Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 791

January 23, 2015

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-003-7, Requirements R2 and R4; CIP-004-7, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-7, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-3, Requirements R1 and R2; and CIP-011-3, Requirement R1.

[1] The 17 requirements are: CIP-003-5, Requirements R2 and R4; CIP-004-5.1, 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.	
106	Based on the explanations provided by NERC and other commenters, we adopt the NOPR proposal with modifications. As we explain below, while we do not require NERC to develop specific controls for Low Impact	The SDT revised Requirements R1 and R2 of CIP-003-7 to include additional specificity regarding the processes that responsible entities must have for low impact BES Cyber Systems. In addition, the SDT developed objective criteria

[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**
	facilities, we do require NERC to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact assets. While NERC may address this concern by developing specific controls for Low Impact facilities, it has the flexibility to address it through other means, including those discussed below.	surrounding the controls for some entities based on asset-type and routable communications. The SDT determined that the additional specificity and objective criteria address FERC's concerns while maintaining the flexibility in controls necessary for such a diverse array of assets in the low impact category. To better define the protection required for low impact BES Cyber System electronic communication, the terms Low Impact BES Cyber System External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) have been added to the NERC Glossary of Terms. These help define the concept of security controls targeted for communication paths at a facility-site level. The SDT confined these revisions in CIP-003-7, Requirements R1 and R2 to the following areas: 1. **Cyber Security Policy:** R1.2 requires a policy addressing the four cyber security subject matter areas specified in the R2 cyber security plan. 2. **Cyber Security Plan(s):** R2 requires the development and implementation of one or more cyber security plan(s) for an entity's low impact BES Cyber System(s).

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		The cyber security plan must cover the 4 areas as specified in Attachment 1 of CIP-003-6: a. **Cyber Security Awareness:** Attachment 1, Section 1 requires responsible entities to implement a security awareness program with timeframes to reinforce cyber security practices. The SDT determined that adding intervals increases the auditability of the requirement part. b. **Physical Security Controls:** Attachment 1, Section 2 and its subparts require physical access controls to low impact BES Cyber Systems as well as Low Impact BES Cyber System Electronic Access Points (LEAP) used for controlling access as specified in Section 3. c. **Electronic Access Controls:** Attachment 1, Section 3 and its subparts address protections around Low Impact BES Cyber System External Routable Connectivity (LERC) and Dial-up Connectivity. d. **Cyber Security Incident Response:** Attachment 1, Section 4 and its subparts outline the criteria required to be in a Cyber Security Incident response plan.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
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 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.	Based on comments and feedback from the draft proposed Section 1600 survey, NERC will no longer be issuing a Section 1600 data request and will be working with the six study participants in developing the information needed for its filing.
132	Based on the explanation provided by NERC and other commenters, we will not direct modifications regarding the 30-day exemption in the definition of BES Cyber Asset. While we are persuaded that it	The threat of connecting transient devices to BES Cyber Systems is addressed in the Reliability Standards through an additional requirement in CIP-010, which requires a Transient Cyber Asset

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	would be unduly burdensome for responsible entities to treat all transient devices as BES Cyber Assets, we remain concerned whether the CIP version 5 Standards provide adequately robust protection from the risks posed by transient devices. Accordingly, as discussed below, we direct NERC to develop either new or modified standards to address the reliability risks posed by connecting transient devices to BES Cyber Assets and Systems.	and Removable Media plan to provide higher assurance against the propagation of malware when connecting transient devices. The terms Transient Cyber Asset and Removable Media have been added to the glossary to define transient devices. In addition, the terms BES Cyber Asset and Protected Cyber Asset have been modified to reference the new Transient Cyber Asset definition. The drafting team determined three distinct scenarios for entities to address in their plan(s) in which transient devices need specific protections: (i) Transient Cyber Assets managed by the Responsible Entity, (ii) Transient Cyber Asset(s) managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media. For Transient Cyber Assets managed by the Responsible Entity, the SDT determined that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices while others have a checklist for transient devices prior to connecting them to a BES Cyber System. The drafting team acknowledges both methods are valid and has drafted requirements that permit either form of management. The controls for this scenario are

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		more specific and recognize the relatively higher frequency in which these devices will be used. In the scenario in which a party other than the Responsible Entity manages the Transient Cyber Assets, the required sections of the plan include those which an entity can verify at the point prior to connecting such as security patch management and malware prevention mechanisms. The security controls entities must apply to Removable Media have considerations for the type of device being protected and include authorization and scanning for malicious code. The Commission provided a list of security controls it expected NERC to consider for addressing transient devices. The consideration of each security section is described as follows: 1. **Device authorization as it relates to users and locations:** CIP-010-3 Requirement R4, Attachment 1 requires entities to authorize Transient Cyber Assets and Removable Media by user(s), location(s) and use prior to connecting them to the BES Cyber System. Transient Cyber Assets managed by another party do not have this authorization because the scenario is often single-use and the entity already conducts an inspection and mitigation of the device prior to connection.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		2. Software authorization: The SDT considered controls relating to software authorization but decided against including specific software as part of the authorization performance because such authorization did not contribute meaningfully to cyber security risk reduction. However, software authorization in the form of application whitelisting is provided as an option to mitigate malicious code. **3. Security patch management:** In CIP-010-2 R4, Attachment 1, both entity and vendor/contractor managed devices must have security patch management or other equivalent forms of mitigation to address security vulnerabilities in software. 4. **Malware prevention:** CIP-010-2 Requirement R4, Attachment 1 requires entities to have malware protection on the Transient Cyber Asset (for both entity- and vendor-managed Transient Cyber Assets) and for Removable Media prior to connection. 5. **Detection controls for unauthorized physical access to a transient device:** The drafting team considered this control and determined this control best applies to entity-managed Transient Cyber Assets with the objective to mitigate the risk of unauthorized use. There are logistical challenges in applying this control to vendor-managed devices, in which the entity likely will

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		have had no control until immediately prior to use. Furthermore, additional guidance is necessary in CIP-011-3 to ensure entities recognize the importance of safeguarding BES Cyber System Information on transient devices. The objective to address the unauthorized release of BES Cyber System Information is sufficiently addressed with the requirements in CIP-011-3 to protect and securely handle BES Cyber System Information. 6. **Processes and procedures for connecting transient devices to systems at different security classification levels (i.e. high, medium, low impact):** The drafting team has considered this control and believes the threat of connecting at multiple impact levels is sufficiently addressed through the proposed Reliability Standards. Rigorous security assessment and controls between classification levels have significant importance to secure authorized information flows. However, connections between impact levels do not carry the same threat for BES Cyber Systems. The flow of BES Cyber System Information is addressed sufficiently through CIP-011-3 requirements. The more concerning threat involves transient devices connecting between BES Cyber Systems and external networks, and this threat is addressed in the proposed CIP-010-3 Requirement R4.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
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 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	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-007-7 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-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." However, the scope of the requirements modifications as well as the existing requirements has more targeted components than the broad concept of

[3] *See infra* P 223.

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		communication networks. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards. The decision to meet the directive without defining the term communication networks does not imply the absence of protection for communication networks components nor do the additional requirements associated with nonprogrammable components denote meaning to the term. Communication networking components associated with BES Cyber Systems and within an Electronic Security Perimeter have the same level of protection applied as the BES Cyber Assets themselves. Additionally, CIP-005-5 communication protections continue to apply at the Electronic Security Perimeter. The drafting team did not find an additional Glossary term useful in the currently applied communication networks protection.
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 that a pilot program will assist responsible entities by	NERC modified the VRF assignment for CIP-006-6, Requirement R3 from Lower to Medium and filed the revision with FERC on 5/15/2014.

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

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	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, Requirement R4 from Lower to Medium, within 90 days of the effective date of this Final Rule.	NERC modified the VRF assignment for CIP-004-7, 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**
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 sections. 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-003-7, Requirements R2 and R4; CIP-004-7, Requirements R2, R3, R4, and R5; CIP-006-6, Requirements R1 and R2; CIP-007-7, Requirements R1, R2, R3, R4, and R5; CIP-009-6, Requirement R2; CIP-010-3, Requirements R1 and R2; and CIP-011-3, Requirement R1. NERC filed the following revisions with FERC on 5/15/2014: 1. **VSLs for CIP-003-7, 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. 2. **VSLs for CIP-004-7, Requirement R4**. This standard includes requirements for personnel

Directives from Order 791		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		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-009-6, 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.