NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-012 Communication Between Control Centers

Webinar Questions – Draft 3

The Project 2020-04 Standard Drafting Team (SDT) conducted an industry webinar on the third draft of the proposed CIP-012-2. The SDT received multiple questions that they were unable to respond to in the given time. This document is a collection of the questions and the response that the SDT received.

CIP-012-2 Industry Webinar Questions	
Question	**SDT Response**
Is an MOU or contractual agreement required to meet compliance to this language? yes or no?	Thank you for your question. A MOU isn't required, but there can be multiple ways to achieve compliance *including* a MOU or contractual agreement. The SDT, however, encourages all entities to be able to provide evidence demonstrating compliance with any parts where the Responsible Entity is not in direct control of meeting the obligation.
Since data can itself be lost while in transit between Control Centers, how does the updated language of Part 1.2 ensure that only the risks posed by the loss of the availability of data while in transit are in scope, as opposed to the risks posed by the loss of the data itself? This is critical in that data loss exposes a business to risks that have more to do with data protection and exposure (i.e. confidentiality & integrity) as opposed to the availability of that data.R1 Part 1.2 appears to only apply to the loss of data, not the loss of the availability of data.	Thank you for your question. The language, "Identification of method(s) used to mitigate the risk posed by loss of Real-time Assessment and Real-time monitoring data while such data is being transmitted between Control Centers;" puts the onus on the Responsible Entity to identify (in their own words) methods, within their plan, to mitigate the risks posed by loss of RTA and RTm data while in transit between CCs.
Do not the EOP-008 standards and specifically R1 and R7 meet the proposed actions in CIP-012? And TOP-001-5 R20 to R24? Did the SDT look at these?	Thank you for your question. As noted in the currently posted Consideration of Comments from the previous posting period, TOP, IRO, and EOP do address availability, but are focused on data exchange infrastructure within the primary control center and do not address data in motion between other Control Centers. In addition, the SDT has been charged with addressing the FERC directive which states in P3 "develop modifications to the CIP Reliability Standards to require protections regarding the availability of communication links and data communicated between bulk electric

	system Control Centers." Regarding your comment about EOP-008-2 and CIP-012; CIP-012 is about the Cyber protections between the Control Centers to provide for availability of data and not the, O&P required use of or ability to use that data. Yes, these Standards were considered within the standards development process.
R1.2 language is different from the posting vs slide 12. The posting states "...risk(s) posed by loss of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers" Slide 12 states "risk posed by loss of Real-time Assessment and Real-time monitoring date..."	Thank you for your comment. The webinar slides have been updated to reflect the current posting language.
Are the implementation guidelines going to provide specific examples of typical solutions to address availability?	Yes, and the Implementation Guidance is currently posted on the project page. Link to Implementation Guidance: Report (nerc.com)
Is it acceptable to use redundancy for R1.2? Other CIP standards do not allow the use of redundancy.	Yes, redundancy may be an acceptable means of achieving the security objective.
Regarding documenting the agreement - is that required in the standard?	Thank you for your question. Responsible Entities should be able to provide evidence demonstrating compliance with any parts, although documenting an agreement isn't explicitly required by the standard.
It was suggested that CIP-009 Recovery Plans could be leveraged as a recovery method for CIP-012 equipment. However, CIP-009 applies to BES Cyber Systems and their associated cyber assets, so this seems to expand scope. Is there an initiative to uniquely classify equipment used in an entity's CIP-012 program?	Thank you for your comment. As documented in the Implementation Guidance, the SDT recognizes that the availability components within the plan may or may not be applied to Cyber Assets identified as BES Cyber Assets. Please see the posted draft Implementation Guidance for more information.
If the data is in transit how do you prevent the loss of that data?	Thank you for your question. There is not a requirement to prevent the loss of data. The requirement is to mitigate the risk posed by the loss of RTA and RTm data while in transit between Control Centers.
The way the standard is drafted, per R1.3 is it implied that in cases where an entity is relying on a third-party to do something preventative to mitigate risk of loss per R1.2, is evidence of actual implementation by the third-party necessary (e.g. path redundancy via communication path diagrams or some technological protection to mitigate risk	Thank you for your question. A documented MOU or other agreement is one of the measures included in the draft standard; however there can be other ways to comply with the standard.

of loss) or would a documented MOU or other agreement alone suffice as acceptable evidence of implementation?	
Do Control Centers transmit data or do systems transmit data? Is the intent to protect ICCP data vs RTA/RTm data? Wouldn't it drive more clarity to protect ICCP data (energy system data) between entities systems?	Thank you for your question. CIP-012 is focused on the secure movement of RTA/RTm data between control centers regardless of protocol used.
As availability is the purview of operations, don't you think it is better suited to be handled in other MRS standards (e.g., IRO-010, TOP-003, TOP-001) or any other applicable standard within the Operations and Planning (O&P) stack of standards rather than in CIP standards (CIP-012)	SDT has been charged with addressing the FERC directive which states in P3 “develop modifications to the CIP Reliability Standards to require protections regarding the availability of communication links and data communicated between bulk electric system Control Centers.”
If we point to our O&P plans for CIP-012 compliance, then won't a single failure result in two separate regulatory violations?	Thank you for your question. The inclusion of components within an O&P or CIP plan in any other plan does not change the scope of applicability for either standard. Please see the draft Implementation Guidance.
if compliance to proposed CIP-012-2 is just pointing to existing plans for other standards, doesn't that strongly imply that there is no point/reason to revising CIP-012?	Thank you for your question. The suggestion of pointing to other plans does not imply that these plans would not need to be updated to cover the components required in CIP-012. The suggestion of utilizing other plans may be a way to decrease the administrative burden of compliance.
Isn't asset recovery under CIP-009 is different than link recovery....just wondering if CIP-009 can be applicable here.	Thank you for your question. The suggestion of pointing to other plans does not imply that these plans would not need to be updated to cover the components required in CIP-012. The suggestion of utilizing other plans may be a way to decrease the administrative burden of compliance.
Is there a difference between data and information?	Thank you for your question. There is a difference between data and information.
If an entity sends unencrypted RTA/RTm via a 3rd party such as a carrier or cloud provider, is that 3rd party, does that 3rd party have access to RTA/RTm and need an agreement?	Thank you for your question, please review CIP-012-1 R1.1.
R1.3 doesn't explicitly mention recovery drills. Is this an expectation of the plan to include?	Thank you for your question. At this time, recovery drills are not included in CIP-012. However, if your CIP-012 plan and or referenced SOP indicates that testing is performed, then you should follow your plan.

Has the IG been approved by NERC	Thank you for your question, CIP-012-1 IG was approved. CIP-012-2 IG will be submitted for ERO endorsement once the standard passes final ballot.
My prior question/concern is regarding the need to produce evidence of implementation by entities not subject to the CIP-012 standard (like a service provider - telco) and the expectation of Responsible Entities subject to the standards on behalf of those service providers.	Thank you for your comment. Third Party Organizations cannot be given the responsibility of meeting compliance for a Responsible Entity. That responsibility of compliance resides entirely with the owner of the Controls Centers. As an Example, a Responsible Entity may choose to have a MOU with a telecom company that states in the event of a communication link outage (e.g., backhoe hits line) that the telecom provider do "XYZ." The agreement of the action that will be taken in that event can be offered as evidence that the Responsible Entity has taken measures to prevent to the loss of RTA and RTM data. See Tech Rationale and IG for further examples.
If the data is in transit how do you prevent the loss of that data? Based on R1.2 which states "Identification of methods method(s) used to mitigate the risk(s) posed by loss of data used for the recovery of Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers;". So once that data has eft my control center I can no longer be responsible for it.	Thank you for your comment. The requirement is not to prevent the loss of data but rather identify methods used to mitigate the risks... The comment "So once that data has left my control center I can no longer be responsible for it" is precisely why this Requirement is being drafted. The idea that if you sent RTA/RTm data, that you no longer have any responsibility to make sure the entity needed the data received it, is false. This requirement is stating that a responsible entity needs to identify alternate measures to be used to ensure that the ability to send and receive data remains possible in a time frame in which the data is needed.
Is there a definition of a data center or associated data center?	Thank you for your comment. Data Center and Associated Data Centers are not defined in the NERC Glossary of Terms.