Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 791
October 28, 2014

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
67 and 76	67. For the reasons discussed below, the Commission concludes that the "identify, assess, and correct" language, as currently proposed by NERC, 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. Accordingly, we direct NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements, while retaining the substantive provisions of those requirements.[1] Alternatively, NERC may propose equally efficient and effective modifications that address the Commission's concerns	The Standard Drafting Team (SDT) removed the "identify, assess, and correct" language from the following 17 Requirements in the CIP standards and their related Violation Severity Levels (VSLs): CIP-003-6, Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1.

[1] The 17 requirements are: CIP-003-5, Requirements R2 and R4; CIP-004-5, Requirements R2 through R5; CIP-006-5 Requirements R1 and R2; CIP-007-5, Requirements R1 through R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	regarding the "identify, assess, and correct" language.[2] The Commission directs NERC to submit the modifications to the CIP Reliability Standards within one year from the effective date of this Final Rule. 76. Accordingly, the Commission directs NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this Final Rule. Alternatively, NERC may develop a proposal to enhance the enforcement discretion afforded to itself and the Regional Entities, as discussed above.	
124	Accordingly, the Commission directs NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Such data	Based on comments and feedback from the draft proposed Section 1600 survey, NERC will no longer be issuing a Section

[2] *See Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, at P 186, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	will help provide a better understanding of the BES Cyber Asset definition. Based on the survey data, NERC should explain in an informational filing 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. The informational filing should not provide a level of detail that divulges CEII data. This filing should also help other entities implementing CIP version 5 in identifying BES Cyber Assets.	1600 data request and will be working with the six study participants in developing the information needed for its filing.
150	We direct NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the reliability gap discussed above. The definition of communications networks should define what equipment and components should be protected, in light of the statutory inclusion of communication networks for the reliable operation of the Bulk-Power System. The new or modified Reliability Standards	The proposed CIP-006-6 Requirement Part 1.10 requires the physical protection of nonprogrammable components of BES Cyber Systems existing outside of the PSP, and the proposed modifications to CIP-007-6 Requirement Part 1.2 include applicability for non-programmable electronic components to prevent unauthorized use of physical ports. These additional requirements address the gap in protection as discussed in the Order by ensuring the physical security for cabling and non-

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this final rule. We also direct Commission staff to include this issue in the staff-led technical conference discussed herein.3	programmable network components not covered by the definition of Cyber Asset. The drafting team reviewed the directives related to submitting a definition for communication network and determined it could address the gap in protection and adequately provide guidance on nonprogrammable electronic components without having a definition. Communication networks can and should be defined broadly. For example, NIST Special Publication 800-53 Revision 4 refers to the CNSSI 4009 definition of Network, which is "Information system(s) implemented with a collection of interconnected components." The requirements modifications as well as the existing requirements have more targeted components. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards.
181 and 184	181. The Commission also supports 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.4 The Commission agrees	NERC modified the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium and filed the revision with FERC on 5/15/2014.

[3] *See infra* P 223.

[4] *See* NERC Comments at 39-40.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	that a pilot program will assist responsible entities by offering best practices and lessons learned during this transition. 184. Consistent with our discussion above, the Commission directs NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium, within 90 days of the effective date of this Final Rule.	
192 and 196	192. The Commission adopts the NOPR proposal and directs NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium. This modification is necessary 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 consistent with Recommendations 40 and 44 of the 2003 Blackout Report. In addition, a Medium VRF assignment ensures consistency with the Commission's VRF guidelines. 196. Consistent with the discussion above, we direct NERC to modify the VRF assignment for CIP-004-5,	NERC modified the VRF assignment for CIP-004-5.1, Requirement R4 from Lower to Medium and filed the revision with FERC on 5/15/2014.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	Requirement R4 from Lower to Medium, within 90 days of the effective date of this Final Rule.	
205	Consistent with the NOPR proposal, we direct NERC to develop modifications to the VSLs for certain CIP version 5 Standard requirements 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. For the VSLs that include "identify, assess, and correct" language, we direct NERC to ensure that these VSLs are modified to reflect any revisions to the requirement language in response to our directives. We grant NERC the discretion to decide how best to address these modifications be it through an errata filing to this proceeding or separate filing.	In conjunction with the SDT's response to the directive in PP 67 and 76, the SDT removed the "identify, assess, and correct" language from the following 17 Requirements' VSLs: CIP-003-6, Requirements R2 and R4; CIP-004-6, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-6, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-2, Requirements R1 and R2; and CIP-011-2, Requirement R1. NERC filed the following revisions with FERC on 5/15/2014: 1. **VSLs for CIP-003-5, Requirements R1 and R2**. This standard addresses security management controls for cyber security. Requirement R1 governs management approval of policies on topics addressed in other CIP standards for medium and high impact BES Cyber Systems. Requirement R2 governs policies for low impact BES Cyber Systems. NERC staff, in consultation with the SDT, revised the VSLs in CIP-003-5, Requirements R1 and R2 to eliminate redundant language.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		2. **VSLs for CIP-004-5.1, Requirement R4**. This standard includes requirements for personnel and training related to cyber security. Requirement R4 governs implementation of access management programs. NERC staff, in consultation with the SDT, revised the VSLs to a percentage-based gradation. 3. **Severe VSL for CIP-008-5, Requirement R2**. This standard addresses incident reporting and response planning for cyber security. Requirement R2 governs implementation of documented Cyber Security Incident response plans. NERC staff revised the Severe VSL to reduce a gap in months between the High VSL and Severe VSL. 4. **VSLs for CIP-009-5, Requirement R3**. This standard addresses recovery plans for BES Cyber Systems. Requirement R3 governs maintenance of the recovery plans. NERC staff revised the timeframe contained in the VSLs from 90-210 days to 90-120 days.