Summary of FERC Order No. 791

On November 22, 2013, the Federal Energy Regulatory Commission ("FERC" or "Commission") issued Order No. 791 adopting a rule that approved Version 5 of the Critical Infrastructure Protection ("CIP") Reliability Standards ("CIP Version 5 Standards") as proposed by the North American Electric Reliability Corporation ("NERC") and directing NERC to develop modifications to those Standards to address FERC's concerns.

Modified and New Standards

The CIP Version 5 Standards include modifications to existing Standards CIP-002 through CIP-009 and new Standards CIP-010 and CIP-011. The biggest change in the CIP Version 5 Standards from the previous versions is that they require Responsible Entities to identify and categorize "BES Cyber Systems"[1] using a new methodology based on whether a BES Cyber System has a Low, Medium, or High Impact on the reliable operation of the bulk electric system. (At a minimum, a BES Cyber System must be categorized as a Low Impact asset.) Once a BES Cyber System is categorized, a Responsible Entity must comply with the associated requirements of the CIP Version 5 Standards that apply to that impact category.

Twelve new requirements were added to the Standards that contain new cyber security controls and extend the scope of the systems that are protected by the CIP Reliability Standards. The Commission also approved 19 new or revised definitions associated with the CIP Version 5 Standards for inclusion in NERC's Glossary of Terms.

[1] "BES Cyber System" is defined as "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." NERC defines "BES Cyber Asset" as follows:

> A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an [Electronic Security Perimeter ("ESP")], a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

Mandated Modifications

FERC directed NERC to develop the following modifications to the final rule and to conduct the survey described below:

1. "Identify, Assess, and Correct Deficiencies"

One of FERC's primary concerns is that language in the Standards requiring Responsible Entities to "identify, assess, and correct" deficiencies is unclear with respect to the obligations it imposes on Responsible Entities, how it would be implemented by Responsible Entities, and how it would be enforced. FERC directed NERC to remove that language from 17 requirements. NERC is to submit its proposal to address the Commission's concerns about that language within one year from the effective date of the final rule.

- FERC believes that the "identify, assess, and correct" language is "ambiguous and results in an unacceptable amount of uncertainty with regard to consistent application, responsible entities understanding their obligations, and NERC and the regions providing consistent application in audits and other compliance settings." [p. 40]

- While FERC understands that NERC's use of the "identify, assess, and correct" language is part of moving the compliance process towards a more risk-based model, FERC believes "that a more appropriate balance might be struck to address the underlying concerns by developing compliance and enforcement processes that would grant NERC and the Regional Entities the ability to decline to pursue low risk violations of the Reliability Standards." [p. 43] To accomplish this balance, FERC suggests modifying NERC's Compliance Monitoring and Enforcement Program.

2. Protections for Low Impact BES Cyber Systems

FERC directed NERC to develop modifications that address security controls for Low Impact assets. FERC finds fault with the CIP Version 5 Standards because they do not require specific controls for Low Impact assets and do not "contain clear, objective criteria from which to judge the sufficiency of the controls ultimately adopted by responsible entities for Low Impact BES Cyber Systems." [p. 62]

- To address that problem, FERC directed NERC to develop modifications to the CIP Version 5 Standards and suggested that NERC can effectively address their concern by:

    - requiring specific controls for Low Impact assets, including subdividing the assets into different categories with different defined controls applicable to each subcategory;

- developing objective criteria against which the controls adopted by Responsible Entities can be compared and measured in order to evaluate their adequacy, including subdividing the assets into different categories and different defined control objectives applicable to each subcategory;

- defining with greater specificity the processes that Responsible Entities must have for Low Impact facilities under CIP-003-5 R2; or

- using another equally efficient and effective solution. [pp. 62-63]

- FERC emphasized that whatever approach NERC decides to take, the criteria NERC proposes for evaluating a Responsible Entity's protections for Low Impact facilities should be clear, objective, commensurate with their impact on the system, and technically justified.

3. Risks Posed by Transient Devices

FERC directed NERC to develop requirements that protect transient electronic devices (*e.g.*, thumb drives and laptops) that fall outside of the definition of "BES Cyber Asset."[2] FERC believes that "there is a gap in the CIP [V]ersion 5 Standards regarding transient devices, and these devices pose a risk to BES Cyber Assets that is not addressed in an adequately robust manner in the CIP [V]ersion 5 Standards." [p. 79]

- FERC directed NERC to conduct a survey of Responsible Entities during the implementation of the CIP Version 5 Standards "to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because they do not satisfy the '15-minute' parameter." [p. 5]

- FERC also directed NERC "to submit an informational filing one year from the effective date of [the final rule] that assesses, based on the survey results, whether the BES Cyber Asset definition will, with the 15-minute parameter, cover the assets that are necessary to the reliable operation of the Bulk Power System."[3] [p. 5]

- FERC expressed concern about whether the CIP Version 5 Standards "provide adequately robust protection from the risks posed by transient devices" and

[2] The definition of "BES Cyber Asset" excludes transient devices by excluding Cyber Assets if for 30 consecutive calendar days or less, they are "directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes." [p. 67]

[3] In its filing, NERC is to explain the following: "(1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition." [p.73]

directed NERC "to develop either new or modified standards to address the reliability risks posed by connecting transient devices to BES Cyber Assets and Systems." [p. 77] The Commission expects NERC to consider the following security elements when designing a Reliability Standard for transient devices and removable media:

- the device authorization as it relates to users and locations;
- software authorization;
- security patch management;
- malware prevention;
- detection controls for unauthorized physical access to a transient device; and
- processes and procedures for connecting transient devices to systems at different security classification levels (*i.e.*, High, Medium, and Low Impact). [p. 79]

4. Protection of Communication Networks

FERC approved NERC's proposed modification to the definition of "Cyber Asset,"[4] which excludes communication networks. FERC expressed concern, however, that a gap in protection may exist because the CIP Version 5 Standards do not address security controls needed to protect the nonprogrammable components of communication networks. [p. 86] Thus, FERC directed NERC to create a definition of "communication networks" and to develop new or modified Reliability Standards to address that reliability gap and to submit those modifications to the Commission within one year from the effective date of the final rule. [p. 87] FERC also directed FERC's Staff to include this issue in a Staff-led technical conference.

Violation Risk Factors/Violation Severity Levels

FERC approved 30 of the 32 Violation Risk Factors ("VRF") proposed by NERC and directed NERC to modify the VRF assignment for CIP-006-5 R3 and CIP-004-5 R4 from Lower to Medium. [p. 98] For CIP-006-5 R3, FERC believes that the modification will ensure that the CIP Version 5 Standards will "afford similar treatment to the testing and monitoring of Physical Access Controls (PACS) as the CIP [V]ersion 4 Standards." [p. 101] FERC also believes that the modification is necessary for CIP-004-5 R4 "to reflect that access to operationally sensitive computer equipment should be strictly limited to employees or contractors who utilize the equipment in performance of their job responsibilities, and to prevent or mitigate disclosure of sensitive information . . . ." [p. 107]

FERC also directed NERC to modify the Violation Severity Levels for certain CIP Version 5 Standards to (1) remove the "identify, assess, and correct" language from the text of the VSLs for the affected requirements; (2) address typographical errors; and (3) clarify certain unexplained elements. [p. 113]

[4] The new definition of Cyber Asset is as follows: "Programmable electronic devices, including the hardware, software, and data in those devices."

Implementation Plan

The Commission approved NERC's proposed implementation plan for the CIP Version 5 Standards. As a result, CIP-002-4 through CIP-009-4 will not become effective, and CIP-002-3 through CIP-009-3 will remain in effect until the effective date of the CIP Version 5 Standards. There will be a 24-month implementation period for High and Medium Impact BES Cyber Systems and a 36-month implementation period for Low Impact BES Cyber Systems. The Commission also indicated support for NERC's proposal to develop transition guidance documents and a pilot program to assist Responsible Entities as they move from compliance with the CIP Version 3 Standards to the CIP Version 5 Standards.