

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation

Docket No. NP18-7

Motion to Intervene and Comment of Public Citizen, Inc. and The Utility Reform Network (TURN)

On March 30, 2018, the Commission issued a Notice that it was extending the time period for consideration whether to review the Notice of Penalty that NERC filed with the Commission on February 28, 2018 in Docket No. NP18-7.

Public Citizen, Inc. and The Utility Reform Network (TURN) submit this Motion to Intervene and Comment. We request that the Commission require public disclosure of the names of the utility and contractor at the center of the Notice of Penalty in this Docket, as publicly revealing the names of the offenders is necessary for the benefit of the public interest.

Motion to Intervene

Public Citizen is a not-for-profit, public interest research and advocacy organization representing the interests of our more than 400,000 members and supporters across the United States. Public Citizen frequently intervenes and comments in FERC dockets.

TURN is a not-for-profit, public interest advocacy organization representing the interests of residential customers of investor-owned gas, electric, telecommunications and water utilities serving end-use customers in California. For the past 40 years, TURN has intervened in proceedings at the California Public Utilities Commission on behalf of residential customers in a wide array of proceedings relating to utility cost recovery and ratemaking. TURN has approximately 20,000 individual members and regularly appears before state agencies, the Legislature, and the California Independent System Operator.

Background

The Notice of Penalty NERC filed with the Commission stems from a Settlement Agreement between the Western Electricity Coordinating Council (WECC) and an Unidentified Registered Entity (URE) regarding “serious and substantial” violations of the Critical

Infrastructure Protection NERC Reliability Standards [NERC Notice of Penalty, at Page 6]. The violations involve a third-party contractor hired by the URE, and the identity of this contractor is also kept secret in the NERC Notice of Penalty. These violations prompted a settlement agreement where the URE agreed to pay a \$2.7 million penalty. According to a media report, this penalty is described as “massive” and unprecedented, and represents by far the largest penalty ever assessed for a CIP reliability standard violation.¹

The only reason the WECC, NERC, the URE and the URE’s contractor even knew about the breach was because of the actions of an unrelated “white hat” hacker that uncovered the contravention and notified the URE. The URE only saw fit to initially “informally” notify the WECC of the white hat’s discovery, and then waited four months to finally file a formal report to the WECC [NERC Notice, at Page 3].

The URE’s cybersecurity violations created vulnerabilities that could have allowed hackers to gain “both physical and remote access” to its systems [NERC Notice, at Page 3]. In all, more than 30,000 records were left exposed on the public internet for 70 days, including Critical Cyber Assets [NERC Notice, at Page 3].

The Need for Public Disclosure of the Names of the Offenders

18 C.F.R. § 39.7(b)(4) states: “Each violation or alleged violation shall be treated as nonpublic until the matter is filed with the Commission as a notice of penalty . . . The disposition of each violation or alleged violation that relates to a Cybersecurity Incident or that would jeopardize the security of the Bulk-Power System if publicly disclosed shall be nonpublic unless the Commission directs otherwise” [emphasis added]. Public Citizen and TURN ask that the Commission direct the public release of the name of the URE and its contractor under 18 C.F.R. § 39.7(b)(4) for the reasons outlined below.

First, if the URE is an electric utility subject to state rate regulation, keeping its name secret may mean that the state regulatory commission with jurisdiction over the URE does not know about the violation and the assessed penalty. Keeping the identity of the URE non-public from state utility regulators and from customer intervenors participating in state utility commission proceedings could allow the URE to seek retail rate recovery for such costs. Absent

¹ Blake Sobczak and Sam Mintz, “Grid regulator issues 'massive' penalty over data exposure,” *E&E News*, March 5, 2018.

the knowledge of the violation, the state utility commission would be unable to assess whether these costs are properly recovered from ratepayers or should be borne by shareholders. This outcome would defeat the entire purpose of the Penalty by forcing ratepayers to absorb the costs of utility imprudence. Furthermore, to the extent that the URE submits cybersecurity-related rate recovery requests to state utility regulators, knowing a URE's track record on such issues may materially affect regulators' assessment of such requests.

Second, if media reports are accurate that the penalty is the largest ever on record for a cybersecurity-related offense, then it is in the public interest to reveal the identity of the violator. Concealing the name of the recipient of the largest fine in history sends a confusing message to the public that large penalties do not come with full accountability, as future violators may be able to similarly hide behind of the veil of anonymity.

Third, directing the public release of the name of the URE will not jeopardize cybersecurity, the security of the Bulk-Power System, or national security. The violations described in the NERC Notice of Penalty do not identify any current or recurring vulnerabilities; rather, they stem from the one-time actions of a URE contractor that improperly handled cybersecurity data. In fact, public release of the name of the URE could *improve* cybersecurity, as regulators and stakeholders could use such public information to better educate and prepare the URE and other utilities' practices. In general, the more information that regulators and the public have about violators, the better able we all are to learn from past mistakes and reduce the likelihood of future ones. But keeping state regulators and the public in the dark about the cybersecurity track record of our electric utilities may actually create a false sense of security, and reduce the likelihood of more public awareness and vigilance needed to protect cybersecurity.

Fourth, for similar reasons, the identity of the URE contractor should also be made public. Although the NERC Notice of Penalty does not apparently involve penalties for the unnamed contractor, the Notice details a significant role that the contractor played in causing the violations. Keeping the identity of the contractor non-public shields the company from any additional scrutiny of its track record from state regulators, consumer advocates and members of the public, particularly if the vendor has other, existing relationships with other utilities. Directing the public release of the name of the contractor will better equip state regulators and

the general public to help ensure the contractor maintains the highest standards for caretaking cybersecurity operations and data.

Fifth, public media reports appear to identify the name of the URE. A June 1, 2016 blog identifies PG&E as an electric utility that suffered an inadvertent exposure of cybersecurity data in circumstances that appear very similar to the one described in the NERC Notice of Penalty². A subsequent *E&E News* article interviews a “white hat” hacker who details violations by PG&E that are very similar to the ones described in the NERC Notice of Penalty.³ If the identity of the URE has already been publicly identified, than Commission action to direct the public release of the name of the URE would be a mere formality, and help alleviate any confusion about similarities between the data breach that identifies PG&E and a similar violation described in the NERC Notice of Penalty.

Respectfully submitted,

Tyson Slocum, Energy Program Director
Public Citizen, Inc.
215 Pennsylvania Ave SE
Washington, DC 20003
(202) 588-1000
tslocum@citizen.org

Matthew Freedman, Staff Attorney
The Utility Reform Network
785 Market St #1400
San Francisco, CA 94103
(415) 954-8084
matthew@turn.org

² <https://mackeeper.com/blog/post/231-pacific-gas-and-electric-database-exposed>

³ Blake Sobczak and Sam Mintz, “Grid regulator issues 'massive' penalty over data exposure,” *E&E News*, March 5, 2018.

Document Content(s)

NERCpenalty.DOCX.....1-4