

April 23, 2013

## Out With the Old, in With the New – CIP Version 5 on the Horizon

Electric utilities and other generation and transmission companies will be subject to new cybersecurity standards under a proposed rule issued by the Federal Energy Regulatory Commission (FERC). FERC proposed to approve the long-awaited Version 5 of the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Reliability Standards, which will overhaul the CIP regulatory framework and trigger new and revised compliance obligations for many users, owners and operators of the bulk electric system. While Version 5 establishes "a more robust cyber security posture for the industry," FERC seeks input on certain ambiguous aspects of Version 5. Industry participants should both start their internal compliance reviews with a view toward meeting the final, approved Version 5 and also consider submitting comments to FERC.

### Background

NERC is charged with developing Reliability Standards, enforceable upon FERC approval, to protect the reliability of the bulk electric system (BES),<sup>1</sup> including the CIP Reliability Standards. NERC's January 31, 2013, petition to FERC for approval of CIP Version 5 included 10 Reliability Standards containing 12 requirements with new cybersecurity controls, new and revised defined terms, violation risk factors and severity levels for assessing penalties for non-compliance, and an implementation plan.

Version 5 represents a drastic shift away from prior methodologies to identify assets subject to the cybersecurity requirements, including Version 4's "bright-line" approach for identifying Critical Assets and associated Critical Cyber Assets. Version 5 adopts a new classification approach that requires each regulated entity to identify its BES Cyber Assets (the only assets subject to Version 5), logically group these assets into BES Cyber Systems, and classify the systems based on their reliability impact (Low, Medium or High) on the bulk electric system. Each BES Cyber System at a minimum will be classified as Low Impact. NERC outlines specific criteria related to facility ratings (generation capacity and voltage levels) to identify an asset's reliability impact, focusing on the adverse impact that loss, compromise, or misuse of the BES Cyber System could have on the reliable operation of the bulk electric system. Once a responsible entity categorizes its BES Cyber Systems, it must then apply the CIP requirements associated with the impact level(s) identified.

### Implementation

FERC proposes to transition from Version 3 directly to Version 5, which would result in Version 4 never going into effect. However, FERC questions NERC's proposal to provide a 24-month implementation period for High and Medium Impact assets to comply with Version 5 and a 36-month period for Low Impact assets. NERC's petition did not provide adequate justification for the proposed implementation periods. FERC therefore requests comments on the necessity of these transition periods, whether they could be shorter, and what activities must be completed to transition to Version 5.

---

<sup>1</sup> In a rehearing order also issued April 18, FERC granted rehearing in part and otherwise reaffirmed its approval of a modified definition of "bulk electric system." See *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*, Order No. 773-A, 143 FERC ¶ 61,053 (2013).

© 2013 Sutherland Asbill & Brennan LLP. All Rights Reserved.

This communication is for general informational purposes only and is not intended to constitute legal advice or a recommended course of action in any given situation. This communication is not intended to be, and should not be, relied upon by the recipient in making decisions of a legal nature with respect to the issues discussed herein. The recipient is encouraged to consult independent counsel before making any decisions or taking any action concerning the matters in this communication. This communication does not create an attorney-client relationship between Sutherland and the recipient.

## “Identify, Assess, and Correct” Deficiencies

Seventeen of the Version 5 requirements instruct the regulated entity to “identify, assess, and correct” deficiencies. NERC explained that these requirements represent a performance expectation, not an enforceable element of Version 5. FERC found this language unclear as to both the regulated entity’s compliance obligations and the requirement’s enforceability as a Reliability Standard. For example, FERC was not sure whether an entity is obligated only to “identify, assess, and correct” deficiencies or if it must also comply with the underlying requirement. Additionally, NERC did not provide a time frame to identify, assess, and correct deficiencies, nor explain how prior deficiencies will factor into an entity’s compliance history. FERC also found the language overly vague and requested further clarity on the meaning of terminology used. Ultimately, FERC may direct NERC to modify this language or remove it entirely based on comments received.

## Low Impact Cybersecurity Protections

FERC found that proposed Requirement 2 of CIP-003-4, which is the only requirement applicable to Low Impact facilities, was ambiguous and could potentially result in inconsistent and inefficient Version 5 implementation. The requirement requires documented policies but fails to require implementation of substantive cybersecurity protections, and thereby provides an insufficient roadmap for protecting Low Impact BES Cyber Systems. FERC proposed to direct NERC to modify Requirement 2 to require that entities adopt specific, technically supported cybersecurity controls for Low Impact assets, as well as maintain a list of these assets.

## Protecting Communication Systems

FERC’s proposal highlights the need to protect communication systems. FERC supports adopting cryptography, including encryption and integrity checks, to further communication protections under Version 5. FERC took issue with NERC’s proposal to remove “communication networks” from the definition of Cyber Assets, which FERC viewed as effectively exempting communication networks from Version 5 oversight. FERC requests comments on whether these networks should be covered and if Version 5 adequately protects non-routable communication systems.

## Reliability Impact Categorization

FERC questions NERC’s proposed categorization methodology, which focuses on an asset’s reliability impact based on facility ratings, such as generation capacity and voltage levels. FERC is concerned that this approach does not address cybersecurity as comprehensively as the National Institute of Standards and Technology’s Risk Management Framework, which categorizes assets based on the loss of confidentiality, integrity, and availability of systems. While FERC opted not to require changes to this aspect of the petition, FERC may revisit NERC’s approach in the future.

## What It Means for You

FERC’s proposal to adopt Version 5 and skip Version 4 should provide welcome relief to regulated entities struggling to develop internal compliance plans. Still, regulated entities should not delay internal reviews to understand Version 5 and its impact on their compliance plans. Importantly, the

implementation period for complying with Version 5 may be shortened from what was expected in the Version 5 stakeholder process. Additionally, Low Impact assets should not be overlooked in the development of compliance plans because they may face a more structured and burdensome compliance obligation. The requirement to “identify, assess, and correct” deficiencies also may gain teeth in the final CIP Version 5 that is adopted. For these reasons, interested parties should consider submitting comments on FERC’s proposed approval of Version 5.



*If you have any questions about this Legal Alert, please feel free to contact the attorneys listed below or the Sutherland attorney with whom you regularly work.*

<a href="#">Daniel E. Frank</a>	202.383.0838	<a href="mailto:daniel.frank@sutherland.com">daniel.frank@sutherland.com</a>
<a href="#">Alison C. Graab</a>	202.383.0861	<a href="mailto:alison.graab@sutherland.com">alison.graab@sutherland.com</a>
<a href="#">Meghan R. Gruebner</a>	202.383.0933	<a href="mailto:meghan.gruebner@sutherland.com">meghan.gruebner@sutherland.com</a>
<a href="#">Jennifer J.K. Herbert</a>	202.383.0822	<a href="mailto:jj.herbert@sutherland.com">jj.herbert@sutherland.com</a>
<a href="#">Alexandra D. Konieczny</a>	212.389.5072	<a href="mailto:alexandra.konieczny@sutherland.com">alexandra.konieczny@sutherland.com</a>
<a href="#">Mark Thibodeaux</a>	713.470.6104	<a href="mailto:mark.thibodeaux@sutherland.com">mark.thibodeaux@sutherland.com</a>