NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2016-02

Modifications to CIP Standards
Consideration of Comments to CIP-012-1
(Comment Period: October 27 – December 11, 2017)

March 2018

RELIABILITY | ACCOUNTABILITY



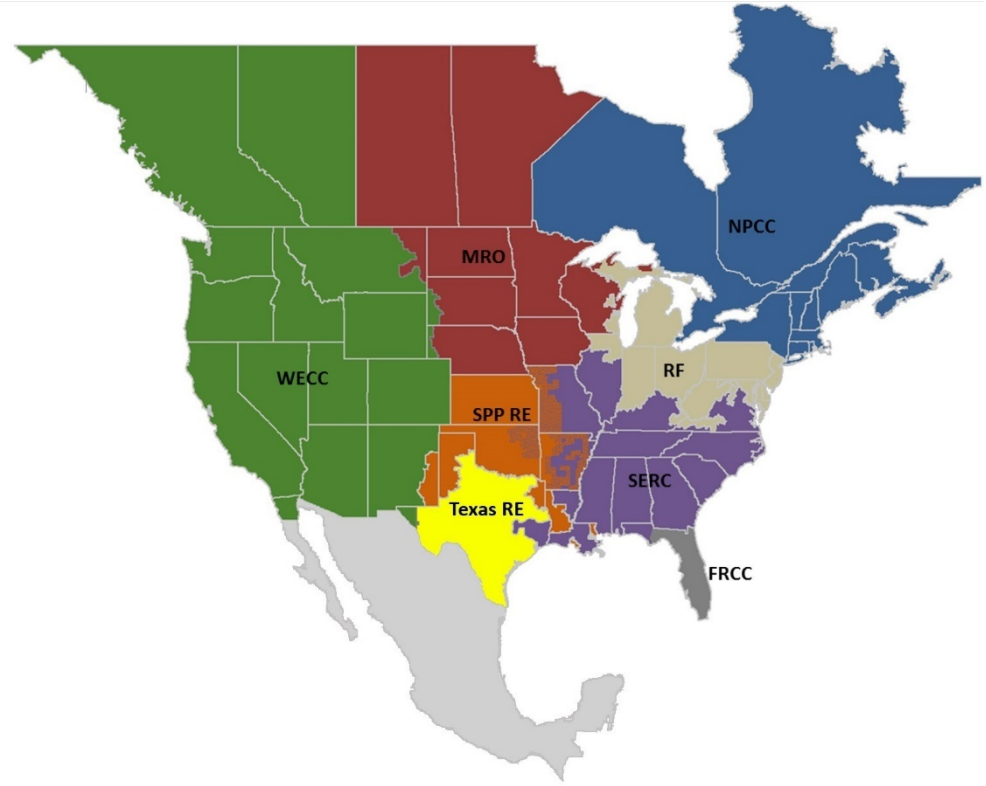

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability and security of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into eight Regional Entity (RE) boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated transmission owners/operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The standard drafting team (SDT) appreciates industry comments on the proposed Reliability Standard, CIP-012. The SDT considered the comments submitted during the additional posting of the proposed Reliability Standard, and adapted its revision approach for the third proposal currently posted. Additionally, the SDT conducted substantial outreach during the revision process, through in-person meetings, conference calls, and stakeholder organization presentations.

On January 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 822 Revised Critical Infrastructure Protection Reliability Standards. In this order, FERC approved revisions to version 5 of the CIP standards.

Response to Comments

The SDT has carefully reviewed each stakeholder comment and has revised language where suggested changes are consistent with SDT intent and industry consensus. The SDT reviewed and responded to each comment in summary form below.

There were 61 sets of comments comprised of approximately 168 different people across approximately 117 companies representing 10 of the Industry Segments.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Senior Director of Standards, Howard Gugel (via email) or at (404) 446-9693.

Creation of CIP-012-1

- Multiple commenters noted that CIP-012 is not needed and can be accommodated within existing CIP Standards. The commenters also noted that encryption may not be feasible and the only remedy is to physically protect the entire communication system.

  The SDT contends that CIP-012 is needed as the application of protection is different for in-scope data while being transmitted between Control Centers than it is with other standards, such as CIP-005. CIP-012 addresses applicable data transmitted between Control Centers and backup Control Centers regardless of BES Cyber System impact rating. CIP-005 is applicable only to high and medium BES Cyber Systems. The SDT disagrees that the only way to achieve the security objective is to physically protect the entire communication system. Further, the SDT asserts that an entity can apply any combination of controls it sees fit to achieve the security objective. CIP-006 even acknowledges that physical protection may not be the only solution. Geographic distance is just one factor that needs to be evaluated that may preclude the use of physical protection alone.

- Several commenters provided support of CIP-012 and the requirements, noting the results-based approach allows Responsible Entities to select and implement the controls appropriate to their organization.

  The SDT thanks you for the comments.

- A commenter noted CIP-012 is not needed.

  The SDT contends that CIP-012 is needed. Applying protection for in-scope data while being transmitted between Control Centers in CIP-012 is different from applying data protection in other standards. CIP-012 is also applicable to all impact levels, unlike CIP-002 through CIP-011

- A commenter remains concerned that the proposed CIP-012 Standard may result in confusion, particularly among Generation Operators with Control Centers subject to the standard regarding the scope of their compliance obligations or, alternatively, may inadvertently result in a significant reliability gap given the structure of the ERCOT market. In ERCOT, generators do not communicate directly with the regional Reliability Coordinator (ERCOT). Instead, generators are required to communicate through designated entities known as Qualified Scheduling Entities (QSEs). In many instances, these QSEs are third-party entities. Within the NERC regulatory construct, Generator Operators have delegated certain NERC compliance functions to these entities, including providing data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring. Critically, Generator Operators remain responsible for all compliance obligations associated with QSE activities in the ERCOT region.

  The Responsible Entity that delegates its functional responsibilities to a third party agent through a contract or otherwise, continues to be responsible for compliance with NERC Reliability Standards. CIP-012-1 is applicable to NERC-registered Generator Operators and Generator Owners. Responsible Entities are to ensure that Real-time Assessment and Real-time monitoring data is protected throughout the transmission between each Control Center, regardless of any other third party in the middle of the transmission of the data. To address the concerns with coordination between Responsible Entities, modified the requirement to include, "If the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time

Assessment and Real-time monitoring data between those Control Centers". This requires entities to participate in this coordination while maintaining flexibility on implementation of this requirement.

Requirement 1

- A commenter requested that the requirement be modified to require each Responsible Entity to mitigate the risk of unauthorized disclosure or modification of its own BES data between its own Control Centers.

  FERC Order 822 specifically notes that the protection of sensitive BES data transmitted between Control Centers should be implemented for both inter- and intra-entity transmissions of data. The SDT developed CIP-012 in response to the FERC Order.

- A commenter recommended a change in the order of the three sub-requirements in Requirement R1.

  The SDT has identified the required actions to be taken within Requirement R1. During SDT discussions, entities varied on which step they would complete first. The requirement parts can be completed in any order. Requirement R1.3 is listed last since it may not be applicable to all entities

- A commenter proposed a few minor non-substantive edits to CIP-012 Requirement R1 and Measurement M2. The edits reference the term "plan(s)" and ensures consistent use throughout the standard

  The SDT has modified Requirement R1 as noted and has combined Requirements R1 and R2.

- Commenters noted concerns regarding the resolution of disagreements under Requirement R1.3.

  The SDT asserts that it is every Responsible Entity's obligation as defined in CIP-012, to protect data while being transmitted between Control Centers. The SDT cannot comment on specific approaches to resolve conflicts that arise in defining responsibilities between entities. Entities should consider working with the Regional Entity where there are unresolved disagreements.

- A commenter noted it is not clear how Requirement R1 addresses future Control Centers since the requirement suggests a one-time plan.

  The SDT asserts that Requirement R1 is not intended to be a one-time plan. A Responsible Entity will need to produce a plan to protect all in-scope data while being transmitted between Control Centers. This plan will need to apply to all Control Centers that a given entity owns or operates. As the number of Control Centers within an entity's purview changes, so should the plan and implementation of the plan be changed.

- A commenter noted that the requirement should specify creation of a documented process instead of a documented plan.

  The SDT disagrees regarding the use of the term "process" instead of "plan," the SDT notes that the term 'documented process' refers to a set of required instructions specific to the Responsible Entity developed to achieve a specific outcome. The plan to meet Requirement R1 may simply be a documentation of the architecture in place to provide the defined security protection and not a series of instructions or steps to be followed.

Requirement 2

- Commenters requested that the SDT consider consolidating Requirement R2 into Requirement R1, noting it is unnecessary to have two requirements. The commenters also noted that the requirement should specify creation of a documented process instead of a documented plan.

  The SDT agrees with comments regarding a single requirement and has modified Requirement R1 accordingly. With regard to the use of the term "process" instead of "plan", the SDT notes that the term documented process refers to a set of required instructions specific to the Responsible Entity, designed to achieve a specific outcome. The plan to meet Requirement R1 may simply be a documentation of the architecture in place to provide the defined security protection and not a series of instructions or steps to be followed.

- Commenters requested that the SDT consider consolidating Requirement R2 into Requirement R1, noting it is unnecessary to have two requirements.

  The SDT agrees with comments regarding a single requirement and has modified Requirement R1 accordingly.

Identification of Data

- A commenter requested that CIP-012-1 or supporting documents explicitly state that market data is out of scope.

  The SDT asserts that the data a Balancing Authority requires to perform Real-time monitoring and Real-time Assessments is the appropriate data to be protected under CIP-012-1. Where there is information being requested by a Balancing Authority or other Responsible Entity performing Real-time monitoring and Real-time Assessments, the SDT advises coordination between the Responsible Entities to ensure the correct data is identified and protected accordingly.

- Multiple commenters noted that all data elements should be evaluated in their unique context and that confidentiality protection is not needed for all data.

  The SDT has established the security objective in Requirement R1 to address the Commission's directive on protecting the confidentiality (unauthorized disclosure) and integrity (unauthorized modification) of the data being transmitted. The SDT asserts that data used for Real-time monitoring and Real-time Assessment is critical to the reliable operation of the Bulk Electric System and needs to be protected from unauthorized disclosure and modification. The SDT determined it would be a complex and difficult exercise for an Entity to define the protection required for various data elements in every situation. Therefore, the SDT chose to high water mark all of the in-scope data. In addition, the SDT notes that most, if not all of the methods applied to protect the integrity of data also inherently protect the confidentiality of the data.

- Commenters noted that viewing Real-time Assessment and monitoring/control data without context will adversely affect reliable operation of the BES and believes not all in-scope data requires the same level of confidentiality.

  The SDT has established the security objective in Requirement R1 to address the Commission's directive on protecting the confidentiality (unauthorized disclosure) and integrity (unauthorized modification) of the data being transmitted. The SDT asserts that data used for Real-time monitoring and Real-time Assessment is critical to the reliable operation of the Bulk Electric System, and thus needs to be protected from unauthorized disclosure and modification. The SDT determined it be a complex and difficult exercise

for an Entity to define the protection required for various data elements in every situation. Therefore, the SDT chose to high water mark all of the in-scope data. The SDT also notes that most, if not all, of the methods applied to protect the integrity of data also inherently protect the confidentiality of data.

- A commenter is concerned that the scope of data is too broad and subject to interpretation during audits without direct ties to the IRO and TOP standards requiring identification of the subject data.

The SDT discussed referencing the two applicable standards in the requirement language and determined that a number of issues could arise by directly referencing applicable IRO/TOP requirements. Possible issues include, but are not limited to, applicability issues and the required coordination of future revisions of the IRO/TOP standards and proposed Reliability Standard CIP-012.

Control Data

- Multiple commenters noted concerns with the meaning of "control data," noting it may create confusion and does not align with TOP-003 and IRO-010 data specification requirement.

The SDT agrees with the comments and has removed "and control" from Requirement R1.

Data Centers

- One commenter noted a concern with the definition of Control Center including associated data centers, specifically noting aggregating devices such as a dual port RTU could be interpreted as an associated data center to a Control Center.

As shown in the reference models and noted in the applicability section, communication between Control Centers and field devices, such as RTUs, are not in scope for CIP-012. The in-scope communications considered in CIP-012-1 are between two Control Centers, as defined in the NERC Glossary of Terms Used in Reliability Standards. Additionally, a data center not associated with the Control Center would be out of scope of CIP-012-1.

- A commenter noted that the communication link between Control Centers is in scope for CIP-012, but the link between Control Center and Data Center is not.

The SDT agrees that a Responsible Entity needs to protect the in-scope data while being transmitted between Control Centers. The SDT notes that the Control Center by definition includes the associated data center and should, therefore be included with protecting intra-Control Center communications. The SDT envisions a scenario where intra-Control Center communications not afforded protection elsewhere in the Reliability Standards would need to be protected under CIP-012 R1.

Administrative Burden

- A commenter noted that defining "roles and responsibilities" may create an administrative burden. They noted that different Responsible Entities may not be willing to share their "security protections" with other entities as this may create a security gap or at the least, letting others know what protections are in place. When each Entity becomes compliant with this Standard, their plans will assure that protections are in place on "their end" of the data stream. This will assure that protections, which is the intent of this Standard.

The SDT developed Requirement R1.3 to only apply to situations where multiple entities are involved in the transmission of the applicable data. Those entities must have an agreement on security protection in order for the transmission to actually happen. The intent is for the entities to agree upon and document who is

responsible for the various aspects of the protection. It may not be practical for both entities to try to control encryption keys, etc.

VSL Language

- Commenters noted concerns with the VSLs for the requirements. First, the VSL for Requirement R2 should be revised to include a moderate and high VSL. Second, it was recommended to add "develop" to the VSL language for Requirement R1.

The SDT combined Requirement R2 into Requirement R1 and revised the VSLs. The SDT removed "develop" from the language of Requirement R1.

Defining Other Terms

- Commenters requested that the SDT define Real-time monitoring.

The SDT asserts that Real-time monitoring is a well understood concept that is included in the TOP and IRO standards.

- Commenters noted that viewing Real-time Assessment and monitoring/control data without context will adversely affect reliable operation of the BES and believes not all in-scope data requires the same level of confidentiality.

The SDT has established the security objective in Requirement R1 to address the Commission's directive on protecting the confidentiality (unauthorized disclosure) and integrity (unauthorized modification) of the data being transmitted. The SDT asserts that data used for Real-time monitoring and Real-time Assessment is critical to the reliable operation of the Bulk Electric System, and thus needs to be protected from unauthorized disclosure and modification. The SDT determined it be a complex and difficult exercise for an Entity to define the protection required for various data elements in every situation. Therefore, the SDT chose to high water mark all of the in-scope data. The SDT also notes that most, if not all, of the methods applied to protect the integrity of data also inherently protect the confidentiality of data.

Alignment to TOP-003 and IRO-010

- Commenters requested the SDT add functional registrations noted in TOP and IRO standards to CIP-012 in order to draw a more clear line to Entities responsible for defining the Real-time Assessment and Real-time monitoring data under TOP-003 and IRO-010.

The SDT agrees with the comments and supports that this provides clarity and prevents all entities subject to CIP-012-1 from creating their own identification of Real-time Assessment and Real-time monitoring data. The SDT has modified Requirement R1 to address this recommendation.

- Commenters noted that the types of data to be within scope, as identified by data specification lists originating from Requirements TOP-003 and IRO-010 are not specific enough to determine or limit the types of data, or communication methods that would need to be protected the data. These lists contain data and methods of communicating data that may not be considered relevant to the scope of CIP-012.

The SDT agrees and has removed "and control" from Requirement R1. The SDT asserts that the data listed in the data specifications required to perform Real-time monitoring and Real-time Assessments is the appropriate data to be protected under CIP-012-1. Where there are concerns with information being requested by another Responsible Entity performing Real-time monitoring and Real-time Assessments,

coordination between the Responsible Entities is advised to ensure the correct data is identified and protected accordingly.

Third Parties

- Commenters noted that the guidance regarding third parties involved in the communication of Real-time Assessment and Real-time monitoring data is unclear. Further, some Generator Owners and Generator Operators neither own nor operate Control Centers due to agency relationships or through contracts with companies that are not NERC registered entities.

  The SDT agrees with the comments regarding the guidance on third parties and has removed the content. The Responsible Entity that delegates its functional responsibilities to a third party agent through a contract or otherwise, continues to be responsible for compliance with NERC Reliability Standards.

Demarcation Point

- Commenters noted that the demarcation point should be constrained to entity's equipment and not include an implied requirement that each entity document both their demarcation points and the demarcation points on neighboring systems.

  The SDT agrees and has modified the draft requirement accordingly.

- Commenters noted the importance of clarifying that demarcation points do not add additional Cyber Assets to the scope of the CIP standards CIP-002 through CIP-011.

  The SDT does not intend for CIP-012 to modify the list of Cyber Assets managed under CIP-002 thru CIP-011. This has been addressed within the Technical Rationale and Justification for Reliability Standard CIP-012-1.

Implementation

- A majority of commenters indicated that twenty-four months is an adequate standard implementation timeline. It allows entities sufficient time to develop internal plans to implement the enhanced security requirements. It also provides time to negotiate the necessary security changes between entities, and to make appropriate contract adjustments with service providers.

  The SDT thanks you for your comments.

- A commenter noted that the CIP-012 implementation period seems to be an excessively long to implement this proposed standard since security of real-time data is important and should be prioritized.

  The SDT determined that the complexity of the implementation needed an allowance of up to twenty-four (24) months for implementation. Entities have the flexibility to phase in their implementation of the requirement as long as all activities are completed within 24 months.

- Several commenters noted that more time is needed for implementation of CIP-012. Reasons included coordination with other entities, as well as specification, design, budgeting, implementation, and testing. Commenters also raised concerns on the impact to existing contractual agreements.

  The SDT carefully considered all comments and concluded that many factors should be considered to determine an implementation period. These factors include complexity of technology solutions, quantity of

telecommunications lines requiring controls and coordination with other Responsible Entities/solution providers. The SDT concluded that a twenty-four (24) month implementation period is appropriate.

- A commenter feels that 12 months is appropriate to develop a plan, but an additional 24 months beyond planning may be needed to implement a reliable technical solution. Given the need to perform a proper engineering study on network infrastructure to assess current state and adapt it to meet the new requirements, additional time is needed to assess how changes may impact system and network response (loading, latency, etc.). It will also be necessary to review and / or establish contracts and memorandums of understanding to ensure that we continue to reliably receive the data we need and to deliver the data that others may need from us. Inherent in these studies and implementations are additional costs that may be impacted by budget cycles, as well as the costs attributable to resource constraints given the constant environment of standards changes currently. These factors prevent any realistic analysis at this time of the cost-effectiveness of such implementations.

  The SDT carefully considered all comments and concluded that many factors should be considered to determine an implementation period. These factors include complexity of technology solutions, quantity of telecommunications lines requiring controls and coordination with other Responsible Entities/solution providers. The SDT concluded that a twenty-four (24) month implementation period is appropriate. Entities have the flexibility to phase in their implementation of the requirement as long as all activities are completed within 24 months.

Cost Effectiveness

- Several commenters noted they were unable to address the issue of cost effectiveness in full at this time. They noted the cost of implementation could not be adequately assessed until discussion and coordination with our neighboring entities. Cost effectiveness of implementation will depend on the technology deployed. Infrastructure may need to be added to support the requirement and may be costly to contract and support.

  The SDT carefully considered all comments and concluded that many factors should be considered to determine an implementation period. These factors include complexity of technology solutions, quantity of telecommunications lines requiring controls and coordination with other Responsible Entities/solution providers. CIP-012 has been written to allow entities flexibility in determining the solutions that work best for the organization and those they share this information with.

- Several commenters noted the need for an encryption standard to be developed across the various regions. The implementation of several different technologies to communicate with several different Reliability Coordinators and utilities would be overly burdensome and at a cost that would not be effective. It was noted that there is little that is mutually agreed upon in the data specification documents as they relate to IRO-010 and TOP-003. The Balancing Authority, Transmission Operator, and Reliability Coordinator specify the data they want to receive in the manner they want to receive it. Others receiving the requests are obligated to comply. Additionally, a commenter noted that the lack of guidance could lead to inconsistency of implementation.

  The SDT agrees a common standard would be highly beneficial to those operating in multiple regions. The SDT will refer the issue to the CIPC for review and consideration as a guideline.

- Several commenters noted the proposal cannot be implemented in a cost-effective manner within twenty-four (24) months. If the implementation period remains 24 months, entities will expend more resources and capital than using a phased implementation. A phased implementation provides the ability to ensure the most effective plan and plan more accurately within budget cycles. Commenters noted a 24-month

implementation timeline could affect reliability because many opportunities exist for encryption to fail and those challenges must be addressed, which has a direct effect on cost.

The SDT carefully considered all comments and concluded that many factors should be considered to determine an implementation period. These factors include complexity of technology solutions, quantity of telecommunications lines requiring controls and coordination with other Responsible Entities/solution providers. The SDT concluded that a twenty-four (24) month implementation period is appropriate. Entities have the flexibility to phase in their implementation of the requirement as long as all activities are completed within 24 months.

- One commenter recommended development of an exception process can be defined if needed to offer flexibility.

In order to evaluate this request, the SDT needs additional information and invites the commenter to participate in the regularly scheduled meetings.

Guideline and Technical Basis / Rationale

- Several commenters raised concerns with the lack of a Guidelines and Technical Basis (GTB) section of CIP-012. They noted the lack of GTB makes it difficult to understand the drafting team's intent, and evaluate the standard.

The SDT developed and posted Technical Rationale and Implementation Guidance documents to support CIP-012. The SDT will submit the Implementation Guidance for ERO endorsement once the requirement language is finalized.

- Several commenters discussed the criticality of having the Technical Rationale completed and Implementation Guidance endorsed for CIP-012. They noted industry will likely find it difficult to make any final judgments on the proposed Reliability Standard without NERC's endorsement of the draft Implementation Guidance. In the event the Implementation Guidance is not endorsed, there are fears the approval of this standard may be at risk.

The SDT developed and posted Technical Rationale and Implementation Guidance documents to support CIP-012. The SDT will submit the Implementation Guidance for ERO endorsement once the requirement language is finalized.

- Another commenter requested that the SDT provide a rationale for including the phrase "CIP Exceptional Circumstances." The same commenter further stated that it is particularly unclear why certain CIP exception conditions necessarily trigger CIP Exceptional Circumstances events. For example, why would an imminent hardware failure under all circumstances require a relaxation of physical security protection for communications links transmitting sensitive data?

The SDT drafted the requirement with the understanding that there may be instances where a Responsible Entity may not be able to maintain compliance with the requirement because of a CIP Exceptional Circumstance. Responsible Entities may need to use alternate, as-yet-unidentified data transmission methods because of a CIP Exceptional Circumstance event. This allowance will enable Responsible Entities to focus on reliability without the risk of a compliance issue.

Control Center Definition

- Commenters raised questions on the prior proposal for modifying the definition of Control Center. The commenters noted modifications to the definition and CIP-012 should move forward together in future steps in the standard development process. They also noted that when reviewing the new current draft of CIP-012, it is unclear if the current approved Control Center definition or the draft revised Control Center definition is what the drafting team intends the reader to use.

  The SDT has developed and posted modifications to the Control Center definition.

Medium / High Impact Control Centers

- Commenters questioned in the case of medium and high impact Control Centers, whether it is intended for the communication to be protected up to an Electronic Access Point on the Electronic Security Perimeter and/or the Physical Security Perimeter. If that is the intent, it is suggested that the demarcation point requirement clearly state this. It was also noted that if the demarcation point for communication is a CIP Cyber Asset, communication of this information and responsibilities between entities may require NDAs between entities.

  The SDT does not intend for CIP-012 to prescribe the point where security protection is applied. Depending on the entity, it may be at an ESP or it may not. It is the point where the protection can be applied before it is transmitted to another Control Center. The same consideration should be made in determining the physical protection. The SDT agrees that proper care should be taken with sharing information that could be considered BES Cyber System Information.

CIP-012 Applicability

- A commenter requested clarification on which Control Centers are applicable under CIP-012.

  The SDT drafted CIP-012 to apply to all types of Control Centers, regardless of the impact rating associated with the Control Centers' BES Cyber Systems.

- A commenter noted that Generator Owners are not listed in the Control Center definition and should be removed from applicability of CIP-012.

  The SDT modified the applicability of the Standard as, "The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center." The SDT intends for the standard to include Generator Owners and Transmission Owners that own or operate a Control Center. The Control Center definition as written addresses the reliability tasks of an RC, BA, TOP, and GOP irrespective of registration. The SDT has developed and posted modifications to the Control Center definition.

Compliance

- A commenter requested clarification on the responsibility for compliance, including who will be audited under CIP-012.

  The SDT asserts that entities that own and/or operate Control Centers, per Section 4 "Applicability" are responsible to document and implement a plan to protect the data specified in CIP-012. The Responsible Entity that delegates its functional responsibilities to a third party agent through a contract or otherwise, continues to be responsible for compliance with NERC Reliability Standards.

FERC Directive 822

- A commenter noted it would be more effective if the SDT specifically identified the security objective described in FERC Order No. 822 paragraph 54, of "maintaining the integrity and availability of sensitive BES data", should account for risk of cyber assets, and should be results based and not zero-defect.

  The SDT asserts that the security objective is clear and aligns with FERC Order 822, taking into consideration the sensitivity of the data being transmitted. As drafted, the development and implementation of a plan allows entities to tailor protection to their environment.