Published on *The National Law Review* https://natlawreview.com

# Data Exposure by Vendor Leads to $2.7 Million NERC Penalty for Utility

Article By:

J. Daniel Skees

Arjun Prasad Ramadevanahalli

A seven-figure penalty reported by the North American Electric Reliability Corporation demonstrates the potentially severe consequences for electric utilities related to improper data handling practices and underscores the challenges in preventing and resolving unauthorized disclosures.

A public filing by the North American Electric Reliability Corporation (NERC) on February 28 reported that an unidentified electric utility agreed to pay a $2.7 million penalty to resolve violations of the Critical Infrastructure Protection (CIP) reliability standards related to the exposure of sensitive data. While settlement agreements resolving CIP violations are commonplace, associated penalties with seven-figure dollar amounts are rare, and are most often reserved for the most severe violations of the reliability standards, typically those related to system disturbances involving the loss of load.

**Background**

The Notice of Penalty resolved two violations of now-retired Reliability Standard CIP-003-3, which the utility self-reported after learning that some of its sensitive network infrastructure data may have been publicly exposed by a vendor. Under CIP-003-3, utilities were required to implement a minimum set of security management controls to protect their critical cyber infrastructure. As part of those mandatory controls, the subject utilities were required to implement information protection programs to classify and safeguard sensitive information—such as network topology diagrams, floor plans for IT centers, and asset security configurations—and appropriately manage access privileges to that sensitive information. CIP-011-2 replaced CIP-003-3 in July 2016 and contains largely identical requirements for the protection of sensitive cybersecurity-related information, making these issues highly relevant to utilities today.

The violations in this case stemmed from improper data handling practices by the utility and its vendor, leading to the exposure of sensitive utility data on a public server. According to the Notice of Penalty, a third-party vendor improperly copied sensitive data from the utility's network to its own network environment. Once on the vendor's network, this information was no longer visible to the utility or subject to its network security controls. More troubling, a subset of the data containing thousands of records, potentially including live IP addresses and host names for utility cyber assets,

was unsecured and publicly available from the vendor's network.

The issue was caused by the vendor's failure to comply with the utility's information protection program on which the vendor was trained. Although the utility did not directly cause the improper data handling—and indeed the violation resulted from vendor noncompliance with utility policies—the Western Electricity Coordinating Council (WECC) nevertheless concluded that the utility failed to adequately implement its information protection program, as required by CIP-003-3. In particular, WECC determined that the utility failed to properly classify the information with the appropriate sensitivity level under its information protection program, believing it was not necessary to do so because the data was part of a preproduction asset management system. In addition, WECC determined that the utility failed to manage access to the information as required by the standard because it did not ensure that the vendor protected the sensitive information after it was improperly copied from the utility's network.

The sensitive data remained exposed for a total of 70 days until it was reported to the utility by a third-party "white hat," a term that often refers to an individual who identifies security vulnerabilities with the intent to report and mitigate them. After discovery, further analysis of the vendor's system logs revealed unauthorized attempts to access the data by unknown IP addresses. As explained in the Notice of Penalty, the exposure of such sensitive information could have enabled a malicious actor to access the utility's network and install a latent malware that may have caused potential harm in the future. As a result, WECC determined that the utility's two CIP-003-3 violations posed a "serious" risk to the reliability of the bulk power system, a factor that undoubtedly contributed to the large penalty amount.

## Implications

In addition to highlighting the potential severity of improper data handling, the Notice of Penalty underscores the challenges facing entities that retain compliance responsibility for the actions of contracted third parties. The use of vendors is ubiquitous in the utility industry. However, using vendors does not absolve the utility for noncompliance created by the vendor's own actions or failures in the utility's cybersecurity and access management programs. In this instance, the utility had established an information protection program and trained its vendor, as required by the reliability standard. Nevertheless, the utility's networks were exposed to security and compliance risks due to the vendor's failure to adhere to the controls prescribed by the utility.

This instance also demonstrates the potentially time-consuming and costly steps both parties may be required to take to resolve a security incident. As part of its mitigation plan the utility required its vendor to shut down the server hosting the utility's sensitive information. In addition, the utility performed three different forensic analyses of the vendor's system to verify the extent to which its data was accessed during the time of the exposure.

Because of the difficulty in imposing comprehensive controls on sensitive information, a utility should ensure that its vendor contracts protect the utility from vendor-created noncompliance as much as practicable. Although there is no one-size-fits-all approach, provisions that require vendor compliance with utility security controls, obligate vendors to indemnify the utility for vendor-created noncompliance, and ensure vendor cooperation following a disclosure of utility information can be key to minimizing the harm and compliance risk to a utility from vendor-caused disclosures.

The risks created by vendors have continued to be a focus of cybersecurity regulators, and this penalty action underlines the seriousness of the threat. To address these concerns, earlier this year

the Federal Energy Regulatory Commission proposed to adopt a suite of reliability standards for managing cybersecurity risks in the supply chains for vendor products and services. If adopted, the reliability standards will also require utilities to address a suite of cybersecurity risks in their procurement contracts. As a result of these new requirements, vendors will likely need to demonstrate that they can assist electric utilities in meeting their compliance obligations, even though only the utilities themselves would be subject to the standards and could be fined for noncompliance.

Copyright © 2025 by Morgan, Lewis & Bockius LLP. All Rights Reserved.

National Law Review, Volume VIII, Number 71

Source URL:https://natlawreview.com/article/data-exposure-vendor-leads-to-27-million-nerc-penalty-utility