the functioning of the Bulk Electric System as a whole. This concept must assume homogeneity of Cyber Assets with strong mutual exclusion features that eliminate major dependencies among Cyber Systems. Otherwise, significant uncontrollable linkages across low, medium and high impact Cyber Systems would make a nonsense of these categories and therefore "Risk Management".

However, CIP standards as promulgated, seldom specify, or even generalize, on modern interlocking endpoint technical controls such as outlined by Forrester above. CIP standards seldom extend beyond elementary cybersecurity hygienics; e.g., port blocking, password characteristics, personnel accesses, logs, etc., with a complete absence of Endpoint-wide SIEM. Further, there are major exceptions to CIP standards that result, almost always for a given utility, in fuzzy and porous security boundaries and vulnerabilities (for example, data flows) that violate the very concept of endpoint security, such as:

- Mass exclusion from CIP standards of most cyber assets in generation facilities and substations rated below a floor of 300 mw/kva; many with direct internet connectivity and with connectivity to medium and high cyber assets. Also excluded is any facility whose loss would not affect the BES within 15 minutes.

- Complete exclusion from categorization as Cyber assets of all communications and networks linking facility "security perimeters" as defined in CIP v5/v6/v7 standards. (Note that FERC has introduced a contradiction with an Order No. 822 task for development of a standard governing communications security of links between "Control Centers").

- Near complete absence of CIP standards for acquisition, remote maintenance and operation of modern cyber-vulnerable substation instrumentation systems; programmable logic controllers (PLCs) and other industrial control systems (ICS), synchrophasor control units and related data consolidation centers, and SCADA systems. And more importantly, the cyber infrastructures that link these operational technologies together and generate massive data sets for analysis in facility Energy Management Systems (EMS).

Conclusion

CIP Standards do not link even indirectly to vulnerabilities, and they fail to offset cyber threats that are being experienced. CIP Standards perpetuate a fallacy that "Electronic Secure Perimeters" for individual utilities collectively but imperfectly functioning as cybersecurity endpoints, secure the BES. This is eerily reminiscent of Hadrian's Wall during the Roman era in England. Hundreds of forts did not contain the Scots. Communications and networking and "Supply Chains" lacked defenses. It took the Romans 400 years to realize they were on an

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

island and the natives had no place to go. And 1400+ individual utility “ESPs” created from current CIP standards cannot obscure the major vulnerabilities in the North American Grid and their exploitation by Russia’s cyber combat forces.

20190927-5014 FERC PDF (Unofficial) 9/26/2019 6:42:37 PM

Document Content(s)