Project 2016-02 Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 822

June 21, 2017

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
53	53. As discussed in detail below, however, the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).	The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 Requirement R1 to require responsible entities to document one or more plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Bulk Electric System (BES) Control Centers. Requirement R2 requires implementation of the documented plan(s). Due to the sensitivity of the data being transmitted between the Control Centers, as defined in the NERC Glossary of Terms Used in Reliability Standards, the SDT created the standard and determined that it applies to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact). The SDT has drafted requirements allowing Responsible Entities to apply protection to the links, the data, or both, to satisfy the security objective of the Commission's directive, consistent with the capabilities of the Responsible Entity's

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		operational environment. The directive language specifically references CIP-006-6 which pertains to physical security controls. CIP-006-6, Requirement R1, Part 1.10 focuses on protecting the nonprogrammable communication components between Cyber Assets within the same ESP for medium and high impact BES Cyber Systems. The SDT asserts that most of the communications contemplated by the Order are not within the same ESP, and that CIP-006-6, Requirement R1, Part 1.10 would not be the appropriate location for this requirement.
54	54. NERC and other commenters recognize that inter-Control Center communications play a critical role in maintaining bulk electric system reliability by, among other things, helping to maintain situational awareness and reliable bulk electric system operations through timely and accurate communication between Control Centers.[59] We agree with this assessment. In order for certain responsible entities such as reliability coordinators, balancing authorities, and transmission operators to adequately perform their reliability functions, their associated control centers must be capable of receiving and storing a variety of sensitive bulk electric system data from interconnected entities. Accordingly, we find that additional measures to protect both the integrity and availability of sensitive bulk	The SDT agrees that inter-Control Center communications play a critical role in Bulk Electric System reliability. Responsible Entities should therefore apply security measures to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring, which the current CIP Reliability Standards do not address. As such, the SDT has defined requirements that are designed to protect the data while it is being transmitted between inter-entity and intra-entity Control Centers. The SDT has drafted requirements allowing responsible entities to apply protection to the links, the data, or both to satisfy the security objective consistent with the capabilities of the responsible entity's operational environment.

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	electric system data are warranted.[60] We also understand that the attributes of the data managed by responsible entities could require different information protection controls. [61] For instance, certain types of reliability data will be sensitive to data manipulation type attacks, while other types of reliability data will be sensitive to eavesdropping type attacks aimed at collecting operational information (such as line and equipment ratings and impedances). NERC should consider the differing attributes of bulk electric system data as it assesses the development of appropriate controls. Footnotes: [59] NERC Comments at 20. [60] Protecting the integrity of bulk electric system data involves maintaining and ensuring the accuracy and consistency of inter-Control Center communications. Protecting the availability of bulk electric system data involves ensuring that required data is available when needed for bulk electric system operations. [61] Moreover, in order for certain responsible entities to adequately perform their Reliability Functions, the associated control centers must be capable of receiving and storing a variety of sensitive data as specified by the	

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	IRO and TOP Standards. For instance, pursuant to Reliability Standard TOP-003-3, Requirements R1, R3 and R5, a transmission operator must maintain a documented specification for data and distribute its data specification to entities that have data required by the transmission operator's Operational Planning Analyses, Real-time Monitoring and Real-time Assessments. Entities receiving a data specification must satisfy the obligation of the documented specification.	
55	55. With regard to NERC's development of modifications responsive to our directive, we agree with NERC and other commenters that NERC should have flexibility in the manner in which it addresses the Commission's directive. Likewise, we find reasonable the principles outlined by NERC that protections for communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers: (1) should not have an adverse effect on reliability, including the recognition of instances where the introduction of latency could have negative results; (2) should account for the risk levels of assets and information being protected, and require protections that are commensurate with the risks presented; and (3) should be results-based in order to provide flexibility to	The SDT drafted Reliability Standard CIP-012-1 to establish requirements to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers. The SDT developed objective-based rather than prescriptive requirements. This approach will allow Responsible Entities flexibility in protecting these communications networks and sensitive BES data in a manner suited to each of their respective environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the Commission. The SDT identified a need to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring regardless of asset risk level. The proposal requires protection for all data used for Operational Planning Analysis, Real-time Assessment, and Real-

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	account for the range of technologies and entities involved in bulk electric system communications.[62] Footnote: [62] See NERC Comments at 20-21.	time monitoring while being transmitted between Control Centers.
56	56. We disagree with the assertion of NIPSCO and G&T Cooperatives that the risk posed by bulk electric system communication networks does not justify the costs of implementing controls. Communications between Control Centers over such networks are fundamental to the operations of the bulk electric system, and the record here does not persuade us that controls for such networks are not available at a reasonable cost (through encryption or otherwise). Nonetheless, we recognize that not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection. We expect NERC to develop controls that reflect the risk posed by the asset or data being protected, and that can be implemented in a reasonable manner. It is important to recognize that certain entities are already required to exchange necessary real-time and operational planning data through secured networks using a "mutually agreeable security protocol," regardless of the entity's	The SDT noted the FERC reference to additional Reliability Standards and the responsibilities to protect the data in accordance with those standards (TOP-003-3 and IRO-010-2). The SDT interpreted these references as examples of potentially sensitive BES data and chose to base the CIP-012 requirements on the data specifications in these standards. This consolidates scoping and helps ensure that Responsible Entities mitigate the risk of the unauthorized disclosure or modification of Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data, rather than leaving the scoping to individual Responsible Entities. The SDT drafted CIP-012-1 to address confidentiality and integrity of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. These are accommodated by drafting the requirement to mitigate the risk from unauthorized disclosure or modification. The SDT contends that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards.

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	size or impact level.[63] NERC's response to the directives in this Final Rule should identify the scope of sensitive bulk electric system data that must be protected and specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted or at rest. Footnote: [63] See Reliability Standards TOP-003-3, Requirement R5 and IRO-010-2, Requirement R3.	The SDT drafted CIP-012-1 to address the data while being transmitted. The SDT contends that this data is maintained within BES Cyber Systems, and is afforded the protections of CIP-003 through CIP-011.
58	58. Several commenters sought clarification whether Control Centers owned by multiple registered entities would be included under the Commission's proposal. We clarify that the scope of the directed modifications apply to Control Center communications from facilities at all impact levels, regardless of ownership. The directed modification should encompass communication links and data for intra-Control Center and inter-Control Center communications.	The SDT created the standard and determined that it applies to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact), regardless of ownership. The SDT defined requirements that are designed to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring while being transmitted between inter-entity and intra-entity BES Control Centers.
62	62. Several commenters addressed encryption and latency. Based on the record in this proceeding, it is reasonable to conclude that any lag in communication speed resulting from implementation of protections should only be measureable on the order of	The SDT developed objective-based rather than prescriptive requirements. This approach will allow Responsible Entities flexibility in mitigating the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis,

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	milliseconds and, therefore, will not adversely impact Control Center communications. Several commenters raise possible technical implementation difficulties with integrating encryption technologies into their current communications networks. Such technical issues should be considered by the standard drafting team when developing modifications in response to this directive, and may be resolved, e.g., by making certain aspects of the revised CIP Standards eligible for Technical Feasibility Exceptions.	Real-time Assessments, and Real-time monitoring in a manner suited to each of their respective environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the Commission.