

September 8, 2009

North American Reliability Corporation  
Attention: Sara Minges ([sara.minges@nerc.net](mailto:sara.minges@nerc.net))  
116-390 Village Blvd. Princeton, NJ 08540

Re: Comments of Encari, LLC in Response to NERC's Request for Comments on Proposed Procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standards and Related Amendments to NERC Rules of Procedure ("Proposed Final TFE Procedure")

In response to the North American Reliability Corporation's (NERC) request dated August 25, 2009 for comments on its Proposed Final TFE Procedure, Encari respectfully submits these comments.

## Summary of Encari's Comments

1. The term "operationally feasible" appearing in Section 3.1 of Appendix 4D to the Rules of Procedure should be defined in Section 2.0 of Appendix 4D to the Rules of Procedure .
2. Pending TFE Requests submitted under NERC's Interim Compliance Process Bulletin #2009-006 "Interim Approach to Technical Feasibility Exceptions" (Interim Approach) should be reviewed under the standards set forth in the Interim Approach.
3. Include an automatic TFE exception under CIP-007-1, R4 and R4.1 for non-programmable network devices.
4. Include an automatic TFE exception under CIP-007-1, R5.3 for non-programmable network devices.
5. CIP 004-1, R3 should be included among the Applicable Requirements listed in the Scope of Appendix 4D to the Rules of Procedure.

### 1. The term "operationally feasible" appearing in Section 3.1 of Appendix 4D to the Rules of Procedure should be defined in Section 2.0 of Appendix 4D to the Rules of Procedure.

While Section 3.1 of Appendix 4D allows for operational feasibility as a basis for approval of a technical feasibility exception ("TFE"), no definition of "operationally feasible" is provided in Appendix 4D. This omission perpetuates the ambiguity that the Federal Energy Regulatory Commission ("Commission") sought to eliminate in directing NERC to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception.

The Commission directed the ERO (i.e., NERC) to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the Critical Infrastructure Protection (CIP) Reliability Standards.<sup>1</sup> In so doing, the Commission stated, "We are persuaded by commenters that the proposed conditions for invoking the technical feasibility exception should allow for operational considerations."<sup>2</sup> The Commission emphasized, "We thus believe it is important to clarify that the meaning of 'technical feasibility' should not be limited simply to whether something is technically possible but also whether it is technically safe and operationally reasonable."<sup>3</sup>

In the absence of a definition of "operationally feasible," Responsible Entities may mistakenly use this term to apply their "reasonable business judgment" which FERC expressly sought to eliminate as a factor in compliance with the NERC CIP Reliability Standards.

We recommend that “operationally feasible” be added to the list of defined terms in Section 2.0 and suggest adoption of the following definition:

Operationally feasible: May be dependent on human resource constraints, limitations imposed by physical facilities, conflict with one or more organizations that share ownership of an asset, or the impact on other legal requirements or government regulations. Reasonable business judgment is not a factor to be considered in determining whether Strict Compliance with an Applicable Requirement is operationally feasible.

## **2. Pending TFE Requests submitted under NERC’s Interim Compliance Process Bulletin #2009-006 “Interim Approach to Technical Feasibility Exceptions” (Interim Approach) should be reviewed under the standards set forth in the Interim Approach.**

The Proposed Final TFE Procedure provides unfair treatment of pending TFE Requests submitted under NERC’s Interim Compliance Process Bulletin #2009-006 “Interim Approach to Technical Feasibility Exceptions” (Interim Approach) after the Proposed Final TFE Procedure has been adopted and made effective.

The final program proposes in pertinent part, “Upon implementation by NERC and the Regional Entities of a final TFE process, any TFE requests that are pending under the interim program will be subject to substantive review under the final program.” In contrast, NERC led Responsible Entities to believe that the process in the Interim Approach would govern all TFE requests submitted pursuant to that approach. The Interim Approach express states at pages 4-5, that “**While obviously not currently in effect or binding**, the proposed Section 3.0 of Appendix 4D to the [Rules of Procedure] ... outlines a number of factors that could be taken into account in evaluating the appropriateness of a TFE [emphasis added].”

By subjecting pending TFE Request to the substantive review process under the final program, NERC is creating a requirement that retroactively changes the legal consequences of acts committed or the legal status of facts and relationships that existed prior to the enactment of the final program. This is akin to an “ex post facto law.” An ex post facto law generally possesses three characteristics: it is a criminal or penal measure, retrospective, and disadvantageous to the offender because it may impose greater punishment. Given the fines that may result following the denial of a TFE Request, TFE requests timely submitted under the Interim Approach should be evaluated under the Interim Approach procedures and not be made subject to standards for review under the final program.

Accordingly, we recommend that page 9 of the Proposed Final TFE Approach be modified as follows:

... On July 1, 2009, NERC issued interim guidance on how to process TFE requests. This interim guidance is available at [http://www.nerc.com/files/2009-006\\_Public%20Notice-V1.pdf](http://www.nerc.com/files/2009-006_Public%20Notice-V1.pdf). NERC and the Regional Entities intend to process TFE requests using the interim guidance until the final TFE process is approved by FERC and becomes effective. Upon implementation by NERC and the Regional Entities of a final TFE process, only TFE requests that are pending under the interim program will be subject to substantive review under the interim program. All subsequent TFE requests shall be subject to substantive review under the final program.

## **3. Include an automatic TFE exception under CIP-007-1, R4 and R4.1 for non-programmable network devices.**

There should be an automatic TFE exception under CIP-007-1, R4 and R4.1 for non-programmable network devices. Currently, many Responsible Entities utilize nonprogrammable hubs or switches in their control or data acquisition system networks. As a consequence, these devices are required to maintain anti-virus and malware protection software under CIP-007-1, R4 and R4.1. Yet, it is technically infeasible for non-programmable devices such as hubs and switches to accept anti-virus or malware protection software. They are not programmable and cannot benefit from anti-virus or malware protection software. Since these devices cannot be compromised by a cyber attack and merely pass traffic according to hardware level configurations, no purpose is served by requiring a TFE for these devices owing to their absence of anti-virus and malware protection software.

#### **4. Include an automatic TFE exception under CIP-007-1, R5.3 for non-programmable network devices.**

There should be an automatic exception under CIP-007, R5.3 for non-programmable network devices that cannot accept and do not have the need for a password. Currently, many Responsible Entities utilize nonprogrammable hubs or switches in their control or data acquisition system networks. As a consequence, these devices are required to use a password under CIP-007-1, R5.3. Yet, it is technically infeasible for passwords to be required for non-programmable devices such as hubs and switches. They are not programmable and cannot benefit from password protection. Since these devices cannot be compromised by a cyber attack and merely pass traffic according to their hardware level configurations, no purpose is served by requiring a TFE for these devices owing to their absence of password protection.

#### **5. CIP 004-1, R3 should be included among the Applicable Requirements listed in the Scope of Appendix 4D to the Rules of Procedure.**

CIP-004-1, R3 raises an issue of operational feasibility and, therefore, should be eligible for treatment as a TFE. In pertinent part, the requirement provides "The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access." The "subject to" clause gives rise to a potential exception to the requirement. FERC has observed that exceptions may be recognized, not only for technical feasibility reasons, but also for operational considerations, and in this case a collective bargaining agreement may constitute an operational consideration that bars a Responsible Entity from implementing the requirement under CIP-004, R3.

The requirement under CIP-004, R3 is not identified as an Applicable Requirement in the list appearing in the Scope of Appendix 4D to the Rules of Procedure, leaving Responsible Entities who invoke an exception under the requirement subject to audit uncertainty and risk of non-compliance. Exceptions under CIP-004, R3 are deserving of safe harbor treatment in the same manner as exceptions invoked under the Applicable Requirements are accorded safe harbor treatment under Section 5.3 of Appendix 4d to the Rules of Procedure.

Respectfully,

Mark Simon  
Senior Information Security Consultant  
msimon@encari.com

---

<sup>1</sup> FERC Order 706, par. 178.

<sup>2</sup> Id.

<sup>3</sup> FERC Order 706, par. 182.

