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 submitted to FERC on October 28, 2019
by the Foundation for Resilient Societies

The Foundation for Resilient Societies ("Resilient Societies") respectfully asks the Federal Energy Regulatory Commission ("FERC" or "Commission") to step up its regulatory game. Unless changes are made at FERC, catastrophic blackouts are coming to America.

FERC has had fourteen years to establish strong grid reliability standards and implement a tough enforcement regime. Instead, FERC has often acted as a captive regulator of the electric utility industry. When catastrophic blackouts hit, it is likely that the utilities responsible will have violated mandatory electric reliability standards. It is also likely that the identity of these violators will have been actively concealed by the FERC's regulatory system.

FERC can make a fresh start by holding a public hearing on how to improve transparency in the enforcement of electric grid reliability standards; we ask that the Commissioners personally attend this hearing. FERC should invite a diverse group of subject matter experts and stakeholders to testify, beyond the regular standard panels of industry Trade Associations and executives. Potential witnesses could include state regulators, insurance and reinsurance executives, Securities and Exchange Commission officials, bond and equity raters, bankruptcy experts, cybersecurity experts, victims of extended grid blackouts, nonprofits with expertise in utility regulation, and other key stakeholders.

If changes in FERC' regulatory process are not made, and if a blackout causing hundreds, thousands, or millions of deaths occurs, much of the blame will fall on this agency and its Commissioners. In 2005, Congress and the President, via the Energy Policy Act, gave FERC regulatory authority over the most critical part of the U.S. electric grid, the high-voltage Bulk Power System. Congress acted in response to the 2003 Northeast Blackout, an event initiated by deficient vegetation management that impacted 55 million people in eight states and two Canadian Provinces.[1] This reform provided authority for *mandatory* reliability standards to be enforced by a to-be-designated Electric Reliability Organization (the "ERO"), subject to FERC oversight. FERC designated the North American Electric Reliability Corporation ("NERC") as the ERO, and promulgated reliability standards starting in year 2007.

The 2010 U.S. government report "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System" made cybersecurity, physical security, and other electric grid threats clear.[2] A stream of official reports and actual events since then have reinforced the urgency of regulatory action.

With the departure of previous commissioners, FERC is now under new management.[3] FERC, to be augmented by additional Commissioners in coming months, has an opportunity to show real leadership. The reconstituted FERC can serve the public interest by shining light on major breaches of reliability standards, early and consistently. The new FERC can and must end

[1] U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada," April 2004.
[2] North American Electric Reliability Corporation and U.S. Department of Energy, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," June 2, 2010. Accessed October 25, 2019 at https://www.energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf
[3] At the time of this docket filing, the FERC Commissioners are Neil Chatterjee, Richard Glick, and Bernard McNamee.

a decade of coverups for utilities that place America's population and critical infrastructures at great peril.

FERC CONCEALED PG&E VIOLATIONS BEFORE CALIFORNIA BLACKOUTS

On the day of this filing, California has just experienced its third round of pre-planned blackouts in two weeks. Pacific Gas & Electric (PG&E) has implemented multiple Public Safety Power Shutoffs to prevent wildfires caused by power lines contacting vegetation. Altogether, over 2 million people have been blacked out.

The Kincade Fire, burning over 54,000 acres and causing more than 180,000 people to flee for their lives, started on October 23rd, just minutes after the failure of a PG&E 230kV transmission line under the regulatory authority of FERC.

Figure 1. Fox News Report of Kincade Fire[4]

[4] https://www.foxnews.com/us/kincade-fire-rages-aided-by-hurricane-force-winds

PG&E is a repeat violator of cybersecurity and other reliability standards. PG&E's identity has a violator has been concealed by FERC. On February 28, 2018, PG&E was fined $2.7 million for violations of cybersecurity and other standards; on October 31, 2016, PG&E was fined $1.125 million for violations of cybersecurity and other standards; on May 29, 2014, PG&E was fined $98,500 for violations of cybersecurity and other standards. The NERC Notices of Penalty filed in the FERC dockets concealed the identity of the violator in each of these cases—PG&E's identity only became known through Freedom of Information Act requests filed by Michael Mabee, [5] a private citizen, and reporting of the *Wall Street Journal*.[6] [7]

On July 31, 2009, before FERC began concealing the identity of standards violators, PG&E was fined $100,000 for violations of vegetation management and other reliability standards. But because FERC changed its enforcement system in 2010, we don't know if PG&E again violated vegetation management in the ten years between its 2009 fine and the latest round of California wildfires. FERC should release information to the California Utility Commission and the public regarding the date of PG&E's last NERC audit and whether any vegetation management violations were found.

Deficient management practices at PG&E have been longstanding, but FERC's concealment of standard violations has kept critical information from investors, state regulators, and the public. California residents are now faced with years of prospective blackouts caused by management shortfalls. Blackouts to prevent wildfires are painful, but if

[5] Mr. Mabee's FOIA requests and FERC's responses are available at: https://michaelmabee.info/cip-violation-database/ Accessed October 27, 2019.
[6] Rebecca Smith, "PG&E Among Utilities Cited for Failing to Protect Against Cyber and Physical Attacks," *Wall Street Journal*, April 9, 2019. https://www.wsj.com/articles/pg-e-among-utilities-cited-for-failing-to-protect-against-cyber-and-physical-attacks-11554821337
[7] FERC Dockets NP14-41-000, NP17-2-000, and NP18-7-000.

PG&E is hit with a cyberattack or physical attack, the impact on California could be even more catastrophic.

It's not just PG&E and California that are at risk. Grid security vulnerabilities are endemic across the United States. The January 2019 Worldwide Threat Assessment of the U.S. Intelligence Community concluded, "Moscow is now staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis and poses a significant cyber influence threat."[8] In January 2019, the *Wall Street Journal* published an article titled, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It."[9]

How did our nation get to this vulnerable point? The answer lies in the story of the secret regulatory system devised by FERC, at the behest of the electric utilities that FERC regulates "in the public interest."

"SETTLEMENTS WILL BE MADE PUBLIC"

For the initial period of FERC's enforcement of grid reliability standards, February 2006 to June 2010, the Notice of Penalty and other documentation for settlement agreements were made public. Public disclosure of the identity of those who settle violations of laws and regulations is a key part of the system of justice in our democracy. In fact, the U.S. Department of Justice prohibits secret settlement agreements in civil matters, except in rare circumstances.[10]

---

[8] Daniel R. Coats, "Worldwide Threat Assessment of the U.S. Intelligence Community," Director of National Intelligence, January29, 2019. Available at: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[9] Rebecca Smith and Rob Barry, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It*," Wall Street Journal*, January 10, 2019. Available at: https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

[10] See "1-18.200 – Settlement Transparency" in the DOJ Justice Manual: "'It is the policy of the Department of Justice that, in any civil matter in which the Department is representing the interests of the United States or its agencies, it will not enter into final settlement agreements or consent decrees that are subject to confidentiality

The FERC attorneys drafting the original enforcement rules knew that an effective regulatory system requires public naming of violators. FERC Order 672, "Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards," clearly stated that "settlements will be made public":[11]

> *[P]ursuant to section 39.7(b)(4) of the Final Rule, the ERO should file, for informational purposes only, any settlement of an alleged violation regardless of whether the agreement contains an admission by the settling user, owner or operator.* ***Settlements will be made public.*** *This is consistent with our own procedures in which enforcement settlements are made public. (Emphasis added.)*

Initially, FERC's regulatory system was functioning, at least at a basic level. FERC's designated auditor for electric reliability standards, NERC and its Regional Entities were finding violations and fining utilities. For example, in 2009, PG&E was fined $100,000 for violations of NERC Standard FAC-003-1, "Transmission Vegetation Management Program" and other reliability standards.

MIXED INTENTIONS ENABLE A SECRET REGULATORY SYSTEM

Even at the formation of the FERC-NERC regulatory system in 2005, FERC and industry players promoted what might be considered both a well-intentioned idea and self-serving concept—that the identities of utilities which violate a subset of the electric reliability

---

provisions, nor will it seek or concur in the sealing of such documents.' 28 C.F.R. § 50.23. While there may be "rare" exceptions to this policy that may be invoked only by certain Department officials, see id., as a general rule, civil settlements are subject to the principles of openness in judicial proceedings."

[11] Order 672, 71 FR 8736, Feb. 17, 2006 at p. 230, 598, FERC Stats. & Regs. ¶31,204, as amended by Order 737, 75 FR 43404, July 26, 2010

standards, so-called "Critical Infrastructure Protection" (CIP) standards for cyber and physical security, should be concealed—ostensibly to prevent so-called "bad actors" from learning which utilities were vulnerable and how to best conduct attacks.[12] Notably, PG&E was a strong and early proponent of secrecy. [13]

By 2010 cybersecurity concerns had increased, spurred by media disclosures of electric grid penetrations by foreign adversaries. But how could a change to the regulatory system be implemented, without alerting those who might oppose it?

In July 2010, FERC approved Order 737, which was titled ""Technical Corrections to Commission's Regulations." A key provision requiring public disclosure of a violating utility's identity was *deleted* from FERC regulations, "PART 39—RULES CONCERNING CERTIFICATION OF THE ELECTRIC RELIABILITY ORGANIZATION; AND PROCEDURES FOR THE ESTABLISHMENT, APPROVAL, AND ENFORCEMENT OF ELECTRIC RELIABILITY STANDARDS," paragraph (d)(6).[14]

A secret regulatory system was born. In NERC's official communications to FERC, redactions and big black bars began to conceal the identity of utilities which violated standards:

[12] Comments of Southern Company Services, Inc., FERC Docket No. RM05-30-000, October 7, 2005, pp. 10-11. "Southern Companies agree with the Commission that vulnerable aspects of the industry at large or of a particular user, owner or operator should not be publicly divulged. Non-public and confidential procedures for enforcement matters involving cybersecurity are thus critically important."

[13] Comments of Pacific Gas & Electric Company, FERC Docket No. RM05-30-000, October 7, 2005, p. 21. "PG&E agrees with the Commission's proposed regulations set forth in Section 38.5(d)(8) with regard to Cybersecurity Incidents, which are reasonable to protect sensitive and confidential information where public dissemination could jeopardize system security and reliability… public notices should be limited to avoid inadvertent disclosure of confidential information…an alleged violator should be permitted to request that a hearing closed to the public…"

[14] Paragraph (d)(6) had read before its deletion: "A form of notice **suitable for publication**;" (emphasis added). In FERC practice, this was a "Notice of Filing" in the public FERC docket system that identified the violating utility and recited the Commission's Rules of Practice and Procedure to persons wishing to intervene on the docket.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

January 25, 2019

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding [redacted]
FERC Docket No. NP19-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty regarding [redacted] with information and details regarding the nature and resolution of the violations[2] discussed in detail in the Settlement Agreement attached hereto (Attachment A), in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

Figure 2. Example of Redacted Notice of Penalty in Accordance with FERC Regulations

To complete FERC's regulatory sleight-of-hand, review by Congress (and public comment, too) had to be forestalled. The attorneys drafting FERC Order 737 dutifully formulated this wording, approved by the Commission:

> *14.* ***The provisions of 5 U.S.C. 801 regarding Congressional review of final rules do not apply to this Final Rule****, because this Final Rule concerns agency procedure and practice and will not substantially affect the rights of non-agency parties.*

> *15.* ***The Commission is issuing this Final Rule without a period for public comment.*** *Under 5 U.S.C. 553(b), notice and comment procedures are unnecessary where a rulemaking concerns only agency procedure and practice, or where the agency finds that notice and comment is unnecessary. (Emphasis added.)*

For good measure, FERC Order 737 reassured the public that it need not be concerned:

> *This rule concerns only matters of agency procedure and will not significantly affect regulated entities or the general public. (Emphasis added.)*

THE SECRET REGULATORY SYSTEM BECOMES EVEN MORE OPAQUE

The electric utility industry and its attorneys can be even more adroit than government attorneys. In quick order, they apparently realized if utilities negotiated a single Notice of Penalty for both CIP and non-CIP standard violations, then under FERC Order 737, the identity of the offending utility would be concealed for *all violations*—including violations that have little to do with cybersecurity: load balancing, transmission planning, personnel training, and even vegetation management.[15]

How effective has FERC's secret regulatory system been in concealing the identity of utilities which violate electric reliability standards? According to the September 26, 2019 NERC Searchable Notice of Penalty (NOP) Spreadsheet, there were 6,317 standard violations filed

[15] It took six years, but eventually FERC and/or NERC got wise to the technique of negotiating a single Notice of Penalty for both CIP and non-CIP violations and this practice was stopped. The last non-CIP reliability standard violator concealed as an "Unidentified Registered Entity" was in NP17-31-000 filed on September 28, 2017. However, as we found out, the record of these violators can still be withheld when Freedom of Information Act requests are made to FERC. Moreover, the identities of CIP standard violators remain secret to the current day.

from July 2010 to September 2019. For 3,892 of these violations, the identity of the utility was concealed, including 273 instances where the identity of non-CIP violators was concealed.[16]

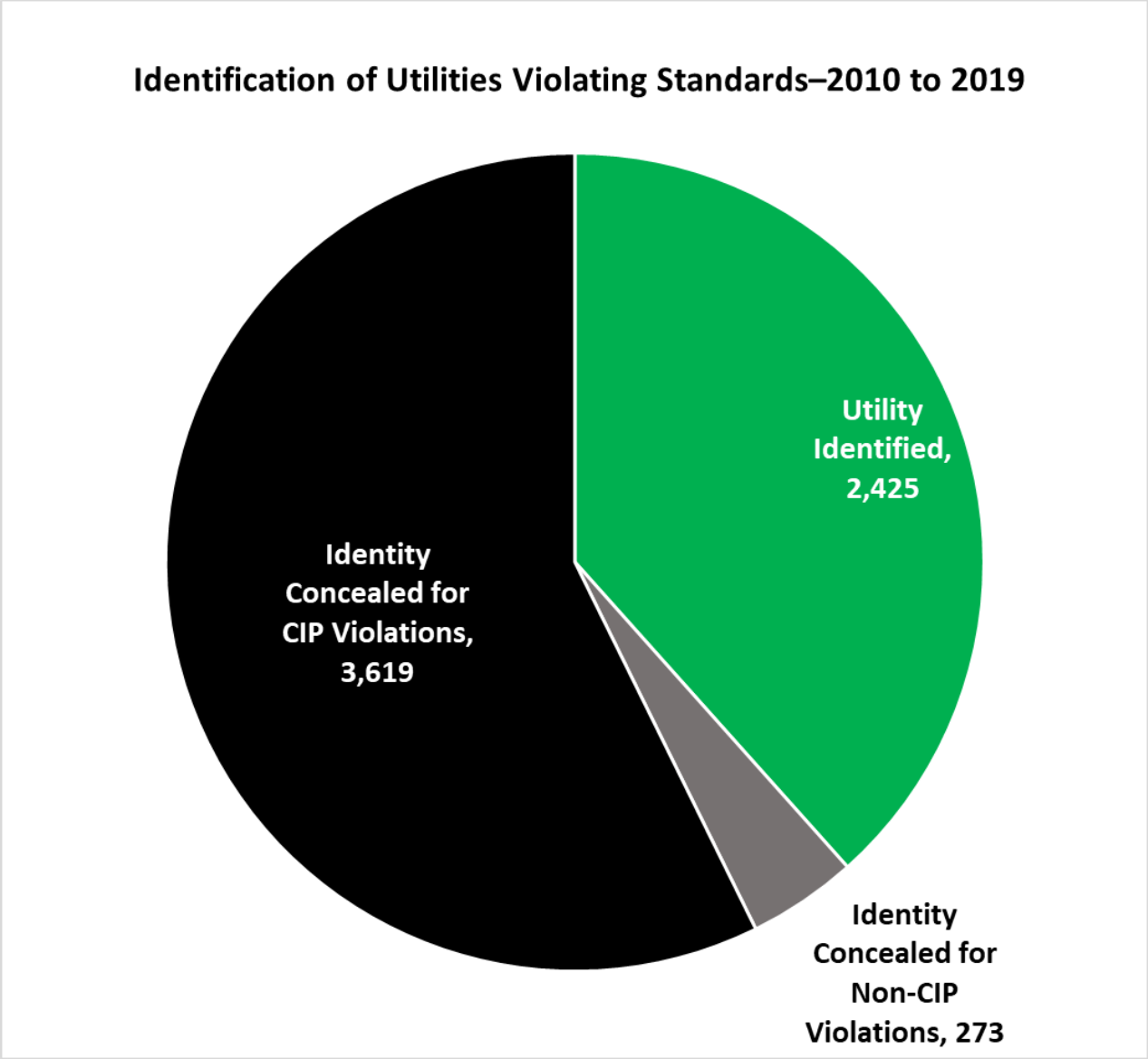

Figure 3. Tabulation of NERC Searchable Enforcement Spreadsheet by Utility Identities

[16] Statistics based on searches of NERC Enforcement and Mitigation webpage, "Searchable NOP Spreadsheet," from July 2010 through September 2019. https://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx. Accessed October 23, 2019.

We believe that the concealment of reliability standard violations, including the identity of the violators, defeats the primary purpose of the Energy Policy Act of 2005. The intent of Section 215 of the Act is to make the Bulk Power System *more reliable*, not *less reliable.*

THE SECRET REGULATORY SYSTEM BLOCKS PUBLIC INQUIRY

We decided to test FERC's regulatory system to see if it had been reformed in 2019 or, alternatively, was still being used to protect the interests of electric utilities. In the aftermath of the deadly California Camp Fire in 2018, we wanted to learn which utilities in the Western United States had been violating vegetation management and other reliability standards. On April 22, 2019, we filed a Freedom of Information Act (FOIA) request with FERC. Here's what we said in our FOIA request:

> *Because of catastrophic and deadly fires in the Western Interconnection caused by transmission lines contacting vegetation, the public has an interest in knowing which utilities have been fined for non-compliance with vegetation management standards and the terms of their settlement agreements. For each standard violation in the above requested Notice of Penalty (NOP), the Violation Risk Factor is "high."*

For the violations listed on requested docket NP11-137-000, the penalty for the utility had been $106,000; for NP11-128-000, the penalty had been $450,000. These are non-trivial fines. All the cybersecurity violations for NP11-137-000 had been mitigated by December 16, 2008; all cybersecurity violations for NP11-128-000 had been mitigated by February 27, 2009. Accordingly, disclosure of the identity of the violating utilities should not have resulted in any information useful to an attacker. National security should not be a factor in these cases.

FERC's Office of External Affairs nonetheless denied our Freedom of Information Act request for the identity of the standards violator. This was their byzantine reasoning:

> *Before determining whether the identity of a URE may be released, the Commission must consider a number of factors. Among other things, these factors include the nature of the Critical Infrastructure Protection (CIP) violation, including whether it involves a Technical Feasibility Exemption (TFE); whether mitigation is complete; the content of the public and non-public versions of the Notice of Penalty; the extent to which the disclosure of the pertinent URE identity would be useful to someone seeking to cause harm; whether an audit has occurred since the violation(s); whether the violation(s) was administrative or technical in nature; and the length of time that has elapsed since the filing of the public Notice of Penalty… Based on application of the various factors discussed above, I conclude that disclosing the identity of the UREs in NP11-137 and NP11-128, in combination with the information contained in the public versions of the Notices of Penalty, would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor.*

We painstakingly examined public Notices of Penalty for these two dockets. We found zero evidence that the reasons FERC gave for our FOIA denial are valid. In fact, we confirmed that all the cybersecurity standard violations were mitigated a decade ago. In order to keep the identities of standards violators from us, it appears that FERC just cut and pasted boilerplate excuses into its letter. We will be appealing FERC's denial of our FOIA request.

FERC'S REGULATORY SYSTEM RELIES ON DISCREDITED CYBERSECURITY CONCEPTS

It is ironic that the rationale for FERC's concealment of standard violations is based on a discredited cybersecurity concept, "Security Through Obscurity." The Software Engineering Laboratory at the National Technical University of Athens provides this description: [17]

> *Security Through Obscurity (STO) is the belief that a system of any sort can be secure so long as nobody outside of its implementation group is allowed to find out anything about its internal mechanisms. Hiding account passwords in binary files or scripts with the presumption that "nobody will ever find it" is a prime case of STO.*
>
> *STO is a philosophy favoured by many bureaucratic agencies (military, governmental, and industrial), and it used to be a major method of providing "pseudosecurity" in computing systems.*

Government experts at the National Institute of Standards and Technology confirm that "Security Through Obscurity" is not a recommended cybersecurity practice:[18]

> *System security should not depend on the secrecy of the implementation or its components.*

[17] Software Engineering Laboratory at the National Technical University of Athens, "What is 'security through obscurity'," Undated. Available at: http://users.softlab.ntua.gr/~taver/security/secur3.html

[18] Karen Scarfone, Wayne Jansen, and Miles Tracy, "Guide to General Server Security," National Institute of Standards and Technology, July 2008, p. 2-4. Available at https://csrc.nist.gov/publications/detail/sp/800-123/final

FERC'S REGULATORY SYSTEM DOES NOT USE BEST PRACTICES FOR DISCLOSURE

When it comes to cybersecurity disclosures, FERC and the electric utility industry have different timelines and processes than best practices at other U.S. government agencies and industries. For example, the Vulnerability Disclosure Policy at the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security has a 45-day timeline and seven-point criteria for release of cybersecurity vulnerabilities:[19]

> *In cases where a vendor is unresponsive, or will not establish a reasonable timeframe for remediation, CISA may disclose vulnerabilities as early as 45 days after the initial attempt to contact the vendor is made, regardless of the existence or availability of patches or workarounds from affected vendors.*
>
> *It is the goal of this policy to balance the need of the system owners and operators to be informed of potential risk associated with security vulnerabilities with the vendors' need for time to respond effectively. The final determination of the type and schedule of publication will be based on the* ***best interests of the community overall****. (Emphasis added.)*

Google has a 90-day timeline for disclosure that can be shortened to 7 days for "zero day" vulnerabilities:[20]

> *We believe that vulnerability disclosure is a two-way street. Vendors, as well as researchers, must act responsibly. This is why Google adheres to a 90-day disclosure*

[19] Cybersecurity and Infrastructure Security Agency, "CISA Vulnerability Disclosure Policy," U.S. Department of Homeland Security, undated. Accessed on October 27, 2019 at: https://www.us-cert.gov/vulnerability-disclosure-policy

[20] Google Application Security, "How Google handles security vulnerabilities," Alphabet Inc., Undated. Accessed October 27, 2019 at: https://www.google.com/about/appsecurity/

deadline. We notify vendors of vulnerabilities immediately, with details shared in public with the defensive community after 90 days, or sooner if the vendor releases a fix.

When we observe a previously unknown and unpatched vulnerability in software under active exploitation (a "0day"), we believe that more urgent action—within 7 days—is appropriate. The reason for this special designation is that each day an actively exploited vulnerability remains undisclosed to the public and unpatched, more devices or accounts will be compromised.

CISCO publishes detailed security advisories, even when there are no workarounds available. Here is an example of an advisory for the Adaptive Security Appliance/Industrial Security Appliance line of firewalls widely used in the electric utility industry:

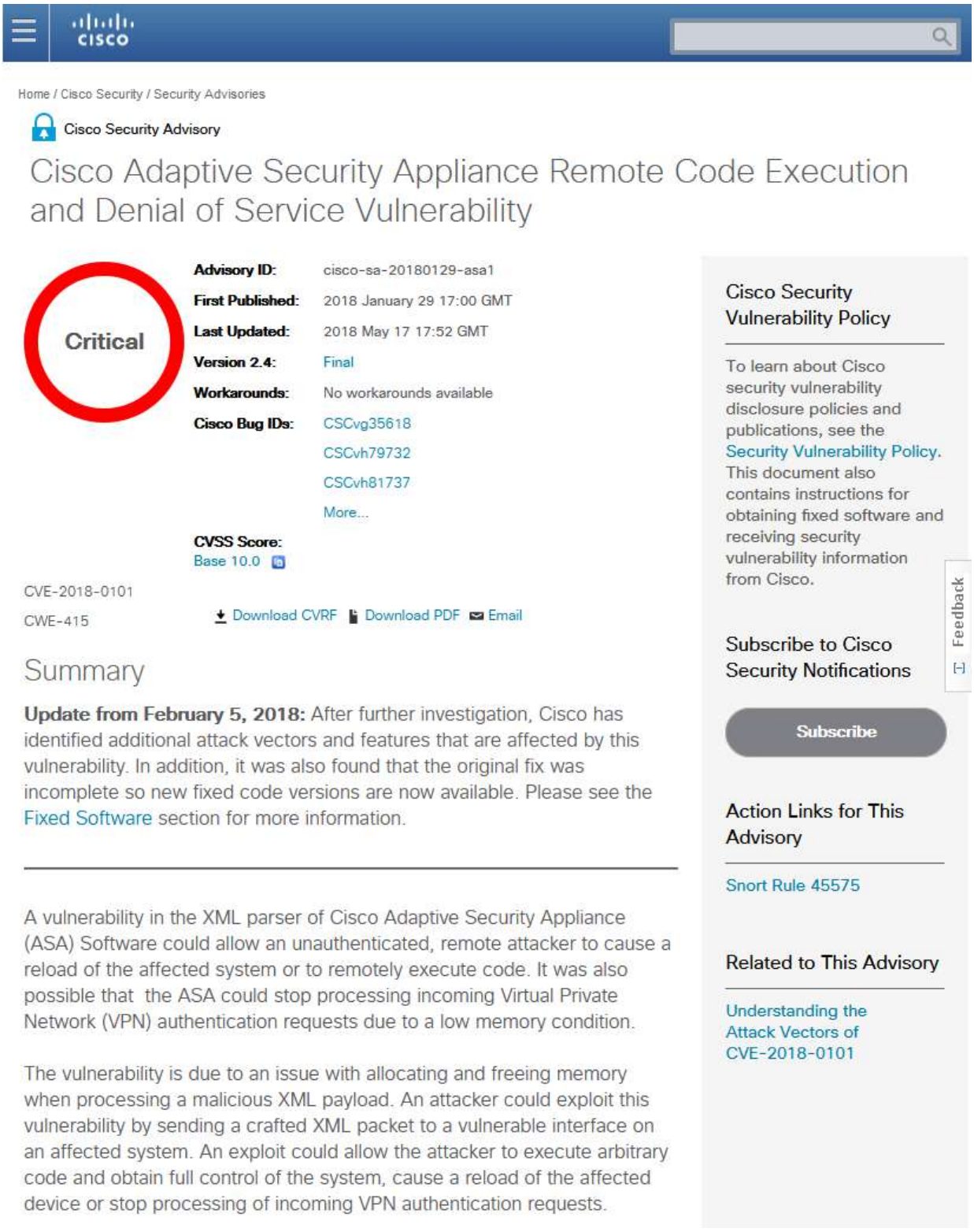

Figure 4. Screenshot of CISCO Security Advisory for CVE-2018-0101

Most U.S. high-tech companies promptly disclose and fix cybersecurity vulnerabilities with engineers, or they will lose customers. Most U.S. electric utilities have market power and most distribution utilities are monopolies; many of them reflexively rely on lawyers and Trade Associations to work for concealment of their vulnerabilities.[21] The public is depending on FERC to regulate these companies where consumers lack choice in providers.

SECRECY PREVENTS FUNDING FOR CYBERSECURITY FIXES

Electric utilities, operating through their cooperative regulator FERC, have been tremendously successful in concealing vulnerabilities from the public, including cybersecurity vulnerabilities. Ironically, utilities have become victims of their own success. In order to recover costs for security improvements, they must make a case before the public utility commissions of the states.

[21] Moody's Investors Service published a recent report that compares the scope of public disclosure of cyber incidents and cyber risks across sectors of the economy. Moody's found that banks, telecommunications and media companies provide the most detailed disclosures among the sectors that Moody's analyzed. These companies generally "discuss in fairly specific terms their cybersecurity risk management strategies." Moody's found that electric utilities in Europe are more likely to discuss publicly their cybersecurity management strategies, while U.S. electric utilities are more likely to provide "boilerplate" disclosures. Market infrastructure providers, securities firms, and electric utilities provide a "medium" level of disclosure. Most companies "list cyber insurance as a mitigant to the financial exposure associated with cyber risk." See Moody's Investors Service, Sector In-Depth Cross Sector Report, "Cyber disclosures reveal varying levels of transparency across high-risk sectors," October 2, 2019, pp. 1, 3-4.

When appropriate public disclosure is lacking, it should not be a surprise when cost recovery is opposed by consumer advocates.

Figure 5. Constance Coram Protests Outside Duke Energy Shareholder Meeting.
Photo credit: Melissa Key, Charlotte Business Journal

The story of Duke Energy illustrates this problem. In January 2019, an unidentified utility was fined $10 million for 127 violations of cybersecurity standards, 126 of the violations being "ongoing" and one having been mitigated in August of 2017. [22] A February 2019 *Wall Street Journal* article exposed the standards violator as Duke Energy.[23] According to the Notice of Penalty, standard violations by Duke Energy go back as far back as January 23, 2017.

In April of 2017, Duke Energy proposed a $13 billion, 10-year plan to modernize the North Carolina electric grid, including protecting against cybersecurity and physical threats. After opposition by environmental groups, the plan was scaled back to $2.5 billion, 3-year

[22] FERC Docket NP19-4-000.
[23] Rebecca Smith, "Duke Energy Broke Rules Designed to Keep Electric Grid Safe," *Wall Street Journal*, February 1, 2019. https://www.wsj.com/articles/duke-energy-broke-rules-designed-to-keep-electric-grid-safe-11549056238

plan.[24] Had the record of cybersecurity problems at Duke been available to the North Carolina Utilities Commission at the time of the utility's grid modernization proposal, the rate case for fixes would have been far stronger.[25]

SECRECY VIOLATES SECURITIES AND EXCHANGE COMMISSION GUIDELINES

FERC's secret regulatory system is out of step with other regulatory processes in our democratic and capitalist society. On February 21, 2018, the Securities and Exchange Commission voted unanimously to approve guidance for public companies in disclosing cybersecurity risks ("SEC Guidance"). The Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 CFR Parts 229 and 249, became applicable on February 26, 2018. According to the U.S. Energy Information Administration, 72% of Americans get their electricity from investor-owned utilities under SEC jurisdiction.[26]

In its guidance, the SEC stated why it is important for public companies to make timely disclosures on cybersecurity risks and incidents:

---

[24] ScottMadden Management Consultants, "What's Next for Duke Energy's North Carolina Grid Modernization Plan?" www.scottmadden.com, Undated. Accessed at https://www.scottmadden.com/insight/whats-next-duke-energys-north-carolina-grid-modernization-plan/

[25] The North Carolina PUC found, "Turning now to the issues presented in the instant proceeding, the Commission finds and concludes that the reasons DEC says underlie the need for Power Forward are not unique or extraordinary to DEC, nor are they unique or extraordinary to North Carolina. Weather, customer disruption, physical and cyber security, DER, and aging assets are all issues the Company (and all utilities) have to confront in the normal course of providing electric service. The Commission further finds and concludes that while DEC intends to expend significant funds for T&D projects over the next ten years, a number of the Power Forward programs and projects proposed by DEC to be recovered through the Grid Rider are the kinds of activities in which the Company engages or should engage on a routine and continuous basis." See State of North Carolina Utilities Commission, "In the Matter of Application of Duke Energy Carolinas, LLC, for Adjustment of Rates and Charges Applicable to Electric Utility Service in North Carolina," Docket No. E-7, SUB 1146, July 25, 2017. Accessed at https://starw1.ncuc.net/NCUC/ViewFile.aspx?Id=80a5a760-f3e8-4c9a-a7a6-282d791f3f23

[26] David Darling and Sara Hoff, "Investor-owned utilities served 72% of U.S. electricity customers in 2017," U.S. Energy Information Administration, August 15, 2019. Available at: https://www.eia.gov/todayinenergy/detail.php?id=40913

Given the frequency, magnitude and cost of cybersecurity incidents, the Commission 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. Crucial to a public company's ability to make any required disclosure of cybersecurity risks and incidents in the appropriate timeframe are disclosure controls and procedures that provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents.

The SEC recognized that appropriate disclosure need not contain a roadmap for potential attackers:

This guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts – for example, by providing a "roadmap" for those who seek to penetrate a company's security protections. We do not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident. Nevertheless, we expect companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences.

Adherence to FERC's secret regulatory system could place company officials in violation of laws on insider trading. The SEC Guidance states:

> *It is illegal to trade a security "on the basis of material nonpublic information about that security or issuer, in breach of a duty of trust or confidence that is owed directly, indirectly, or derivatively, to the issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information. As noted above, information about a company's cybersecurity risks and incidents may be material nonpublic information, and directors, officers, and other corporate insiders would violate the antifraud provisions if they trade the company's securities in breach of their duty of trust or confidence while in possession of that material nonpublic information.*

It is notable that on February 28, 2018, PG&E was fined $2.7 million for violations of reliability standards but the identity of PG&E was concealed in the Notice of Penalty. in its 2018 10-K disclosure to the SEC, PG&E did not disclose the underlying cybersecurity breach that occurred in 2016, nor did it disclose the penalty imposed in 2018.

The identity of PG&E as a repeat violator of reliability standards became definitively known on August 24, 2018 through Freedom of Information Act requests by Michael Mabee, a private citizen and subsequent reporting by the *Wall Street Journal*. It appears that PG&E may have violated SEC guidelines by not disclosing its standards violations. PG&E executives trading its stock when its status as a violator was not publicly known may be guilty of insider trading.

SECRECY PREVENTS SOCIETAL CORRECTIONS

Perhaps the most significant disadvantage of concealing the record of standard violations is the prevention of societal corrections outside of the FERC-NERC regulatory system. When the capital markets lack timely information, they cannot discipline investor-owned utilities through declines in their stock price and bond ratings (and declines in the value of stock options for utility executives.)[27] When insurance underwriters lack information, they cannot raise rates or withdraw coverage for imprudent utilities.[28] And when state utility commissions lack information, they cannot adjust tariffs to motivate better behavior.[29]

PG&E is a case study of opportunities lost. If timely information had been available a decade earlier on PG&E's vegetation practices for high voltage transmission lines—including the full record of audits (or lack of audits)—the capital markets might have disciplined this firm

[27] For example, the former risk officer of the U.S. Department of Energy led a multi-author report on the financial impacts of the wildfire liabilities and PG&E bankruptcy on energy utility equity prices. See John J. MacWilliams, Sarah La Monaca, and James Kobus, PG&E: Market and Policy Perspectives on the First Climate Change Bankruptcy, Columbia Center on Global Energy Policy, August 2019. For other assessments of cyber risks to various sectors of the U.S. and global economy, see Moody's Investors Service, "Credit implications of cyber risk will hinge on business disruptions, reputational effect," February 28, 2019, at p. 3, finding that disruption events have a greater impact on financial markets than cyber data disclosures. A more fulsome and publicly-released database on cyber incidents is likely to improve risk modeling by credit rating firms. See Lesley Ritter, "The Financial and credit Implications of Cyber Risk," Moody's Investors Service, PowerPoint, EnergyTech 2019, Cleveland, Ohio, October 24, 2019. 11 pp. For a review of a wide range of naturally-occurring, weather-related risks to the pricing of energy equities, see Andre Bertolotti, Debarsh Basu, Kenza Akallal, and Brian Deese, "Climate Risk in the US Electric Utility Sector: A case study," New York: BlackRock Sustainable Investing, Working Paper, March 2019. 27 pp.

[28] For a review of potential financial losses due to cybersecurity vulnerabilities of the U.S. electric grid, see Lloyd's and the University of Cambridge Centre for Risk Studies, "Business Blackout: The insurance implications of a cyber attack on the US power grid," Judge Business School, London, 2015.

[29] The Commission may note that several state public utility commissions have filed in Docket AD19-08-000, seeking notifications respecting Notice of Penalties for electric utilities that operate in their respective states and affect vital interests of those state regulators.

much earlier. Instead, PG&E's management practices contributed to catastrophic fires, resulting in its bankruptcy.[30]

Figure 6. Graphic Showing Decline in PG&E Stock Price.
Graphic credit: Bay Area News Group

TIMELY PROPOSAL FOR REFORM OF THE NOTICE OF PENALTY REPORTING SYSTEM

Before the retirement of FERC Commissioner Cheryl LaFleur in August 2019, FERC initiated a joint NERC-FERC review of the Notice of Penalty reporting system. Between year 2007 and July 2010, the FERC-approved system had publicly identified "Registered Entities"

[30] See S&P Global Ratings, "Will California Still Have an Investment-Grade Investor-owned Electric Utility?" Report, February 19, 2019, 7 pp.

which were fined for violation of reliability standards.[31] Shortly before Commissioner LaFleur became a FERC Commissioner, the Commission reversed its policy. Between July 2010 and the present, the Commission has concealed the identity of "Registered Entities" fined for violating cybersecurity standards, and sometimes other standards as well.

On August 27, 2019 FERC published a White Paper jointly prepared by FERC and NERC staff. The White Paper proposes a new process—to publicly name the violator of all reliability standards and disclose the amount of penalty assessed, but only after the mitigation is complete and the Notice of Penalty filed with FERC. This proposed process would purportedly reduce "the risk of inadvertent disclosure of public information" by withholding details and significance of the violations. The process would use the "Critical Energy Infrastructure Information" exemptions allowed under the FAST Act, now Section 215A of the Federal Power Act.[32]

Outgoing Commissioner LaFleur, in a Statement accompanying release of the Joint White Paper recognized that "state regulators, members of the public, and others have a legitimate interest in such violations…." She also encouraged "suggestions for alternative processes."[33]

[31] FERC Order No. 672 (February 3, 2006) proposed that level of transparency in promulgating its criteria for reliability standards and procedures for enforcement. Exceptions to transparency might be allowed for certain cybersecurity incidents.
[32] FERC Docket AD19-18-000, Joint White Paper, released August 27, 2019. Joint Staff White Paper on "Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards."
[33] Commissioner Cheryl LaFleur, "Statement on FERC/NERC Staff White Paper on CIP Standards Notices of Penalties," August. 27, 2019.

OUR EVALUATION OF THE FERC-NERC WHITEPAPER PROPOSAL

The White Paper proposal as is currently drafted, suffers from potentially fatal flaws. If implemented as is, the procedures in the White Paper could be a major step backwards.

The White Paper proposes, for the first time, the withholding from public visibility the specific "Requirements" within a Reliability Standard that have been (or are) being violated.[34] This would preclude public tracking of specific requirement violations for registered entities individually, by a class of entities within NERC regions; and by each of the four Interconnections. As a foreseeable result, the public may become aware of adverse compliance trends only after a series of catastrophes occur.

Under the White Paper proposal, NERC would submit Notices of Penalty for cybersecurity standard violations "only after mitigation of the underlying violation is completed." This would give utilities a perverse incentive to delay mitigations to forestall their identification as a standards violator. Examination of past violations shows that regulators can allow years to pass between when a violation is first detected and when it is mitigated.

Utilities could even obtain indefinite delays in public disclosure by asking NERC for a Technical Feasibility Exception (TFE). The acceptable reasons for obtaining a TFE are many, including "scarce technical resources" and "incurrence of costs that, in the determination of the Regional Entity, far exceed the benefits to the reliability of the Bulk Electric System…" Significantly, "a TFE Request may be approved without a specified Expiration Date."[35]

---

[34] See Joint White Paper, *ibid.*, at p. 3: The NERC and FERC staffs propose that the Revised Notice of Penalty "discloses the name of the violator, the Reliability Standard(s) violated (but not the Requirement), and the penalty amount."

[35] North American Electric Reliability Corporation, "APPENDIX 4D TO THE RULES OF PROCEDURE; PROCEDURE FOR REQUESTING AND RECEIVING TECHNICAL FEASIBILITY EXCEPTIONS TO NERC CRITICAL INFRASTRUCTURE

Approval and use of TFE's by utilities to excuse compliance with reliability standards is surprisingly common. On June 30, 2018, TFEs accounted for 16,704 unique assets across NERC, including two TFEs approved by the Western Electric Coordinating Council that accounted for 7,608 assets. Across NERC, the average number of TFE per registered entity (or regulated utility) was five.[36]

The public should take little comfort from the statement in the White Paper, "Because most violations are fully mitigated before submission of the NOP, we do not expect a backlog to result." We knew that FERC has routinely tolerated lengthy delays in filing of the Notices of Penalties, which is one of the reasons that violations are often mitigated by the time of submission.

Rather than rely on the White Paper's hopeful expectations, we decided to do database analysis of backlogs in standards enforcement. While we cannot determine from searchable data the dates that violations are detected, we can use the NERC Searchable NOP Spreadsheet[37] to find the first and last mitigation dates for each Notice of Penalty. We can also find the date the Notice of Penalty was filed. Our analysis displayed in Table 1 reveals lengthy delays in processing of some Notices of Penalty. The examples we list below all have penalties of $100,000 or more and delays of at least one year:

PROTECTION STANDARDS," April 1, 2016, pp. 5-6. Available at https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/ROP_App_4D_Rev_CIPV5_07172015_clean.pdf

[36] North American Electric Reliability Corporation, "ANNUAL REPORT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION ON WIDE-AREA ANALYSIS OF TECHNICAL FEASIBILITY EXCEPTIONS," September 28, 2018, pp. 13, 15. Available at https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Final%20TFE%20Annual%20Report%202018.pdf

[37] North American Electric Reliability Corporation, "Searchable NOP Spreadsheet," September 26, 2019. Available at https://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx. Accessed October 23, 2019.

Table 1. Delays in CIP Violation Mitigation and Notice of Penalty Filing

Docket_Number	NERC Region	Registered_Entity_Name	Total Penalty	First Mitigation Date	Last Mitigation Date	NOP Date	Mitigation Months	Filing Months
NP15-33-000	RF	Unidentified Registered Entity	$425,000	2013-04-16	2015-05-22	2015-08-31	25	28
NP16-10-000	RF	Unidentified Registered Entity	$150,000	2013-01-01	2015-07-15	2016-01-28	30	36
NP16-12-000	RF	Unidentified Registered Entity	$1,700,000	2014-06-06	2016-02-16	2016-02-29	20	20
NP16-23-000	SERC	Unidentified Registered Entity	$225,000	2013-10-31	2016-03-11	2016-07-28	29	33
NP16-24-000	SERC	Unidentified Registered Entity	$180,000	2014-09-23	2016-04-28	2016-07-28	19	22
NP16-5-000	WECC	Unidentified Registered Entity	$200,000	2013-04-23	2015-08-27	2015-12-01	28	32
NP17-2-000	WECC	Unidentified Registered Entity	$1,125,000	2013-07-12	2015-12-05	2016-10-31	29	39
NP17-31-000	SERC	Unidentified Registered Entity	$500,000	2013-09-06	2018-12-31	2017-09-28	63	48
NP18-14-000	RF	Unidentified Registered Entity	$180,000	2016-02-01	2017-10-31	2018-05-31	20	27
NP18-25-000	SERC	Unidentified Registered Entity	$220,000	2016-08-22	2018-10-18	2018-08-30	26	24
NP19-10-000	XXXX	Unidentified Registered Entity	$1,000,000	2015-12-14	2018-12-31	2019-05-30	36	41
NP19-11-000	XXXX	Unidentified Registered Entity	$1,000,000	2017-10-10	2018-12-31	2019-05-30	14	19
NP19-14-000	SERC	Unidentified Registered Entity	$775,000	2016-10-26	2019-04-19	2019-06-27	30	32

Data Source: NERC Searchable Notice of Penalty Spreadsheet, September 26, 2019.

In summary, under the FERC/NERC White Paper proposal, many years could pass before anyone outside the regulatory system learns the identity of utilities which violate reliability standards and when their violations occurred. Instead, FERC should release identity of standards violators shortly after the violation occurs and is detected, because this will motivate the utility to make fixes quickly. FERC should no longer tolerate delays of months or years in mitigating vulnerabilities, negotiating Notices of Penalty, and filing the notices at FERC.

To inform investors, public utility commissions, and the public, it is not necessary to release details that could aid attackers, although in many cases potential attackers know vulnerabilities already. FERC should retain in the Notices of Penalties specific references to the enumerated "Requirements" in the CIP reliability standards, which enable state regulators, insurance and reinsurance companies, bond rating agencies, and financial analysts to better model and assess which of the "registered entities" pose above or below average risks to investors and to customers. Market signals can be more prompt and more powerful than can NERC fines by themselves.

Waiting years for utilities to make mitigations on their own timetable and even longer for a redacted Notice of Penalty to be filed at FERC keeps the public at risk.

A PUBLIC HEARING IS NECESSARY

A public hearing should examine the counterproductive rationales for concealment of the identity of utilities that violate reliability standards and how disclosure in the standards enforcement process can be improved. Such a hearing could call these potential witnesses:

1. Commissioners of state public utility commissions, especially California.
2. Officials of the Securities and Exchange Commission.
3. Bond rating agencies.
4. Insurance underwriters.
5. Bankruptcy experts.
6. Experts on cybersecurity disclosure from the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security.
7. Experts on cybersecurity best practices from the National Institute of Standards and Technology.
8. Utility Consumer Advocates of the various states.
9. Nonprofits with expertise in electric grid regulation.
10. Victims of extended grid blackouts.

In this matter involving both economic losses and potential deaths from blackout, docket comments are no substitute for in-person testimony before the Commission.

CONCLUSION

Coverups have consequences, especially when they persist for long periods of time. Increasingly, the consequences of concealing the identity of utilities which violate reliability standards could be deaths from blackout. We have filed a Motion in this Docket asking the Commission to hold a Public Hearing or Technical Conference to improve processes for standards enforcement, including greater transparency. [38] We urge the Commissioners to conduct a public hearing and then reformulate its Notice of Penalty and disclosure processes.

The public, state regulators, insurance companies, financial investors, bond rating agencies, and technology innovators need to promptly learn which utilities are putting America at risk and which utilities are leaders on the pathway to reliable and resilient energy systems.

Respectfully submitted by:

Thomas S. Popik, President
thomasp@resilientsocieties.org

William R. Harris, Director and General Counsel
williamh@resilientsocieties.org

for the
Foundation for Resilient Societies
24 Front Street, Suite 203
Exeter, NH 03833
www.resilientsocieties.org

[38] See the Foundation for Resilient Societies' Motion filed in Docket AD19-18-000, Filing 20191023-5103 October 23, 2019.