Posting Document/Unofficial Comment Form

# Project 2016-02 Modifications to CIP Standards

Communication Networks

**Do not** use this form for submitting comments. Use the [electronic form](https://sbs.nerc.net/) to submit comments
on the Standard Drafting Team’s (SDT) approach and draft language **to address the Federal Energy Regulatory Commission (Commission or FERC) directive regarding** **Communication Networks**. The electronic form must be submitted by **8 p.m. Eastern, March 13, 2017.**To minimize the number of posted documents, the SDT included everything in this single document with the questions following the suggested approach and draft language.
Additional information is available on the [project page](http://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx). If you have questions, contact Senior Standards Developer, Al McMeekin (via email) or at (404) 446-9675.

## Introduction

On January 21, 2016, the Commission issued [Order No. 822](https://www.ferc.gov/whats-new/comm-meet/2016/012116/E-2.pdf) approving seven CIP Reliability Standards and new or modified definitions and issuing certain directives requesting modifications to the CIP Reliability Standards. The focus of this informal comment period is on the directive from the Commission requesting NERC to “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).” (Order 822, Paragraph 53)

The SDT is working through an evaluation process to determine appropriate actions to take in order to meet the Commission’s directive. The informal posting reflected herein represents the initial exploratory efforts to research the scope and objectives of the draft standard and associated requirements. The SDT will consider all comments received from industry stakeholders and will revise the draft language accordingly. The revised language may expand in scope and the security objective(s) may be modified to align with industry comments.

The SDT is considering the following assumptions and is requesting stakeholder input through the comment form below on the validity of these assumptions:

* A formal definition of “sensitive BES data” is not required because Responsible Entities are already required to identify operational reliability data in FERC-approved Reliability Standards TOP-003-3 and IRO-010-2.
* Data at rest within a BES Cyber System is already afforded protections in existing CIP standards (CIP-003, 005, 007, etc.), is perishable, and has a diminished need for protection over time.
* The existing definition of Control Center is adequate.

In addressing the directive, the SDT’s initial efforts are focused specifically on the communication links transmitting sensitive data between Control Centers. While the directive language in Order 822 specifically references modifications to CIP-006-6 which handles physical security controls, the SDT is considering language around logical protections of these communication links through a programmatic approach. Because these requirements will apply to Control Centers at all impact levels (high, medium, and low), the SDT is also proposing to create a new CIP Reliability Standard, CIP-012-1, to address the protection of sensitive BES data transmitted between Control Centers. While the SDT is not yet certain of the full scope of requirements necessary to address the directive found in paragraph 53 of Order 822. Some of the draft language the SDT is currently considering and requesting stakeholder feedback on is as follows.

**Draft Language**

The Responsible Entity shall implement one or more documented plan(s) that achieve the security objective to protect confidentiality and integrity[[1]](#footnote-1) of data required for reliable operation of the BES. The plan applies to data being transferred across communication networks between Control Centers, both inter-entity and intra-entity and shall include each of the applicable parts below:

* 1. Procedure(s) to identify the communication networks requiring protections;
	2. Procedure(s) for defining the boundaries of communication networks transmitting data required for reliable operation identified in 1.1, if applicable;
	3. Method(s) for protecting communication networks between Control Centers identified in 1.1, where technically feasible.

Examples of evidence may include, but are not limited to, plan documents; documentation such as representative diagrams, configuration settings or demonstration materials to illustrate and verify that confidentiality and integrity of data transmitted between Control Centers has been protected and satisfies the security objective. Information gathering during walk-downs or visual inspections can validate the implementation of necessary controls. The documentation as referenced may be used to further validate where protections may or may not be required.

## Draft Guidance

This draft language mandates that communication networks required for reliable operation between Control Centers be identified and protected. The Responsible Entity has flexibility in determining how to implement the draft language.

In developing plan(s), the number of plan(s) and their content should be guided by a Responsible Entity's management structure and operating conditions. Each Responsible Entity is required to implement one or more documented plan(s) that achieve the stated security objective of protecting the confidentiality and integrity of data that is required for reliable operation and is transmitted between Control Centers. To achieve this objective, the Responsible Entity is required to document and implement plan(s) that include a procedure(s) for the identification of communication networks that transmit operational reliability data between Control Centers. The plan(s) should identify the applicable communication networks both within the entity’s footprint, and any applicable networks between Responsible Entities. When defining the procedures for identifying applicable communication networks, the Responsible Entity should ensure that the methods chosen include rationale supporting the identification of such communication networks. As one possible solution, the Responsible Entity could apply CIP-002 criteria to identify all inter-Control Center and intra-Control Center communication links that could adversely impact the reliable operation of the Control Center within 15 minutes. Another possible solution to identifying in-scope communication networks is to take a data-centric approach. The Responsible Entity could identify applicable operational reliability data that is transmitted between Control Centers. This data has already been identified for some applicable entities (Reliability Coordinator (RC) and Transmission Operator (TOP)) in the data specification requirements. Responsible Entities such as the Distribution Provider (DP) and Generator Operator (GOP) that do not have existing data specification requirements should identify, at a minimum, operational reliability data that has been requested by a Balancing Authority (BA), RC, or TOP as operational reliability data.

The Responsible Entity could then use the data identified in the previous step to determine which communication links require protection under CIP-12-1. Examples of these communication links are:

1. Data link(s) between neighboring Transmission Operators
2. Data link(s) between a Balancing Authority and a Reliability Coordinator
3. Data link(s) between a Generator Operator and a Balancing Authority
4. Data link(s) between a Transmission Owner and a Transmission Operator
5. Data link(s) between a Distribution Provider and a Transmission Operator
6. Data link(s) between Reliability Coordinators
7. Data link(s) between two Primary Control Centers owned by a Responsible Entity
8. Data link(s) between a Primary and Backup Control Center owned by a Responsible Entity

The plan(s) should address how the boundary is determined for all communication networks that are identified using the entity-developed procedure(s) (e.g. ESP boundary, Router outside of an ESP but within a PSP, Cyber Asset used as an electronic access control for a low impact BES Cyber System, etc.). A Responsible Entity has the freedom to identify these boundaries as it sees fit. The entity should take the various features of its environment into account and determine the most effective and efficient solution when defining these boundaries. There is no limitation on where boundary protection must begin and terminate, other than ensuring that the endpoint identified is controlled by the Responsible Entity. The SDT recommends that when selecting the endpoint, Responsible Entities carefully consider reliability concerns and technical limitations. Endpoints identified by the Responsible Entity are not meant to represent additional assets to be included in the scope of the CIP Reliability Standards. The intent of the endpoint identification is to ensure each Responsible Entity identifies clear demarcation of where the protections applied to the in-scope communications networks exist. The boundaries can vary based upon impact levels of the Control Center containing BES Cyber Systems, different technologies, or infrastructures. The list of example network boundaries is provided below:

* Electronic Access Point on the Electronic Security Perimeter boundary of a High or Medium Impact BES Cyber System
* Router outside of an Electronic Security Perimeter that is protected under an Entity’s Physical Security Program
* A Cyber Asset that performs the role of an Electronic Access Control for a low impact BES Cyber System

Additionally, the Responsible Entity must document and implement plans for the protection of the confidentiality and integrity of operational reliability data communicated between Control Centers. This security objective could be achieved through a variety of methods or combination of methods (e.g. site to site encryption, application layer encryption, physical protection, etc.). The methods must address the confidentiality and integrity of the operational reliability data and protect the data on the applicable communication networks/data links between Control Centers. The protections to be applied to the communication links identified by the Responsible Entity are chosen at the Responsible Entity’s discretion. However, the Responsible Entity should exercise caution to ensure that both confidentiality and integrity of the in-scope communication links are protected. Some examples of methods that can be implemented include but are not limited to:

* Site to site encryption: Site to site encryption provides a means to securely transmit and access information between two or more sites. Site to site encryption allows peers at both ends of the identified link to encrypt and decrypt packets using mutually agreed-upon keys or certificates and methods of encryption. This method can be used to achieve the protection of both the confidentiality and integrity of the communication link provided that the encryption method chosen not only obfuscates the data payload, but also provides a means to verify that the data payload did not change between the source and destination.
* Application layer encryption: Application-layer encryption protects the data at the highest layer in the BES cyber system providing the sensitive data, making it invisible to all the layers below. If a Responsible Entity chooses this option, care must be taken to ensure the inclusion of both confidentiality and integrity. If the solution implemented only addresses confidentiality, the Responsible Entity will need to also implement a complementary control, such as a hashing mechanism, to protect against the manipulation of the data.
* Physical protections: In some cases, a Responsible Entity may choose to implement physical protections on the communication links in question. Secure conduit can be a method to help secure the confidentiality and integrity of an in-scope link between Control Centers, as well as helping ensure availability. While this measure can be used, it is suggested that a Responsible Entity complement physical protections with logical protections to fully ensure that the integrity and confidentiality of data transmitted between Control Centers is protected.

## Questions

1. The SDT asserts that the referenced data is already afforded protections at rest under existing CIP standards (CIP-003, 005, 007, etc.), is perishable, and has a diminished need for protection over time. Do you agree with the SDT’s assertion? If you agree, please supply a rationale to support the position.

[ ]  Yes

[ ]  No

Comments:

1. If you do not agree with the SDT’s assertion in Question 1, please identify the type of data, the risk posed at rest, and supply the rationale to support the position.

Comments:

1. Future enforceable Reliability Standards IRO-010-2 and TOP-003-3 identify “data required for reliable operation.” For example, Requirement R1 of IRO-010-2 states:

**R1.** The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real‐time monitoring, and Real‐time Assessments. The data specification shall include but not be limited to:

* 1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real‐time monitoring, and Realtime Assessments including non‐BES data and external network data, as deemed necessary by the Reliability Coordinator.

TOP-003-3 Requirements R1 & R2 also have similar requirements for BAs and TOPs.

Do you agree that outlining this approach for identifying “data required for reliable operation” in the Guidelines and Technical Basis is sufficient; consequently, an additional definition of “sensitive BES data” or a requirement to identify “sensitive BES data” is not necessary? If not, please explain.

[ ]  Yes

[ ]  No

Comments:

1. The SDT asserts that “availability” of inter-and intra-entity Control Center communication of data is being addressed in Project 2016-01 Modifications to TOP and IRO Standards, specifically Reliability Standards TOP-001-4 and IRO-002-5. The proposed standards require redundant and diversely routed data exchange capabilities at a Responsible Entity’s primary Control Center. Do you agree that “availability” is adequately addressed by these standards? If not, please provide rationale to support your position.

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing to develop a new CIP standard because the directives of FERC Order 822 related to the protection of communication networks used to exchange sensitive BES data regardless of the entity’s size or impact level. Do you agree with the drafting of a new CIP standard to address this issue? If you disagree and would prefer to include requirements in existing CIP Standards, such as CIP-003 and CIP-005, please provide rationale and propose requirement language.

[ ]  Yes

[ ]  No

Comments:

1. The SDT evaluated multiple approaches to addressing the directive. The approach proposed in this informal posting focuses on the protection of communication links. An alternative approach could focus on the protection of the sensitive BES data itself. Do you agree with the SDT’s approach to focus the draft language on the protection of communication links? If not, please provide rationale and propose alternative language.

[ ]  Yes

[ ]  No

Comments:

1. Do you agree with the security objective of the draft language? If not, please propose alternative language.

[ ]  Yes

[ ]  No

Comments:

1. Is it clear what types of plans, procedures, and methods are needed to meet the draft language? If not, please propose alternative language.

[ ]  Yes

[ ]  No

Comments:

1. The SDT uses the term “communication networks” throughout the draft language including an obligation to define the boundaries of such communication networks. Does the SDT need to define the term for inclusion in the NERC Glossary of Terms? If so, please propose a definition of “communication networks.”

[ ]  Yes

[ ]  No

Comments:

1. **NIST Special Publication 800-53A :** Revision 4, Appendix B : <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf> [↑](#footnote-ref-1)