

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

NERC Notice of Penalty regarding)	Docket Nos. NP18-7-000, RM18-2-000,
Unidentified Registered Entity)	AD17-9-000, RM17-13-000

**Comments of Isologic, LLC and the Foundation for Resilient Societies, Inc. on a Notice of
Penalty for an Unidentified Registered Entity**

(submitted to FERC on May 29, 2018)

The undersigned provide the following Comments, without a formal Motion to Intervene, because we recognize that the decision to name a presently “Unidentified Registered Entity” is discretionary among the Commissioners, and a decision to retain a *de minimus* penalty as proposed by a regional entity, the Western Electricity Coordinating Council (hereafter “WECC”), is also discretionary in the sole decision-making of the Commission.

So we do not seek to Intervene formally, but seek to persuade the Commissioners of the Federal Energy Regulatory Commission (hereafter “FERC” or “the Commission”) that they are at an important crossroad, signaling to the registered entities of the bulk power system, their vendor-contractors, the regional enforcement institutions, and the relevant state Public Utilities Commissions that FERC emphatically rejects a culture of insensitivity to inadequate cybersecurity and cyber-physical protections that can put entire grid Interconnections and the nation at risk. Or not.

Will FERC, with many new Commissioners now in office, determine whether to harness the power and accountability that flows from *transparency* by publicly naming both the “Unidentified Registered Entity” and their contractor-vendor which recklessly exposed an entire topology of grid network assets and communication links to potential cyber and cyber-physical attack? Or will FERC relapse into the presumption of anonymized fines that to the public signals and amplifies fears of *regulatory capture* by the *regulated* of the *regulators*? Does the

Commission now recognize the disinfecting role of public transparency as a foundational resource in fulfilling the Commission's mandate to maintain reliable operation of the bulk electric system (BES)?

Who We Are

Isologic LLC is a limited liability company registered in the State of Maryland. It has a ten-year record of White Papers addressing *Security in the North American Grid*; physical, energy supply and most importantly cybersecurity. These White Papers have documented the evolution of Critical Infrastructure Standards (CIP) since the creation of the program by the Energy Policy Act of 2005. *Isologic* LLC has commented in filings with FERC on Notices of Proposed Rulemakings (NOPRs), Final Rules, and major related technical and policy issues involving cybersecurity issues and programs. Recent *Isologic* LLC filings on open dockets¹ include Incidence Reporting and Supply Chain standards which are relevant to this request to Intervene in the FERC Review of a penalty assessed in a significant security breach involving an Unidentified Responsible Entity (hereafter "URE") and its unidentified contractor-vendor who together caused the exposure of critical assets, network relationships, and communication links that apparently extended over more than 84 weeks or about 590 days.

The *Foundation for Resilient Societies, Inc.* (hereafter "Resilient Societies") is a research and education non-profit incorporated in New Hampshire in March 2012. Its primary mission is to develop understanding of vulnerabilities and remedies to strengthen the reliability and resilience of critical infrastructures, particularly in but not exclusively in the United States. In the month before the tsunami at Fukushima Dai-Ichi, Japan, we filed a draft Petition for Rulemaking with the Nuclear Regulatory Commission, finally accepted by that Commission in December 2012, to strengthen backup-power capabilities to mitigate and recover from solar geomagnetic storms. We have subsequently filed on improvements in physical security, cybersecurity, and other reliability standards, including criteria for cost recovery or resilient

¹ NOPR Cyber Security Incident Reporting Reliability Standards Docket Nos. RM18-2-000 and AD17-9-000 Issued December 21, 2017

capacity auctions to strengthen flexibility, adaptability, and recovery from threats to critical infrastructure operability. Further information is available at www.resilientsocieties.org.

Background

On February 28, 2018, the North American Electric Reliability Corporation (hereafter “NERC”) filed with FERC a Notice of Penalty², with information and details regarding Western Electricity Coordinating Council (WECC) and the URE having entered into a Settlement Agreement **“to resolve all outstanding issues arising from WECC’s determination and findings of two violations of the Critical Infrastructure Protection (CIP) NERC Reliability Standards.”** The NERC filing asserted, without further comment, that the **“URE neither admits nor denies the violations, but has agreed to the assessed penalty of two million seven hundred thousand dollars (\$2,700,000), in addition to other remedies and actions.”**

Facts of this security incident included in the NERC Notice of Penalty (NP) filing can be summarized as follows:

As part of an asset development effort, a URE contractor was given access to the URE asset DataBase (hereafter “DB”), which was subsequently transferred from the URE’s server over a URE network to the Vendor’s network. A 30,000 asset subset of that transferred DB was put on a vendor server that was freely accessible to the Internet (no ID or password [PW] was required). (URE permissions for any or all of this are not stated; however, URE asserted that its contractor failed to comply with URE’s information protection program on which it was trained.)

In May 2016, the existence of this open DB was discovered by a security researcher who downloaded it to his infrastructure.

The exposed DB was publicly available in 2016 for 70 days on the vendor’s network and an additional 10 days before deletion on the security researcher’s system.

² NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP18-07-000 filed on February 28, 2018, 162 FERC ¶ 61,291.

Data exposure included Critical Cyber Assets including ID's, passwords and (unspecified) cryptographic information.

Upon URE notification to the Western Electricity Coordinating Council (WECC), (one of two reliability authorities in the Western Interconnection), discussions and research into the incident ensued for a period of four months involving the URE, presumably its vendor, and the WECC. According to NERC: ***"analysis of the system logs showed that only the security researcher executed commands to view and download data. More detailed system logs would be required to determine definitively that no other third party had downloaded the data, but the short duration of the connections decreased the likelihood that additional accessing or downloading of data had occurred."***³ However, it could not be conclusively shown that there was no compromise of the URE's asset data during the period of exposure on the vendor's or security researcher's sites.

The URE was instructed by WECC to self-report the incident and an incident report was filed by the URE with the WECC.

In its assessment of the incident, the WECC estimated the period of violation at 590 days, from the first exposure to CCA data on the vendor's internet site to the point where the URE completed mitigation by properly classifying and protecting CCA data. WECC ultimately concluded that the URE had violated 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.***) The WECC concluded that the violation posed a severe risk to the Bulk Electric system ("BES") and assessed a penalty of \$2.7M plus an additional sanction.

³ IBID

Additional Background

The security researcher and several media outlets have confirmed that the URE is, in fact, the Pacific Gas and Electric Company, San Francisco, CA.⁴ In response to a query to FERC on whether the URE would be publicly identified, a FERC spokesman said ***“If the commission determines to take further action on a NERC notice of penalty, it may result in a subsequent FERC order or settlement providing more detail. However, commission investigations are non-public, so if they do not result in an order/settlement the specific details would not be public.”***

PG&E issued the following statement⁵ in response to several media inquiries:

“With this incident, it is important to know that none of PG&E’s systems were directly breached in any way and no customer or employee data was involved. A PG&E vendor was hosting an online demonstration using PG&E asset management data to show the capabilities of a platform that they were developing for us. This data contained information on PG&E’s technology assets, such as computers and servers. This data was exposed online by the vendor and was discovered by a third-party researcher. That researcher contacted PG&E security and was unintentionally misinformed that the data was non-sensitive, mocked-up data. We based this feedback on an initial response from the vendor stating that the information in the database was demo or “fake” data. Following further review, we learned that the data was not fake, removed it, and contacted the researcher to correct our statement. We continue working with all of our vendors to have appropriate procedures in place at all times.”

In his blog⁶ issued about the same time, the security researcher identified as MacKeeper researcher Chris Vickery noted that he discovered a MongoDB server exposed to the Internet with no administrator account password. The exposed information, which could have been accessed by anyone without authentication, included IP addresses, hostnames, MAC addresses,

⁴ See for example, “Pacific Gas and Electric Claims Recent Data Breach Only Exposed Fake Details” Softpedia News May 31, 2016 01:55 GMT By Catalin Cimpanu

⁵ Database of California Electric Utility Exposed Online, [Security Week](#) By Eduard Kovacs, May 31, 2016

⁶ Pacific Gas and Electric Database Exposed, MACKEEPER 30 / 05 / 2016 UPDATE (Jun 1st)

locations, operating system data, and over 100 employee passwords. While some of the passwords were hashed, the expert also found ones stored in clear text. He informed PG&E that the unprotected database could not be fake since it also included more than 688,000 unique log entries. Vickery noted that the database was taken down on May 26th after PG&E was notified. Before this happened, he made a copy to forward to the DHS. (It is not clear if the DB was ever forwarded to DHS.)

Reasons for This Filing and Comments

Media reports exposed factual gaps in initial reports of this security violation by the security researcher, PG&E, the WECC, and NERC. PG&E was apparently told by its vendor that the data used in their development was fake and said so publicly, but this was contested immediately by the researcher, with substantial detail on the massive breach as shown above. PG&E later retracted that claim. The PG&E mention of a “demonstration” of the vendor’s development product, not commented on by the researcher, suggests the vendor moved some or all the DB to a separate server for demonstrations of its product. There was no information on whether or not the vendor’s product demonstration contained CCA information, and if the data was further compromised. In truth, the scope of the breach is scanty and unclear and only available from the researcher.

Extensive sanitization by WECC or NERC cannot be justified; either organization should have at least supported the researcher’s factual findings and whether the exposure of asset data was “capped”. The information of value to an adversary, if not the full data set, was already exposed. Confirmation has the obvious value of documenting the severity of the breach for basic understanding by the public, other utilities, and of course, PG&E clients and stockholders.

And as noted in the introduction, we find direct relevancy to outstanding security issues that are central to proposed rulemaking involving inadequate Critical Infrastructure Protection (CIP) standards, Incident Reporting, plus expansive discussion of Supply Chain vulnerabilities –all of which are prominent in this PG&E security issue.

The VPN/Filter malware just revealed⁷ by E & E News is but another wake-up call to the industry, the WECC, NERC and FERC. How many examples of the Russian Federation swath of Grid attack systems are needed before defense of the nation's electric system become high enough priority for breaches such as the PGE case to be taken seriously as National Security incidents? Is there anyone on this green earth who really understands what PGE gave up in this breach? Paired with VPN/Filter, what hope is there that the lights will stay on during a serious US-Russian dust-up?

Admittedly, PG&E was institutionally unable to anticipate the frailty of its vendor's cybersecurity reliability; nonetheless, the vagueness of CIP 003-3 security management requirements; the ambiguity on security of interconnectivity across the BES coupled to NERC determination to rely solely on individual site security perimeters for Grid protection, contributed significantly to this violation. And note the following FERC statement⁸ limiting vendor liability: ***"In addition, the Commission stated that NERC's response to the Order No. 829 directive should respect the Commission's jurisdiction under FPA section 215 by only addressing the obligations of responsible entities and not by directly imposing any obligations on non-jurisdictional suppliers, vendors or other entities that provide products or services to responsible entities."*** Such a statement is distinctly unhelpful in any serious efforts to address Supply Chain vulnerabilities; the principal attack vector of this nation's adversaries. Frankly, NERC is an industry organization and protects utilities' interests; FERC's basic responsibilities are significantly broader. The settlement, therefore, deserves far more careful review than is evident in NP documentation.

Identity of Principals

With the receipt of the NP, FERC is obliged to identify PG&E as the security violator; particularly since the settlement negotiated by the WECC and approved by NERC states that PG&E neither confirms nor denies culpability for the infractions. With its near-bankruptcy failure to deal with

⁷ "Digital 'timebomb' discovered in devices worldwide", ,Blake Sobczak, E&E News, published: Thursday, May 24, 2018

⁸ Docket No. RM16-18-000, Cyber Systems in Control Centers (Issued July 21, 2016)

an energy supply conspiracy a decade ago⁹, and the San Bruno gas pipeline explosion costing 8 fatalities (including failure to admit to gas leaks to the NSTB)¹⁰, PG&E's reluctance to be identified with this 2016 data breach is understandable. But it should not be allowed in the interest of its customers and investors. Furthermore, the PG&E contractor should also be identified if there would ever be a "lessons-learned" from this affair. The NP filing fails to state whether the vendor is still under contract or if it has been blacklisted by PG&E or the WECC.

Legal and Regulatory Concerns

Contractual Relationships

At this point, this major event is not deserving of Critical Energy Infrastructure Information (CEII) protection. The damage has, long since, been catalogued by the nation's adversaries. The gaps in public understanding of this event should be closed. Was the development effort a new contract or a continuing one? If the latter, what were the security provisions governing vendor actions? PG&E's actions? How did they conform to CIP standards? When was this contract entered into? Were there any provisions in the continuing contract that were major factors in the settlement negotiations? If there were, and they put PG&E's cyber assets or operations in harm's way (in retrospect) how far back in time did they extend? If this was a continuing contract, it's important to understand the nature of security vulnerabilities, both at PG&E and at its vendor, and how far back in time they extend.

If it was a new contract, did the contractor have PG&E's permission to access the Asset Database (hereafter "DB") on-line, across the Internet? If so, was that access through secure means or "*en clair*"? Did the contractor have PG&E's permission to download the DB? If so, what restrictions were applied by PG&E? If the contractor did not have permission to take possession of the DB, that was potentially a criminal act. In that event, was it reported to California authorities, to the FBI? If not, why not? If any PG&E authority gave permission for

⁹ California State Senate Energy, Utilities and Communications; Background Relative to Bankruptcy Proceedings, PG&E Bankruptcy Filing, April 6, 2001

¹⁰ Prosecution rests its case in PG&E's federal criminal trial, Mercury News By George Avalos | gavalos@bayareanewsgroup.com

the downloading, that should be reported along with the corrective action taken by PG&E. The entire investigation should have been documented in the settlement and in the NERC NP, unless embargoed as part of a criminal investigation.

CIP Standards

Events of the last several years have conflated several important CIP Standards issues, notably Communications between Control Stations, Incident Reporting vs. malware extraction, and Supply Chain vulnerabilities. Efforts by FERC and NERC to deal with these separately have failed; the interrelationships are too complex. Isologic LLC, Resilient Societies, and Applied Control Solutions, LLC petitioned FERC to reopen the evidentiary record on Order No. 822 following the 2014 Russian incursion in the US Grid and the 2015 follow-on attack on the Ukrainian Grid.¹¹ That request was denied by FERC¹² but led to issuance of Order No. 829 to address intercommunications between control stations (including Internet connectivity). The latter issue links into vendor-utility relationships. The CIP 002-5.1a exclusion of communications and networks from CIP standards is a huge impediment to management of vendor and supply chain vulnerabilities, to say nothing about vendor- support to BES substations industrial control systems (ICS). If this absurdity is not fixed, there is no hope for protection of cyber assets.

PG&E interactions with its vendor are, of course, grist for their contractual relationships. The vendor has already paid some price for his actions, but PG&E would certainly have benefited in the settlement if there existed a hard CIP standards requirement that specifically held the utility responsible for controlling the electronic interfaces with vendors; thereby almost certainly to be addressed in contracting. NERC will argue that CIP 003-7 essentially does this, but it really doesn't. Isologic LLC and Resilient Societies have recommended¹³ blacklisting, whitelisting and independent third party security evaluations relative to supply chain vulnerabilities; essentially ignored to now by FERC.

¹¹ Filings of March 29, 2016, seeking reopening of the record supporting FERC Order No. 822.

¹² North American Electric Reliability Corporation Docket No. RR15-2-005 Order on Compliance Filing (Issued Nov 16, 2016).

¹³ Isologic LLC Filing on NOPR Supply Chain Risk Management Reliability Standards, [Docket No. RM17-13-000] (January 18, 2018) .

Throughout 2016 and 2017, several NERC SDT's developed proposals addressing issues in FERC Order No. 829, proposals that are still open FERC actions, including CIP 003-7. Were those Standard Drafting Teams (SDT's) made aware of the PG&E CIP violations, if not, why not? NERC was most certainly aware of the event and the direct relationship to Order No. 829 tasks. To what extent did NERC seek FERC guidance on "lessons learned" from the PG&E negotiations?

The 2016 CMEP Report

A review of the Compliance Monitoring Enforcement Program (CMEP) report for 2016¹⁴ fails to highlight the extraordinary facts of the PG&E event. Admittedly the annual report is a statistical and anonymous summary, but it does cite major violations and regulatory infractions and should have alluded to this event, as one means of keeping utilities seriously engaged in compliance. For the past several years, security incidents occurring on the North American Grid have been suppressed despite a clear DOE requirement¹⁵ to file OE-417 reports on any incident that has the potential to disrupt the BES. The May 2016 PG&E incident certainly qualified but it was not entered. And this NP studiously avoids that issue. NERC continues its push for non-public reporting of industry infractions in its Reliability Assurance Initiative (RAI) program, the latest being a proposed extension of self-reported medium risk violations as Compliance Exceptions (CEs).¹⁶ The proposal has been denied by FERC but the misuse of CEI, if that is present in this event, needs to be addressed.

Assessment of Risk to the Bulk Electric System

Not unexpectedly, the limited facts of the event promulgated by PG&E and the WECC assessment of BES risk reflect understatement, minimization of details, misstatements and corrections, and serious mischaracterization and omission of vulnerabilities. Along with almost zero inclusion of ongoing threats to PG&E cyber assets, and by extension, much broader threats to other utilities in the Western Interconnection, the Public Utility Commissions of California,

¹⁴ North American Electric Reliability Corporation's annual compliance monitoring and enforcement program filing, Docket No. RR15-2-000 February 21, 2017

¹⁵ OE-417 Electric Emergency Incident and Disturbance Report, Revised November 2014

¹⁶ NERC CMEP for 2016, Docket No. RR15-2-000 February 21, 2017

the clients for PG&E, the National Security installations on the West Coast are significantly put at risk. Risk to the BES spells risk to the Distribution systems serving major urban areas, industries other than the electric utilities, other critical infrastructures of the region. It is simply incredible that the WECC would state the duration of the infraction as 590 days, and yet conclude that there was low likelihood that the massive data breach was accessed by other than the security researcher. The breach included over 680,000 log entries; a gold mine for adversarial analysis. Did PG&E or WECC contact DHS/US CERT for assistance on forensics or the overall security assessment?

The timing is equally important. During 2015/2016 and continuing into 2017, while the PG&E event was transpiring, Russian SVR(Foreign Intelligence) and Russian Ministry of Defense (MOD)/GRU (Military Intelligence) actors were busy exploiting our 2016 national election while continuing its extensive reconnaissance (and worse) in the North American Grid. Exploitation and development of destructive tools occurred, with testing of Russian malware improvements in the Ukrainian Grid in 2015 and 2016. Yet a proposed CIP standard requiring removal of known malware was opposed by NERC and others.¹⁷

There is literally no way to ensure that the exposure of the PG&E asset database has not been exploited by Russian cyber forces. They have demonstrated mastery of reconnaissance, surreptitious entry, modification of software and firmware, an ability to withdraw without leaving traces of their presence. They have shown they can exploit supply chains, deep in system development; capabilities to understand and modify control systems, a deep knowledge of industrial control systems and their vulnerabilities.¹⁸ Those who would undertake assessments of such incidents should study these threats, their flexibility, and their ultimate goals. The simple admission of “Risk” does not do justice to the topic.

The PG&E extended security evaluation left many gaps. The entire flow, every communications node, multiple networks and servers, programmable interfaces, storage systems and all

¹⁷ NERC Comments, Cyber Security Incident Reporting Reliability Standards Docket Nos. RM18-2-000 AD17-9-000, February 26, 2018

¹⁸ See for example, ESET Research Report, “Sednit adds two zero-day exploits using ‘Trump’s attack on Syria’ as a decoy” ESET Research 9 May 2017 - 08:00PM

personnel accesses should have been analyzed to reliably document the violations. Only in this way would it be possible to identify leakages, opportunities for exploitation, and need for standards improvement. There needed to be collection of every access to the network and storage systems holding asset data. There needed to be rigorous examination against holdings of Grizzly Steppe and other intelligence on Russian intrusions in US systems, both Grid and other infrastructure. For the risks are not just to the BES, but to the entire nation. The WECC and PG&E assessment was far from a cover-up but given the events of the past three-four years, it was decidedly myopic.

FERC's Fiduciary Responsibilities to Assist the Several States in Reforming a Culture of Physical-Cyber Insecurity Tolerance

We wish to remind especially the newly-serving FERC Commissioners that the Critical Infrastructure Protection (CIP) reliability standards are mandatory for registered entities in the bulk electric system, but generally are only advisory within electric distribution entities serving the several states. The states have their own need to strengthen cybersecurity. And helping the states attain these goals is also essential for improved physical-cybersecurity of the bulk electric system. FERC Commissioners need only look to what happened in the Ukrainian grid during December 2015 and December 2016. Foreign actors, operating from remote systems within Russia, entered the Ukrainian distribution system operator control systems, which also provided cyber entry pathways back to regional transmission and control systems.

If FERC determines to provide *fig leaf cover* for the largest gas-electric utility in the State of California, by averting formal acknowledgment that the presently Unidentified Registered Entity (URE) is in fact Pacific Gas & Electric Corporation, and by identifying the unnamed Contractor-Vendor materially responsible for the resulting hazards, how will the California Public Utilities Commission change the business-as-usual culture that places at risk the entire system operated through the California Independent System Operator and the entire Western Interconnection?

Initiatives of the California Public Utilities Commission Deserving FERC Support

On August 27, 2015 the California Public Utilities Commission (hereafter “CPUC”) which regulates gas and electric services of Pacific Gas & Electric Corporation within California, commenced a formal investigation:

“into whether the organizational culture and governance of PG&E Corporation and the Utility prioritize safety and adequately direct resources to promote accountability and achieve safety needs and standards...”

PG&E has been fined \$2.25 billion -- three orders of magnitude more than the proposed cyber-security fine announced on February 28, 2018 -- for deaths, fires, and a failure of accountability linked to the San Bruno pipeline fire. Further, in April 2013, the Metcalf Substation shootout of 17 high voltage transformers was ascribed by PG&E spokespersons as mere “vandalism.”

Following a preliminary investigation by the California PUC (CPUC), both by an internal CPUC staff unit and by a designated monitor, on May 8, 2017 the CPUC released the Consultant’s report, with a scoping memo proposing a second stage of investigation of the operating culture within PG&E Corporation. Further, the CPUC “will evaluate the safety recommendations of the consultant... The scoping memo will also consider all necessary measures, including but not limited to, a potential reduction of the Utility’s return on equity until any recommendations adopted by the CPUC are implemented”

One of the remaining issues in dispute, after PG&E and the CPUC agreed on several findings and recommendations, was and remains “cyber security.”¹⁹

Hence, if FERC proceeds to conceal the name of the Unidentified Registered Entity to be fined merely \$2.7 million as of February 28, 2018,²⁰ the California PUC Staff will know who failed

¹⁹ PG&E Corporation, Form 10-Q for the Quarterly Period ended March 31, 2018, Part II, Item 1 (“Legal Proceedings”), filed with the SEC May 3, 2018, available online via the SEC’s EDGAR database.

²⁰ Relying upon the latest 10-Q financial statement from PG&E Corporation, the net assets of the PG&E Corporation, after subtracting outstanding liabilities, as of March 31, 2018 were \$19.983 Billion dollars. So a fine of

California ratepayers and citizens, but it will not receive formal, public notice of these hazards. It will receive less than minimal support from FERC to change a culture of “business as usual” disregard of protective standards, not intentional disregard, but complacency, and false claims of a “fake” database being at risk” and an undetected infrastructure exposure that apparently lasted as long as 590 consecutive days before exposure, not by PG&E but by an independent “white hat” cyber specialist.

Conclusion and Recommendations

The proposed settlement should not be accepted by FERC. The penalty is less than one-tenth of one percent of PG&E’s operating income for 2017,²¹ and far less of the corporation’s net worth. This penalty is hardly enough for the wake-up call this data breach deserves.²² The Commission will probably conclude that no useful purpose would be served by a larger penalty, but much is in turmoil in the Western Interconnection:

At least three separate organizations are claiming responsibility as the Western Interconnection Regional Reliability Coordinator, the WECC that lost the job several years ago, Peak RC facing the loss of member PG&E, and CAISO (with PG&E as its cornerstone.)

- The loss of the Canadian Province of Alberta to the Western Interconnection.

merely \$2.7 million dollars is just 1.35 thousandth of one percent of the net equity of the firm. A fine so minimal, particularly with the benefits of FERC-sponsored anonymity, would be an invitation to future safety, reliability, and security impunity by PG&E and its vendors.

²¹ PG&E 2017 Revenue: \$17.14B, Operating Income \$2.96B, Net Income \$1.66B, SEC Annual Report 2017

²² Although PG&E was not the original source of the system wide compromise, that corporation was reckless in failing to monitor its vendor’s practices, willful in claiming the compromised database was “fake,” and tardy in its responsive actions. When there has been reckless behavior resulting in harm, punitive damages are widely assessed in civil tort actions. See the following literature: Robert D. Cooter, “Economic Analysis of Punitive Damages,” 56 *S. Cal. L. Rev.* 79 (1982); K. S. Abraham and J. C. Jeffries, “Punitive damages and the rule of law: the role of defendant’s wealth,” 18 *J. Legal Studies* 415 (1989); S. M. Polinsky and S. Shavell, “Punitive Damages: An Economic Analysis,” 111 *Harv. L. Rev.* 869 (1998); Note, “Common Sense Legislation: The Birth of Neoclassical Tort Reform,” 109 *Harv. L. Rev.* 1765 (1996); N. R. Mead, “Who is liable for insecure systems?” 37 *Computer*, July 2004, 27-34; I. B. Utne, et al. “A method for risk modeling of interdependencies in critical infrastructure,” *Reliability Engineering & System Safety*, 2011, v. 96, 671-678; Chee-Woo Ten, et al. “Impact assessment of Hypothesized Cyberattacks on Interconnected Bulk Power systems,” *IEEE Trans. Smart Grid*, Jan. 2017

- The contemplated defection of the Southwest Power Pool (SPP) from the Eastern Interconnection in favor of a partnership with Mountain West Transmission Group Initiative.
- A potential partnership between PEAK RC and a unit of PJM with the same objective.
- And a declaration by PG&E's CAISO of intention to compete for RTO control as well.

FERC's authorities in these efforts are apparently being ignored. But what is the effect of all of this on Grid Reliability, and its stepchild Cybersecurity? Not good to say the least. This Notice of Proposed Penalty without a significant upgrading of the fine and public identification of the Unidentified Registered Entity and its Contractor-Vendor will reinforce the sense of impunity to the foregoing participants. FERC should not let that happen.

We note with regret that in response to a third party FOIA request,²³ FERC has as recently on May 25, 2018 claimed that the Unidentified Responsible Entity (URE) should be shielded from disclosure as a matter of protecting Critical Energy Infrastructure Information. We understand the CEII protection through completion of review by the FERC Commissioners. But if FERC continues to shield the URE and its Contractor-Vendor and agrees to a fine that is miniscule in relation to annual operating income or equitable net worth as high as \$19.983 billion dollars, we would propose an alternative acronym: Critical Energy Impunity Inducement, also CEII.

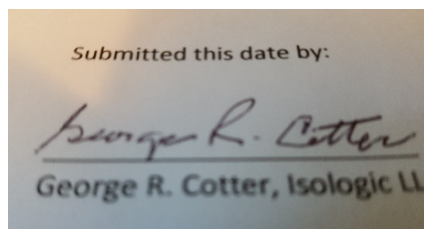
Despite loss of two years, FERC should create a joint FERC-DOE-FBI team to comprehensively review the PG&E event. That study should address the real-world facts of potential compromise, interview the security researcher who made the initial report, investigate any linkages to Russian incursions in the North American Grid, make recommendations on changes to reliability and cybersecurity standards arising out of the investigation, and validate or revise a penalty amount recommendation to FERC.

We respectfully request the FERC Commissioners signal the benefits of transparency, impose a significantly higher penalty, publicly identify the Unidentified Responsible Entity, publicly identify the Unidentified Contractor-Vendor, and request a FERC, DOE, and FBI joint

²³ Michael Mabee. FERC Response and denial dated May 25, 2018.

investigation to determine whether adversary actors have acquired access to the asset and communications linked Data Base at risk for approximately 590 consecutive days in years 2015-2017.

Respectfully submitted,



Submitted this date by:
George R. Cotter
George R. Cotter, Isologic LLC

Respectfully submitted by:



Thomas S. Popik, Chairman,



William R. Harris, Secretary,

For the

Foundation for Resilient Societies

52 Technology Way

Nashua, NH 03060-3245

www.resilientsocieties.org

williamh@resilientsocieties.org

Document Content(s)

NP18-7-000 Joint Isologic & Resilient_Societies Comments.PDF.....1-16