NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2020-04 Modifications to CIP-012 | Draft 2
Comment Period Start Date:	11/30/2021
Comment Period End Date:	1/24/2022
Associated Ballots:	2020-04 Modifications to CIP-012 CIP-012-2 AB 2 ST

There were 69 sets of responses, including comments from approximately 144 different people from approximately 94 companies representing 10 of the Industry Segments as shown in the table on the following pages.

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 Vice President of Engineering and Standards, Howard Gugel (via email) or at (404) 446-9693.

Questions

1. The SDT revised CIP-012-1 R1 to address the comments received during initial ballot and to meet the directives outlined in FERC Order No. 866 seeking to provide for the availability of real-time assessment and real-time monitoring data while in transit between control centers. Do you agree that the proposed language in R1 addresses security and availability as identified in FERC Order No. 866? If not please provide comments and suggested requirement language.

2. Do you believe that you can demonstrate compliance with R1.3 to identify where your availability protections are applied? If not please provide comments and suggested requirement language.

3. The SDT proposes that the modifications in CIP-012-2 meet the FERC directives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

4. The last ballot showed industry approval of the proposed 24-month implementation plan. Do you still agree the proposed timeframe is appropriate in light of the proposed revisions to the standard language? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

5. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale and implementation guidance document, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
DTE Energy - Detroit Edison Company	Adrian Raducea	5		DTE Energy - DTE Electric	Karie Barczak	DTE Energy - Detroit Edison Company	3	RF
					Adrian Raducea	DTE Energy - Detroit Edison	5	RF
					patricia ireland	DTE Energy	4	RF
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC

					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Santee Cooper	Chris Wagner	1		Santee Cooper	Jennifer Richards	Santee Cooper	1,3,5,6	SERC
					Rene' Free	Santee Cooper	1,3,5,6	SERC
CMS Energy - Consumers Energy Company	Jeanne Kurzynowski	3,4,5	RF	Consumers Energy Company	Jeanne Kurzynowski	Consumers Energy Company	1,3,4,5	RF
					Jim Anderson	Consumers Energy Company	1	RF
					Karl Blaszkowski	Consumers Energy Company	3	RF
					Theresa Martinez	Consumers Energy Company	4	RF
					David Greyerbiehl	Consumers Energy Company	5	RF
ACES Power Marketing	Jodirah Green	1,3,4,5,6			Bob Solomon	Hoosier Energy Rural	1	SERC

			MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations		Electric Cooperative, Inc.		
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					Susan Sosbe	Wabash Valley Power Association	3	RF
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
					Dominic Birk	Big Rivers Electric Corporation	1	SERC
					Kylee Kropp	Sunflower Electric	1	MRO

						Power Coorporation		
Public Utility District No. 1 of Chelan County	Joyce Gundry	3		CHPD	Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF

					Tricia Bynum	FirstEnergy - FirstEnergy Corporation	6	RF
					Mark Garza	FirstEnergy- FirstEnergy	4	RF
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern	6	SERC

						Company Generation		
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
Eversource Energy	Quintin Lee	1		Eversource Group	Quintin Lee	Eversource Energy	1	NPCC
					Christopher McKinnon	Eversource Energy	3	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee no NGrid	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC

David Burke	Orange & Rockland Utilities	3	NPCC
Helen Lainis	IESO	2	NPCC
David Kiguel	Independent	7	NPCC
Nick Kowalczyk	Orange and Rockland	1	NPCC
Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC

					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service	1	NPCC

						Electric and Gas Co.		
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
Dominion - Dominion	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion	3	NA - Not Applicable

Resources, Inc.						Resources, Inc.		
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable

1. The SDT revised CIP-012-1 R1 to address the comments received during initial ballot and to meet the directives outlined in FERC Order No. 866 seeking to provide for the availability of real-time assessment and real-time monitoring data while in transit between control centers. Do you agree that the proposed language in R1 addresses security and availability as identified in FERC Order No. 866? If not please provide comments and suggested requirement language.

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

While the language in R1 may address security and availability, the availability portion of this proposed standard is better suited for IRO-010, TOP-003, TOP-001 or any other applicable standard within the Operations and Planning suite of standards. Ensuring availability of communication links through redundancy and/or diversity is a significant departure in scope from the CIP standards. The CIP standards generally require controls and protections to be applied at the device level. This proposed language involves protections outside of the device and, in this case, the Entity's Electonic Security Perimeter.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. TOP and IRO 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. The revisions to CIP-012 will address elements that TOP and IRO do not address. 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." The SDT has developed language to help clarify that controls and protections are the focus of the requirement as it pertains to *availability*. The focus of CIP-012 is Control Center to Control Center communication and this communication may or may not take place outside of the ESP. Regardless of where the Control Center to Control Center communications occur, the communications must be protected.

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
There is currently no definition of "availability". AEPCO agrees with ACES comments of adding a NERC definition for "availability" or adoption a NIST definition.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. There is currently a NIST based definition of *availability* within the included Implementation Guidance. The SDT has refined this definition to better reflect industry feedback. Additionally, the word availability has been removed from the Standard language which now reflects the concept of availability rather than a direct reference to availability.	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	No
Document Name	
Comment	
Duke Energy does not believe the SDT revised CIP-012-1 in a way that best meets the directives outlined in FERC Order No. 866. The SDT's use of "availability protections" is unclear and would require further definition of this term versus referring to the NIST definition of *availability* defined as "ensuring timely and reliable access to and use of information". Using the language "security and availability protections" leaves us with questions. We prefer the language of FERC Order No. 822 specifically directing NERC to modify the Reliability Standards to require entities to implement controls to protect communication links and data communicated between BES Control Centers. FERC Order No. 866 conveys FERC's assertion that NERC did not address *availability*. We think that *availability* should be addressed using language that references	

controls to protect availability of communication links and data. Please see Question 5 below and our suggested rewording of sub requirement 1.2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has revised the R1 subpart language to focus upon “Identification of method(s) used to mitigate the risk” to better reflect the requirement for availability controls based on industry feedback. The SDT appreciates the inclusion of suggested language below in question 5.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
While the language in R1 may address security and availability, the availability portion of this proposed standard is better suited for IRO-010, TOP-003, TOP-001 or any other applicable standard within the Operations and Planning suite of standards. Ensuring availability of communication links through redundancy and/or diversity is a significant departure in scope from the CIP standards. The CIP standards generally require controls and protections to be applied at the device level. This proposed language involves protections outside of the device and, in this case, the Entity’s Electonic Security Perimeter.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. TOP and IRO 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. The revisions to CIP-012 will address elements that TOP and IRO do not address. 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." The SDT has developed language to help clarify that controls and protections are the focus of the requirement as it pertains to *availability*. The focus of CIP-012 is Control Center to Control Center communication and this communication may or may not take place outside of the ESP. Regardless of where the Control Center to Control Center communications occur, the communications must be protected.

Jennifer Malon - Black Hills Corporation - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

The proposed language states that entities are to have a plan to mitigate the risks of a loss of availability of data while being transmitted between control centers. As worded, this does not direct entities to implement redundant or highly avaialble communications infrastructure, which we believe is the intent of Order No. 866, but rather it directs entities to have a plan for mitigating the risks of a loss of avaialbility of the data. We would recommend making the availability directive a stand alone requirement.

Likes 3	Black Hills Corporation, 3, Stahl Don; Black Hills Corporation, 5, Silbaugh Derek; PNM Resources - Public Service Company of New Mexico, 3, Bratkovic Amy
Dislikes 0	

Response

Thank you for your comment. The SDT has revised the draft language based on feedback.

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No
Document Name	

Comment

Eversource supports the comments of EEI.

Likes 0	

Dislikes 0	
Response	
Please see response to EEI.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
We do not recommend adding availability to the scope of CIP-012, since availability of operational data is already addressed in other NERC Reliability Standards. This may be creating a conflict with other standards by including availability of data when we feel it is already included in other standards	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. While the TOP and IRO O&P Standards do address *availability* to an extent, they are scoped to data exchange infrastructure within the primary Control Center and do not address data in motion between other Control Centers. The revisions to CIP-012 address elements that TOP and IRO do not address. 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." The SDT has developed language to help clarify that "methods used to mitigate the risk" of loss is the focus of the requirement as they pertain to *availability*.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	

What exactly are “availability protections”? Can examples be provided?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Based on industry comments, the “availability protections” language has been revised to reflect a requirement for “Identification of method(s) used to mitigate the risk” associated with loss of communication links. This change should better allow entities the flexibility they need to meet the compliance and security objectives of the Standard. Please see the revised Implementation Guidance for examples.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO	
Answer	No
Document Name	
Comment	
The MRO NSRF (“NSRF”) generally agrees revised CIP-012-2 meets the FERC Order 866 directives; however, to be useful the term “availability” must be clarified in the requirements. While the NSRF appreciates the NIST definition of “availability” contained in the proposed Implementation Guidance, it is not certain that the Implementation Guidance will be endorsed by the ERO. Therefore, the NSRF recommends the SDT draft a formal definition of “Availability” for inclusion in the CIP-012-2 Standard, which could be the adoption of the NIST definition, or something similar. The NSRF recognizes the challenges and unintended consequences associated with “availability” being added as a new definition to the NERC Glossary of Terms since “availability” is used in other standards which could be impacted. In light of that, the NSRF suggests a definition be added (and limited in scope) to the CIP-012 standard itself. Additionally, clarification of “availability” could also be included in the Technical Rationale for CIP-012. The benefits of a definition include formalization within the Standard’s vernacular, thereby reducing potential ambiguity and likelihood of different interpretations by registered entities and audit teams. The NSRF also believes that the Measure M1 should provide examples of what types of evidence would meet the	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

availability requirement (e.g., an entity executing plans in support of the recovery of compromised communications links and the use of back-up communications capability when primary communications are unavailable). This would provide additional clarity to the industry.

Similarly, while having the concepts of "diversity, redundancy, or a combination of both" in the Implementation Guidance is needed, the NSRF recommends the SDT consider including the concepts in M1 to achieve a clearer measure of what constitutes meeting the requirement.

Proposed R1.2 requires identification of methods used for recovery, but the SDT fails to provide any examples of methods to recover a loss of a data link. The information currently contained in the Implementation Guidance is very broad and it would be helpful if examples are provided. Also, CIP-009 deals with CIP assets and restoration in the event of a loss but does not contain requirements regarding communications links and, therefore, is not applicable to CIP-012. The NSRF recommends clarifying language be added to show the relation between CIP-012 and CIP-009.

The NSRF recommends the SDT clarify within the Implementation Guidance at **Identification of Methods Used for the Recovery of Communication Links (R1.2)** the phrase "This objective is consistent with TOP and IRO O&P Standards" by identifying which standards are are being referenced.

The term "recovery" as used in R1.1.2 is very broad, and, as many entities will be dependent on telecommunication companies to restore communications, the NSRF recommends the SDT consider including a clause to mitigate compliance issues if a line goes down and it is not the entity's fault.

Additionally, the task of restoring availability predominantly resides with the telecommunication provider. In the event a communication link goes down, electric reliability entities are reliant on telecommunication provider to restore service. The NSRF requests the SDT add an exemption for links and equipment owned by telecommunication providers.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Thank you for your comments. The SDT appreciates the feedback. There is currently a NIST based definition of *availability* within the included Implementation Guidance. The SDT has refined this definition to better reflect industry feedback. The SDT asserts that because the term is being used within the context of a Cyber-Standard it should lend itself toward a cyber understanding of the term. The team has revised the measures in the latest CIP-012 draft to include more examples in order to provide additional clarity regarding availability and example controls around it. Please see the revised Implementation Guidance regarding carriers, diversity, recovery of links and other topics. Additionally, the revised language is focused now on identification of methods for recovery and examples of those methods are now in the Measures section of the draft Standard.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

Dominion Energy supports the comments from EEI. In addition, we would like to emphasize particular concern around the term "availability". This should be a defined term to eliminate ambiguity and reduce confusion. The current NIST definition used in the Technical Rational and the Implementation Guidance could be used as a basis for a definition.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. There is currently a NIST based definition of *availability* within the included Implementation Guidance. The SDT has refined this definition to better reflect industry feedback. The SDT asserts that because the term is being used within the context of a cyber-standard it should lend itself toward a cyber understanding of the term. In addition, the term “availability” has been removed from the Standard. The Requirements are now focused upon “identification of methods used to mitigate the risk posed by loss” and “Identification of methods to be used for recovery". This should better reflect the focus upon a results-based approach to maintaining Confidentiality, Integrity, and Availability.

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Although BPA supports the revisions made in the latest draft, the additional availability requirement is added into the standard with an 'and' statement and not clearly distinguished. Because availability requires significantly different controls than confidentiality or integrity, BPA recommends:

1. R1.1 should be maintained, as it is currently written, limited to confidentiality/integrity.

a) The Drafting Team should insert a new subpart (R1.2) for the availability requirement. This will assist both entities and auditors in a cleaner approach to implementation and assessing compliance.

b) The Drafting Team should insert a new subpart (R1.2) for the availability requirement. This will assist both entities and auditors in a cleaner approach to implementation and assessing compliance.

2. BPA appreciates that the SDT has clarified the definition of the term "availability" in the Technical Rationale and Implementation Guidance. However, the Requirement is confusing, and it is inconsistent with the approach taken for the existing confidentiality/integrity requirement:

a. The terms "confidentiality" and "integrity" are not used in R1.1; rather, they are described as "unauthorized disclosure" and "unauthorized modification", respectively. They are only linked to the cybersecurity terms of Confidentiality and Integrity in the Technical Rationale, for clarity. The Drafting Team should use the same approach for Availability.

b. “Availability” means different things to cybersecurity professionals and communications professionals (who will be interpreting and implementing this Requirement):

i. Availability in cybersecurity circles is ‘Ensuring timely and reliable access to and use of information.’ BPA agrees that this definition meets the intent of the FERC Order.

ii. Availability in communications circles is a ‘Quantitative measurement of the expected desirable performance criteria of a communications link/channel/system.’ (i.e., Block Error Rate < 10^-6, < 2 Serverly Error Seconds in 24 hours, 99.9999% uptime in any given year period, etc.) This definition doesn’t meet FERC’s intentions, but will be the first thing that comes to mind in telecom engineers who read it.

c. Because of this important and potentially confusing difference, BPA recommends that the SDT:

i. Replace “availability” in the new proposed subpart (R1.2, proposed above): “Identification of protection(s) used to ensure timely and reliable access to, and use of, Real-time Assessment and Real-time monitoring data while such data is being transmitted between Control Centers.”

ii. The term availability should only appear in the Technical Rationale and Implementation Guidance for additional clarity, as is already done for confidentiality and integrity.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Please see the responses below:

1. The SDT has revised the standard language as suggested.
2.
    a. The SDT has removed the term “Availability” from the requirement language as suggested and Implementation Guidance will reflect the availability concept within the context of subpart 1.2.
    b. The SDT has removed the term “Availability” from the requirement language. Please see IG and TR for an updated definition. Ensuring timely and reliable information. The “use of” phrase in the definition is more of an O&P component and will be removed from the revised definition.
    c. The SDT revised the language of subpart 1.2 to remove the word availability. Please see the updated IG and TR

Based on industry feedback, the STD has further modified the draft requirement subparts to include the availability component in its own subpart. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement for availability. The SDT appreciates the inclusion of alternate language for R1.2.

Joyce Gundry - Public Utility District No. 1 of Chelan County - 3, Group Name CHPD

Answer	No
Document Name	

Comment

While CHPD supports revisions made in the latest draft and appreciates the effort that went into consolidating R2 into R1, CHPD does not believe this revision best meets the directives of FERC Order No. 866. Because availability requires significantly different controls than confidentiality and integrity, CHPD recommends the SDT insert a new subpart (R1.2) for the availability protections requirement. This will assist both entities and auditors in a cleaner approach to implementing and assessing compliance.

CHPD appreciates that the SDT clarified the definition of the term “availability” in the Technical Rationale. However, R1 is confusing with regards to availability and inconsistent with the approach taken for the existing confidentiality/integrity requirement. The current revision remains ambiguous with the term “availability”. Availability should be addressed using language that references controls to protect availability of communication links and data. The Technical Rationale is helpful, and including its clear examples (e.g., “redundant communication links and data paths”) or adding a requirement table with a measures column with similar evidence examples would minimize inconsistent interpretations among Registered Entities and Regional Entities.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Based on industry feedback, the STD has further modified the draft requirement subparts to include the availability component within its own subpart. The revised language is focused now on “identification of methods to mitigate the risk of loss” of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Please see the

Implementation Guidance and Technical Rationale for the thought that went into defining availability and measures that can demonstrate availability much like CIP-012-1 has definitions for confidentiality and integrity within the IG.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
The scope of 'availability' is not clear and should be furher clairified in R1 or in the Technical Rationale and/or Implmenation Guidance. Noting on page 2 of the TR the SDT does reference TOP-001 and IRO-002 ("diversity, redundancy, or a combination of both"), but it is not clear what scope of availability is also required in R1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Based on industry feedback, the SDT has refined the context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement for availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the IG. Please see the updated Technical Rationale and Implementation Guidance.	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	

While the NSRF appreciates the NIST definition of "availability" contained in the proposed Implementation Guidance, the NSRF recommends the SDT draft a formal definition of "availability" for inclusion in the NERC Glossary of Terms, even if it entails adoption of the NIST definition, or something similar. By doing so, the new definition would be formalized within NERC's vernacular and within the Standard, thereby reducing potential ambiguity and likelihood of different interpretations by registered entities and audit teams.

Similarly, while having the concepts of "diversity, redundancy, or a combination of both" in the Implementation Guidance is needed, the NSRF recommends the SDT consider including the concepts in R1 to achieve a clearer requirement.

Proposed R1.2 requires identification of methods used for recovery, but the SDT fails to provide any examples of methods to recover a loss of a data link. The information currently contained in the Implementation Guidance is very broad and it would be helpful if examples are provided. Also, CIP-009 deals with CIP assets and restoration in the event of a loss but does not contain requirements regarding communications links and, therefore, is not applicable to CIP-012. The NSRF recommends clarifying language be added to show the relation between CIP-012 and CIP-009.

The NSRF recommends the SDT clarify within the Implementation Guidance at Identification of Methods Used for the Recovery of Communication Links (R1.2) the phrase "This objective is consistent with TOP and IRO O&P Standards" by identifying which standards are are being referenced.

The term "recovery" as used in R1.1.2 is very broad, and, as many entities will be dependent on telecommunication companies to restore communications, the NSRF recommends the SDT consider including a clause to mitigate compliance issues if a line goes down and it is not the entity's fault.

Additionally, much availability relies on Telecommunication Providers that in the event they go down, we are reliant on them to bring it back up. In the event a line or their telecommunication equiptment goes down, the Registered Entity does have to rely on them to bring it back up. The NSRF requests the SDT to add an exemption for links and equipment used by telecommunication providers.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Based on industry feedback, the SDT has refined the context of *availability* to better reflect the cyber security objective of the Requirement. The revised language removes the word availability from the Standard language and is focused now on “identification of methods to mitigate the risk of loss” of availability. Examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. The SDT asserts that because the term is being used within the context of a cyber-standard it should lend itself toward a cyber understanding of the term. Please see the revised Implementation Guidance and Technical Rationale updated to reflect these and other suggested changes.

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

While AEP agrees that R1 addresses both security and availability concerns as identified in FERC Order No. 866, potential scope creep could exist within Requirement R1.1, as it is not explicity stated that loss of data availability is due to communication link failure. Data loss can occur for a variety of of reasons, and as such, AEP recommends that R1.1 specify that data loss is due to communication link unavailability.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Based on industry feedback, the SDT has refined the context of *availability* to better reflect the cyber security objective of the Requirement. The revised language removes the word availability from the Standard language and is focused now on "identification of methods to mitigate the risk of loss" of availability.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST believes the proposed language in R1 does not fully address FERC Order 866. The Order directs NERC to modify CIP-012 to address availability of communications links and the data they carry while it's in transit. The proposed "combination" requirement to address data confidentiality, integrity, and availability fails to identify communications links between in-scope Control Centers as requiring availability protections. The need to do so is implied in R1.2, but N&ST believes this should be made explicit. In addition, R1's proposed language does not identify any requirement for a Responsible Entity's CIP-012 plan(s) to include provisions for continuity of operations, as directed by the FERC Order.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Based on feedback received in this comment period, the Standard Drafting Team has revised the subparts of Requirement R1 to refine the context of *availability* to better reflect the cyber security objective of the Requirement. The revised language removes the word availability from the Standard language and is focused now on "identification of methods to mitigate the risk of loss" of availability. Continuity of Operations is addressed in implementing "methods to mitigate the risk of loss". Provided that an entity's methods preserve or restore the flow of data in a timely manner, continuity of operations is achieved.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	

BC Hydro appreciates the opportunity to comment and provides the following comments.

Although the Requirement 2 wording from Draft 2 of CIP-012-2 is removed however it appears that the wording of the Requirement 2 from Draft 1 has only been moved or merged into Requirement 1 of Draft 2. BC Hydro's previous concerns raised on CIP-012-2 Draft 1 appear to still hold valid. The changes in Requirement 1 in Draft 2 of CIP-012-2 still imply a possible reliance on redundancy, which does not align with the approach taken in the other existing CIP standards, particularly CIP 002-5.1a. As availability is the purview of operations, it would be better suited to other MRS standards (e.g., IRO-010, TOP-003, TOP-001) or other applicable Standard(s) within the Operations and Planning (O&P) domain..

BC Hydro recommends removing the 'availability' requirement from CIP-012-2 and revising other MRS standards to address this need as appropriate.

Alternatively BC Hydro suggests providing a clear understanding of the term 'availability' and a clarity that it does not imply the use of redundant setups. For most of the entities, 'availability' of communication networks depends on 3rd party telecommunication providers and in the event of a line or telecommunication equipment going down, the entity is reliant on the 3rd party telecommunication providers to fix the problems. BC Hydro suggests that SDT include an exemption for the links and equipment used by 3rd party telecommunication providers as changing or enhancing the third party telecommunication infrastructure to support 'availability' may not be feasible for many entities.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. 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.” The SDT has modified the Requirement language to help clarify that controls and protections are the focus of the requirement as it pertains to *availability*. The Standard Drafting Team has also revised the subparts of Requirement R1 to refine the context of *availability* to better reflect the cyber security objective of the Requirement. Please see the updated Technical Rationale and Implementation Guidance.

Larry Watt - Lakeland Electric - 1

Answer	No

Document Name	
Comment	
Availability should be handled as part of the TOP or EOP series of standards and does not belong in the CIP Standards. In fact, response to unavailability is already built into standards of the TOP/EOP series.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. 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." TOP and IRO 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. The revisions to CIP-012 are addressing elements that TOP and IRO do not address.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
While we agree the proposed language in R1 addresses the availability modifications being proposed in this draft to meet FERC Order No. 866, the definition of "availability" is not a NERC defined term. Providing an alternative standard's term definition does not provide an avenue to meet strict NERC CIP compliance. To aid Entities, a formal definition of "availability" should be adopted to the NERC Glossary. By defining "availability", it alleviates the potential of differing interpretations of the term. R1.1.2 is too broad in using the term "recovery". Entities are more often dependent on telecommunication providers to restore communications when a circuit goes down between Control Centers. This is due to the number of physical mediums and cyber assets data	

traverses from Control Center to Control Center. There should be an exception in the requirement allowing for restoration issues outside of the control of the entity being required to comply.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has worked to refine the NIST definition of availability to better reflect industry feedback and included it in the Implementation Guidance. Additionally, the word availability has been removed from the Standard language which now reflects the concept of availability rather than a direct reference to availability. Based on feedback received in this comment period, the Standard Drafting Team has also revised the subparts of Requirement R1 to refine the context of *availability* to better reflect the cyber security objective of the Requirement. The revised language removes the word *availability* from the Standard language and is focused now on "identification of methods to mitigate the risk of loss" of availability. These changes combined with the Requirement R1 language to "implement…one or more documented plan(s)", aligns the focus of the requirements on having a plan to mitigate risks, which is better aligned with a results based approach.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the response to EEI.	
Kinte Whitehead - Exelon - 3	

Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the response to EEI.	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	

Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the response to EEI.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No: As mentioned by others and NCPA agress that availability is not well defined and can have multi meanings and expectations relating to the standards.	
Likes 0	
Dislikes 0	
Response	
Based on feedback received in this comment period, the Standard Drafting Team has revised the subparts of Requirement R1 to refine the context of *availability* to better reflect the cyber security objective of the Requirement. The revised language removes the word *availability* from the Standard language and is focused now on "identification of methods to mitigate the risk of loss" of availability. These changes combined with the Requirement R1 language to "implement…one or more documented plan(s)", aligns the focus of the requirements on having a plan to mitigate risks, which is better aligned with a results-based approach.	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	No

Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT's response to MRO NERC Standards Review Forum.	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
SCPSA believes that the previous version of the CIP-002-2 draft addressed FERC Order No. 866 more effectively. Integrating the security and availability components into a single requirement potentially leads to confusion because the methods of implementation for security and availability protections are different. Furthermore, the term "availability protections" is unclear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has revised the language of the Requirements to better reflect the feedback received from the industry as a whole. Based on industry comments, the "availability protections" language is being revised to reflect a requirement for "Identification of method(s) used to mitigate the risk" associated with loss of communication links. This change should better allow entities the flexibility they need to meet the compliance and security objectives of the Standard. Please see the revised Implementation Guidance for examples.	

James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
LCRA believes that the term “Availability” in this context, offers unnecessary opaqueness. Similarly, the NIST definition provided in the Technical Rational which states “Ensuring timely and reliable access to and use of information” is vague and lacks actionable direction. Furthermore, entities have little to no control over the availability of communication networks. Entities can, however, provide redundancy. The SDT may benefit from using explicit terms that cannot be misinterpreted by the different industry segments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Based on industry feedback, the SDT has refined the context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on “identification of methods to mitigate the risk of loss” of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG. Please see the updated Technical Rationale and Implementation Guidance.	
Teresa Krabe - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
LCRA believes that the term “Availability” in this context, offers unnecessary opaqueness. Similarly, the NIST definition provided in the Technical Rational which states “Ensuring timely and reliable access to and use of information” is vague and lacks actionable direction.	

Furthermore, entities have little to no control over the availability of communication networks. Entities can, however, provide redundancy. The SDT may benefit from using explicit terms that cannot be misinterpreted by the different industry segments.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Based on industry feedback, the SDT has refined the context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG. Please see the updated Technical Rationale and Implementation Guidance.

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

While we agree the proposed language in R1 addresses the availability modifications being proposed in this draft to meet FERC Order No. 866, the definition of "availability" is not a NERC defined term. Providing an alternative standard's term definition does not provide an avenue to meet strict NERC CIP compliance. To aid entities, ACES believes a formal definition of "availability" be adopted to the NERC Glossary. By defning "availability", it alieves the potential of differing interpretations of the term.

Further, ACES believes R1.1.2 is too broad in using the term "recovery". Entities, are more often dependent on it's telecommunication providers to restore communications when a circuit goes down between Control Centers. This is due to the number of physical mediums and cyber assets data traverses from Control Center to Control Center. There should be an exception in the requirement allowing for restoration issues outside of the control of the entity being required to comply.

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Based on industry feedback, the SDT is refining the context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Neville Bowen, Ocala Utility Services, 3; - LaKenya VanNorman	
Answer	No
Document Name	
Comment	
Availability should be handled as part of the TOP or EOP series of standards and does not belong in the CIP Standards. In fact, response to unavailability is already built into standards of the TOP/EOP series.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. 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."	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee no NGrid	
Answer	No

Document Name	
Comment	
The inclusion of “availability” in R1 is not well defined. R1’s availability is subtly but importantly different than the question. The question adds “data while in transit between control centers.” We recommend adding this language to R1. Per previous feedback, in most cases, communications between Control Centers are handled by a third party. If that third party cannot provide communications, the Service Level Agreement provides compensation but does not guarantee availability. IRO-002 and TOP-001 already have Requirements that mandate diversity and redundancy as they pertain to communications. It is not clear that diversity and redundancy equate to availability. We recommend removing availability from CIP-012 since other Standards cover this topic OR moving availability to other Standard(s)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Based on industry feedback, the SDT has refined the context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on “identification of methods to mitigate the risk of loss” of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	

PG&E supports the comments provided by the Edison Electric Institute (EEI) related to the undefined term “availability” and the proposed modifications to R1. As EEI indicated in their comments, dividing R1 into two (2) sub-parts and changing “availability protection” with “availability controls, or another term that better aligns with NERC’s results based standards philosophy and does not inappropriately cause confusion with entity internal controls” helps remove the subjectiveness of just “availability protections”. This would allow the entity to indicate the “controls” to meet “availability” which could be measured more easily than “protections”,	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GTC finds the term ‘availability protections,’ as used in the proposed language to be lacking in specificity or unsupported by industry standard terminology. For the purposes of clarity, in order to eliminate the need for the inexact term ‘availability protections,’ while still capturing the requirements of Order 866, GTC proposes the following alternate language for Requirement 1.1: “Identification of protections used to mitigates risks posed by: (1) unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers; and (2) loss of availability of Real-time Assessment and Real time monitoring data while being transmitted between Control Centers.”	

GTC has identified similar use of the term ‘availabiltiy protections’ in Requirement 1.4, and similarly proposes the following alternate language: “If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying the protections as required in Part 1.1.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Based on industry feedback, the SDT has refined the context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on “identification of methods to mitigate the risk of loss” of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics. Based on feedback the SDT has modified the subparts to include the availability component within its own subpart.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No
Document Name	
Comment	
See EEI Comments.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
While EEI appreciates the changes made to CIP-012, Requirement R1; additional modifications are still needed to ensure that entities have adequate flexibility to demonstrate that availability is fully addressed and provides responsible entities with results-based requirements that are achievable and clearly defined. For this reason, we suggest that the SDT consider splitting Requirement R1, subpart 1.1 (as indicated below) and substitute “availability protection” with the term “availability controls”. Such a change, in the context of availability, is important because protections for availability are subjective whereas making availability controls is something that is regardless of the approach is achievable and clearly understood. **R1.1** Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers; **R1.2** (proposed new) Identification of availability controls used to mitigate the risk posed by loss of availability of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers; Additionally, the use of Measures supporting these two requirements provided above would alleviate the regulatory certainty concerns many companies are facing with the proposed language used in the 2nd Draft. As examples of measures that could be developed to support the two requirement above are as follows: (1.1) Security Protectiion • Identification of points where encryption/decryption of the data occurs at either a transport, network, or application layer.	

- Physical access restrictions to unencrypted portions of the network

(1.2) Availability Controls

- Network diagrams showing redundancy of paths between Control Centers
- Procedures explaining the use of alternative systems or methods for providing for the availability of the data
- Service-level agreements with carriers containing high availability provisions

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT has modified the subparts and expanded the measures section to include examples for each subpart as suggested.

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT agrees with the IRC SRC comments regarding a common understanding of the use of "availability" within the standard. ERCOT notes, however, that promoting availability consists of actions and measures to provide redundancy and diversity rather than a specific metric.

In Paragraph 16 of Order No. 866, FERC identified a gap concerning the availability of communication links and data communicated between bulk electric system Control Centers. In Paragraph 33, FERC clarifies the intent of its directive to NERC to "address the risks associated with the availability of communication links and data communicated between all bulk electric system Control Centers . . . ." As stated in its previous comments, ERCOT believes FERC's intent of "availability" is to identify a proactive approach to promote the continuity of operations through availability of communication links and, relatedly, the data passing through those links. The technical guidance provides similar insight to understanding "availability" where, on page 2 (pdf page 10), the technical guidance explains availability and states that this standard should mitigate the risk posed by the loss of "data flow." However, the proposed standard revisions may not achieve that same level of understanding of "availability" within the standard itself, as explained in the IRC SRC comments. Availability is not necessarily an object to be measured, but rather a process illustrated by providing redundancy and diversity to provide for the continuity of operations if the primary communication link is lost or compromised.

ERCOT provides the following language (with explanations in brackets at the end of each paragraph/part), which leaves the security protection of data the same as in the current version of the standard and addresses the concept of promoting availability as well as establishing an identification/recovery process as noted by FERC in Paragraph 35 of Order No. 866.

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure, unauthorized modification, and loss of availability of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: ***[same language as provided in Nov 2021 Draft]***

1.1. Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of data used for Real-time Assessment and Real-time monitoring data while such data is being transmitted between Control Centers; ***[identical to approved CIP-012-1, Part 1.1]***

1.2. Identification of measures to promote the availability of communication links used to transmit Real-time Assessment and Real-time monitoring data between Control Centers, including use of redundant or backup communication capability between Control Centers in the event of an unavailable or compromised communication link between Control Centers; ***[new Part to address availability]***

1.3. Identification of a process to identify and recover unavailable or compromised communication links used to transmit Real-time Assessment and Real-time monitoring data between Control Centers; ***[from Nov 2021 Draft Part 1.2, with some modifications to address recovery as a process]***

1.4. Identification of where the Responsible Entity applied security protection as required in Part 1.1; and ***[from Nov 2021 Draft Part 1.2, modified to be consistent with CIP-012-1, Part 1.2]***

1.5. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection as required in Part 1.1, identifying availability measures as required in Part 1.2, and identifying of a process to identify and recover communication links as required in Part 1.3. ***[similar to and consistent with CIP-012-1, Part 1.3]***

Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Based on industry feedback, the SDT has refined the language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on “identification of methods to mitigate the risk of loss” of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
PNMR supports EEI comments and proposed lanuguage for CIP-012-2 R1. If the STD rejects the proposed EEI language, PNMR recommends defining availability and a restoration metric.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Benjamin Winslett - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	CIP-012-2 Comment Form (Final Draft).docx
Comment	

GSOC finds the term 'availability protections,' as used in the proposed language to be lacking in specificity or unsupported by industry standard terminology. For the purposes of clarity and to eliminate the need for the inexact term 'availability protections,' while still capturing the requirements of Order 866, GSOC proposes the following alternate language for Requirement 1.1:

"Identification of protections used to mitigates risks posed by: (1) unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers; and (2) loss of availability of Real-time Assessment and Real time monitoring data while being transmitted between Control Centers."

GSOC has identified similar use of the term 'availabiltiy protections' in Requirement 1.4, and, similarly, proposes the following alternate language:

"If the Control Centers are owned or operated by different Responsible

Entities, identification of the responsibilities of each Responsible Entity for

applying the protections as required in Part 1.1."

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for

confidentiality and integrity within the V1 IG. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
I support the comments submitted by Sean Erickson (WAPA).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to WAPA.	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
A. We do not agree with the draft language proposed. Once RTA/RTm data has left the physical Control Center or associated data center equipment, an entity relies on intermediary companies such as Telecom carriers to ensure availability of data communication paths for RTA/RTm data between Control Centers. Therefore they have no control over the operation, maintenance or availability of such equipment nor the availability. Identifying methods used to recover communication links does not at all ensure the availability of those paths – which is the intent of the requirement. Entities already have to comply to TOP-001-5 R20 to R24 to ensure said data exchange protections of RTA/RTm exists. Secondly, entity's must protect BES Cyber System Information in CIP-011 and CIP-004.	

We recommend the SDT remove or revise the term availability, or add a requirement to have “at lease 2 or more communications paths between Control Centers.” We also recommend the SDT provide technical guidance related to RTA/RTm being BES Cyber System Information.

B. Without prescribing encryption of RTA/RTm and key management, entities have no control of such RTA/RTm data beyond the last managed and maintained communication equipment interface. Therefore entities will not be able to meet the requirements of confidentiality and integrity as they are giving information to others beyond the entity’s control. This becomes a zero defect situation because an entity will not be able to guarantee that RTA/RTm data was compromised.

We Recommend that the SDT change the language to include the word “potential” confidentiality and integrity. This would allow entities to determine, implement and document a best effort set of security controls and clarify for industry and regulators that encryption and key management is or is not required.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on “identification of methods to mitigate the risk of loss” of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG. Confidentiality and integrity is already in the approved standard going into effect on July 1, 2022.

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institute's (EEI) response to Question 1. Evergy would also suggest that the drafting team consider including their final definition of "availability" in the standard itself. Given that Implementation Guidance represents one way to meet compliance, a definition that is fundamental to the interpretation of the standard is not appropriately captu red in Implementation Guidance. documents have not been approved by NERC for over a year, including it in the standard itself would provide the clarity that entities will need to implement this change.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Southern Company strongly disagrees with asking for **Availability** to be defined. We are aligned with EEI in most of our comment that follows, but please note some important differences in the proposed language.

We feel additional modifications are needed to ensure that entities have adequate flexibility to demonstrate that availabilit y is fully addressed and provides responsible entities with results-based requirements that are achievable and clearly defined. For this reason, we suggest that the SDT consider splitting Requirement R1, subpart 1.1 (as indicated below) and substitute *"availability protection"* with the term **"availability provisions"**. Such a change, in the context of availability, is important because protections for availability are subjective whereas making ***availability provisions*** is something that, regardless of the approach, is achievable and clearly understood. To address the above concern, we suggest that R1.1 could be split. Note the following suggested Language:

R1.1 Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

R1.2 (new) Identification of availability provisions used to mitigate the risk posed by loss of availability of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

Additionally, the use the Measures supporting these two Requirements provided above would alleviate the regulatory certainty concerns many companies are facing with the proposed language used in the 2nd Draft. As examples of Measures that could be developed to support the two requirement above are as follows:

M1. Examples of evidence may include, but are not limited to:

(1.1) Security Protections

- Identification of points where encryption/decryption of the data occurs at either a transport, network, or application layer.
- Physical access restrictions to unencrypted portions of the network

(1.2) Availability Provisions

- Network diagrams showing redundancy of paths between Control Centers
- Procedures explaining the use of alternative systems or methods for providing for the availability of the data
- Service-level agreements with carriers containing high availability provisions

(1.3) <and the rest>	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI. The SDT considered availability provisions, but ultimately went with "methods used to mitigate the risk" to better align with the language in other standards.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee no NGrid's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see response to NPCC Regional Standards Committee.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We believe it is unclear what controls are required to protect the availability associated with communication of real -time assessment and real-time monitoring data, as this is not a defined term in the NERC CIP glossary of terms. In addition, examples of protections are not	

provided in the revision of this standard. Is the expectation of the SDT that there be redundant paths of communication between control centers, as well as a plan for failure or loss of both of those communication paths?

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG.

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	Yes
Document Name	

Comment

Manitoba Hydro agrees with the language in R1. The language could be simplified by eliminating sub-requirement R1.3 and combining with R1.1 directly. Current language: R1.3 "Identification of where the Responsible Entity applied security and availability protection(s) as required in Part 1.1" . Proposed modification to R.1.1: Identification of security and availability protection(s), including where protections are applied, used to mitigate the risks posed by unauthorized disclosure and, unauthorized modification, and loss of availability of data used for Real-time Assessment and Real-time monitoring data while such data is being transmitted between Control Centers

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT has modified the language based on industry feedback.

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Reclamation recommends that communications paths between Control Centers be on physically separated, redundant communications paths where feasible. Reclamation also recommends third-party vendors be included to ensure all parties are covered.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes that the draft language proposed in this draft allows for this approach. Please see the update d Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
While IESO supports the comments submitted by the ISO/RTO Council SRC and NPCC, we further amend those comments by suggesting that “availability” be considered “as defined by the Responsible Entity” within the proposed standard. This is already implied in the proposed wording, thus IESO supports the proposed standard, however an explicit statement would further clarify this	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The term availability has been removed from the proposed language. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on “identification of methods to mitigate the risk of loss” of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	

Comment

The NAGF recommends that the SDT either define availability or integrate language into the Standard that addresses how availability is to be accomplished.

Likes 0

Dislikes 0

Response

Thank you for your comment. The term availability has been removed from the proposed language. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on “identification of methods to mitigate the risk of loss” of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG.

Adrian Raducea - DTE Energy - Detroit Edison Company - 5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Matthew Jaramilla - Salt River Project - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Daniela Hammons - CenterPoint Energy Houston Electric, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joseph Amato - Joseph Amato On Behalf of: Terry Harbour, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4	
Answer	
Document Name	
Comment	
MGE does not support the defining of the word "availability", as the NIST definition is sufficient.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the updated Implementation Guidance regarding the definition of availability.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment	
Texas RE appreciates the Standard Drafting Team's (SDT) modifications to proposed CIP-012-2, R 1.1 to better address the identification of security and availability protections to mitigate the risks posed by, among other things, the loss of availability of data us ed for Real-time Assessments and Real-time monitoring. Texas RE further appreciates the proposed changes to CIP-012-2, R 1.2 requiring "[i]dentification of methods to be used for the recovery of communication links used to transmit Real -time Assessment and Real-time monitoring data between Control Centers." Texas RE notes, however, that CIP-012-2, R1.2's focus on "recovery" may not encompass the full range of proactive scenarios to ensure communications link availability. For instance, entities may need to consider eliminating single points of failure in their communication links to ensure "communication link availability" rather than simply focusing on recovery from a link outage. Texas RE recommends the SDT consider adopting explicit language requiring strategies to implement communication link availability in C IP-012-2, R 1.2 similar to that proposed by FERC in Order No. 866, paragraph 3.	
Likes 1	PNM Resources - Public Service Company of New Mexico, 3, Bratkovic Amy
Dislikes 0	
Response	
Thank you for your comments. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to be used for the recovery of communication links" and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP -012-1 has definitions for confidentiality and integrity within the V1 IG.	

2. Do you believe that you can demonstrate compliance with R1.3 to identify where your availability protections are applied? If not please provide comments and suggested requirement language.

David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
For us this would be dependent on the SDT response to our commnets in Question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to question 1.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee no NGrid's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to NPCC Regional Standards Committee.	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company is concerned that Requirement R1.3 as currently proposed would create compliance problems, however, replacing the term availability protections with availability provisions would resolve this concern. (See our response to Question 1.)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to question 1.	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institute's (EEI) response to Question 2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Erin Green - Western Area Power Administration - 1,6	

Answer	No
Document Name	
Comment	
I support the comments submitted by Sean Erickson (WAPA).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to WAPA.	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
PNMR supports EEI comments. Protections should be replaced with controls. Or "Identify methods to address the risk of loss of RTA and RTm data between contorls centers.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI. The SDT has revised the draft language based on industry comments.	
Dana Showalter - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	

Comment	
As stated in comments to question 1, availability is not an object to be measured, but rather a process illustrated by providing redundancy and diversity to provide for the continuity of operations if the primary communication link is lost or compromised.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes that the draft language proposed in this draft allows for this approach. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI is concerned that Requirement R1.3 as currently proposed would create compliance problems, however, replacing the term availability protections with availability controls would resolve this concern. (See our response to Question 1.)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to question 1.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No
Document Name	

Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E supports the comments submitted by the Edison Electric Institute (EEI) comments that indicated the term “availability” is subjective in the context in which it is used and may create confusion for registered entities leading to inconsistent compliance enforcement actions. Refer to our response to Q1 for more details.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI and response to question 1.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee no NGrid	
Answer	No
Document Name	
Comment	

"Availability" is not well defined. Availability of data? Availability of the application? See feedback to question 1 The double jeopardy question with IRO and TOP Standards needs addressing. The SDT's December 8, 2021 webinar raised this question. We recommend removing availability from CIP-012 since other Standards cover this topic OR moving availability to other Standard(s) How does CIP-012 distinctly cover any gaps that are not covered in other Standards?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG. In revising the context around availability and its focus on a cyber context, the SDT believe that the draft language addresses the issue of double jeopardy. TOP and IRO 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.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Neville Bowen, Ocala Utility Services, 3; - LaKenya VanNorman	
Answer	No
Document Name	
Comment	

Availably protections seem to boil down to 'redundant and divergently routed' connectivity. As it is common to use the limite d number of commercial paths between Control Centers and a customer cannot be 100% sure of the current path it will be difficult to prove compliance.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The revised draft language and its focus on the “identification of methods used to mitigate the r isk” addresses this concern.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
Again, most often entities depend on external communication providers for availabity of data between Control Centers. This further supports the need for an exceptmption when communication provider’s links fail. A Registered Entity has no control over how or when a communication path will be restored in this case and therefore strict compliance is difficult or impossible to achieve.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The revised draft language and its focus on the “identification of methods used to mitigate the r isk” addresses this concern. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity o f links, and similar topics.	
Teresa Krabe - Lower Colorado River Authority - 1,5	
Answer	No

Document Name	
Comment	
LCRA has similar concerns to what was raised in response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to question 1.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
LCRA has similar concerns to what was raised in response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to question 1.	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	No
Document Name	
Comment	

MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to MRO NSRF.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
Without further clarity on the definition of "availability", organizations will have issues with consistently scoping the controls to be applied and the documentation to demonstrate compliance.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No

Document Name	
Comment	
The term "availability" is subjective in the context in which it is used and may create confusion for registered entities leading to inconsistent compliance enforcement. ITC recommends a definition for the term "availability" be developed within the Reliability Standard itself.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
When a third party is providing the availability protections, the specific components/details may be unknown and the monitoring / troubleshooting /resolution of availability issues would be outside of the registered entity's purview.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The revised draft language and its focus on the "identification of methods used to mitigate the risk" addresses this concern. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

No: As mentioned above NCPA does not believe this can be answers until availability has been better defined.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG.

Becky Webb - Exelon - 6

Answer	No
Document Name	

Comment

Exelon has chosen to align with EEI in response to this question.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment, please see response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
Again, most often Entities depend on external communication providers for availability of data between Control Centers. This further supports the need for an exception when communication provider's links fail. A Registered Entity has no control over how or w hen a communication path will be restored in this case and therefore strict compliance is difficult or impossible to achieve.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The revised draft language and its focus on the “identification of methods used to mitigate the risk” addresses this concern. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Larry Watt - Lakeland Electric - 1	
Answer	No
Document Name	
Comment	
Availably protections seem to boil down to 'redundant and divergently routed' connectivity. As it is common to use the limited number of commercial paths between Control Centers and a customer cannot be 100% sure of the current path it will be difficult to prove compliance.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on “identification of methods to mitigate the risk of loss” of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
CIP-012-1 is not yet in effect in British Columbia and BC Hydro has not implemented a solution to comply with CIP-012-1 yet. This question on compliance will be difficult to address at this stage and will be best answered once CIP-012-1 has been designed and implemented. As	

identified in response to Question # 1, BC Hydro suggests that SDT add an exemption for the links and equipment used by 3rd party telecommunication providers.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The revised draft language and its focus on the "identification of methods used to mitigate the risk" addresses this concern. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST believes this could be a difficult question to answer for some Responsible Entities, depending on their approach(s) to addressing availability protection. If the mainstay of an Entity's CIP-012 availability protection plan is a service level agreement with a wide-area communications carrier (an option the FERC Order suggests but appears to have been ignored by the SDT), the "where" of that Entity's protections would be in its contractual document. Similarly, the "where" might be within an Entity's disaster recovery procedures defined for its communications and networking infrastructure. N&ST believes it is neither practical nor necessary to compel Responsible Entities to identify the "where" of its availability protections, and we therefore recommend that it be removed from R1.3. We believe R1.1's requirement to identify and describe availability protections is sufficient.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has revised the draft language to focus upon "methods used to mitigate the risks". Examples given in the measures section address this concern.	

Bryan Koyle - Southern Indiana Gas and Electric Co. - 6 - RF	
Answer	No
Document Name	
Comment	
Demonstrating compliance will be difficult to prove if the communication link is provided by a third party.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has revised the draft language to focus upon “methods used to mitigate the risks”. Examples given in the measures section address this concern.	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP believes it could demonstrate compliance with Requirement R1.3 if the language from the Techincal Rationale document on page 9 under General Considerations for Requirement R1 is added to the the R1 measurement language. AEP recommends M1 read as follows: Evidence may include, but is not limited to, documented plan(s) that meet the mitigation objective of Requirement R1 and documentation demonstrating the implementation of the plan(s). *Identification of where the Responsible Entity applied security and availability protection(s) as required in Part 1.1. can be accomplished with a document describing the locations of the components, diagrams indicating the locations or a combination of both, within the plan.*	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has revised the draft requirements and measures based on industry feedback.	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
In many instances, availability relies on telecommunication providers; and in the event service is interrupted, Registered Entities are solely reliant on the telecom providers to bring service back up. Similarly, in the event a line or telecommunication equiptment goes down, the Registered Entity is again reliant on the telecommunication providers to fix the issues. NSRF requests the SDT add an exemption for the links and equipment used by telecommunication providers.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The revised draft language and its focus on the “identification of methods used to mitigate the risk” addresses this concern. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	

The scope identification of availability protections is not clear for entities using 3rd party telecommunction networks. This should be further clarified in R1 or the Technical Rationale and/or Implmentation Guidance.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The revised draft language and its focus on the "identification of methods used to mitigate the risk" addresses this concern. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Joyce Gundry - Public Utility District No. 1 of Chelan County - 3, Group Name CHPD	
Answer	No
Document Name	
Comment	
CHPD has concerns demonstrating compliance for "security protections" in the common scenario where the Reliability Coordinator contracts with a telecommunications company for communication links between Control Centers operated by different Registered Entities. These Registered Entities depend on the telecommunication company to implement the security protections and do not have direct access to evidence that it is in place and functioning. With more descriptive "availability protections" requirement language, CHPD could more confidently demonstrate "availability protections" compliance. Possible ways of clarifying include using alternate wording from the Technical Rationale (e.g., "redundant communication links and data paths") or adding a requirements table with a measures column with evidence examples to minimize inconsistent interpretations among Registered Entities and Regional Entities.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The revised draft language and its focus on the “identification of methods used to mitigate the risk” addresses this concern. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Daniela Hammons - CenterPoint Energy Houston Electric, LLC - 1	
Answer	No
Document Name	
Comment	
Demonstrating compliance will be difficult to prove if the communication link is provided by a third party.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The revised draft language and its focus on the “identification of methods used to mitigate the risk” addresses this concern. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO	
Answer	No
Document Name	
Comment	
The NSRF requests the SDT add an exemption for the links and equipment owned by telecommunication providers. In many instances, availability resides with telecommunication providers; and in the event service is interrupted, Registered Entities are reliant on the telecommunication provider(s) to restore service. Similarly, in the event a telecommunication line or other piece of telecommunication equipment goes down, the Registered Entity is again reliant on the Telecommunication Provider(s) to address the issue(s).	

The term "availability" is subjective and should be clearly defined prior to approving CIP-012-2.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Thank you for your comment. The revised draft language and its focus on the "identification of methods used to mitigate the risk" addresses this concern. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
What exactly are "availability protections"? Can examples be provided?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a	

measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
We do not recommend adding availability to the scope of CIP-012, since availability of operational data is already addressed in other NERC Reliability Standards. Concept of availability between control centers would need to be clarified.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. TOP and IRO 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.”	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
Eversource supports the comments of EEI.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see response to EEI.	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	No
Document Name	
Comment	
Without access to the equipment CE doesn't own, CE cannot definitively demonstrate that the compliance has been achieved.	
Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	
Response	
Thank you for your comment. The revised draft language and its focus on the "identification of methods used to mitigate the risk" addresses this concern. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Jennifer Malon - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Black Hills Corporation has concerns with R1.1 with regards to the scenario where vendors like CAISO and SPP are providing the communications infrastructure. Entities would be relying on the vendors to implement the security (and avaialbility) protections and the entity will not have direct access to evidence that it is in place and functional.	
Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response	
Thank you for your comment. The revised draft language and its focus on the “identification of methods used to mitigate the risk” addresses this concern. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	No
Document Name	
Comment	
Duke Energy takes issue with the term “availability protections” and not with the concept of availability. We prefer addressing the “where” in our rewording of sub requirement 1.4 as provided in Question 5 below.	
Likes 1	PNM Resources - Public Service Company of New Mexico, 3, Bratkovic Amy
Dislikes 0	
Response	
Thank you for your comment. Please see response to question 5 below.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
Entities are dependent on telecommunicatino carriers to maintain availability which makes R1.3 almost impossible to meet compliance with. Providing entities with an exception in this scenario should be considered.	
Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response	
Thank you for your comment. The revised draft language and its focus on the “identification of methods used to mitigate the risk” addresses this concern. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Requirement 1.3 is is redundant to requirement 1.1 and not needed. Producing evidence to show overall compliance of requirement 1 more specifically requirement 1.1 will always lead to the identifications of where the responsible entity applied the appropriate controls. In addition, the language is requiring an entity to ensure availability beyond the Control Center. An entity will not be able to demonstrate compliance to availability beyond an entities physical equipment and contract language with carriers. Most entities communication links are managed by Telecom carrier companies. Entities have no control over the availability of the paths. It is recommended that the SDT remove the language.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT believes that the issues of Requirement 1.3 being redundant to Requirement 1.1 was addressed in CIP-012-1 that is going into effect July 1, 2022. The revised draft language and its focus on the “identification of methods used to mitigate the risk” addresses this concern. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	

Comment	
While IESO supports the comments submitted by the ISO/RTO Council SRC and NPCC, we further amend those comments as follows: If the “availability” be considered “as defined by the Responsible Entity” within the proposed standard, then this gives IESO the flexibility in the application of availability protections. This is already implied in the proposed wording, thus IESO supports the proposed standard, however an explicit statement would further clarify this.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to ISO/RTO Council. The term availability has been removed from the proposed language. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on “identification of methods to mitigate the risk of loss” of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG.	
Benjamin Winslett - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Joseph Amato - Joseph Amato On Behalf of: Terry Harbour, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Matthew Jaramilla - Salt River Project - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Raducea - DTE Energy - Detroit Edison Company - 5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE believes registered entities should be able to demonstrate compliance with the Requirement Part 1.3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

3. The SDT proposes that the modifications in CIP-012-2 meet the FERC directives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

NRG does not believe that these modifications meet the FERC directives in a cost effective manner. A more cost effective solution would be to include such modifications in IRO-010, TOP-003, TOP-001, or other applicable Operations and Planning standards. Including this verbiage in the CIP standards means the same or similar compliance activities have to be documented for multiple standards and represented in more audits (i.e. 693 and 706 standards).

Likes 0	
Dislikes 0	

Response

Thank you for your comment. TOP and IRO 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. The revisions to CIP-012 will address elements that TOP and IRO do not address. 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.”

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

NRG does not believe that these modifications meet the FERC directives in a cost effective manner. A more cost effective solution would be to include such modifications in IRO-010, TOP-003, TOP-001, or other applicable Operations and Planning standards. Including this verbiage in the CIP standards means the same or similar compliance activities have to be documented for multiple standards and represented in more audits (i.e. 693 and 706 standards).

Likes 0	
Dislikes 0	

Response

Thank you for your comment. TOP and IRO 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. The revisions to CIP-012 will address elements that TOP and IRO do not address. 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.”

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	No
Document Name	

Comment

Reclamation observes there is an environment of constant churn with reliability standards. This results in ineffective use of resources associated with the planning and adjustments required to achieve compliance with frequently changing standard versions. NERC should foster a compliance environment that allows entities to fully implement technical compliance with current standards before moving to subsequent versions.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT will pass this comment on to NERC staff.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
We do not recommend adding availability to the scope of CIP-012, since availability of operational data is already addressed in other NERC Reliability Standards. Protection of availability implies physical actions to protect the communications between control centers. This is impractical given the distance between control centers.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. TOP and IRO 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. The revisions to CIP-012 will address elements that TOP and IRO do not address. 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." Additionally, the word availability has been removed from the Standard language which now reflects the concept of availability rather than a direct reference to availability. Additionally, the revised language is focused now on identification of methods for recovery and examples of those methods are now in the Measures section of the draft Standard.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	

Without having a more thorough understanding as to what “availability protections” are, it is inderterminant as to the impact of what costs would be.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. There is currently a NIST based definition of *availability* within the included Implementation Guidance. The SDT has refined this definition to better reflect industry feedback. Additionally, the word availability has been removed from the Standard language which now reflects the concept of availability rather than a direct reference to availability. Additionally, the revised language is focused now on identification of methods for recovery and examples of those methods are now in the Measures section of the draft Standard.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
Where new technology will be required to support availability, we have no basis to determine the cost effectiveness of implementing this standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. There is currently a NIST based definition of *availability* within the included Implementation Guidance. The SDT has refined this definition to better reflect industry feedback. Additionally, the word availability has been removed from the Standard language which now reflects the concept of availability rather than a direct reference to availability. Additionally, the revised language is	

focused now on identification of methods for recovery and examples of those methods are now in the Measures section of the draft Standard.	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not agree that the modification meets FERC directives in a cost effective manner. The proposed language for CIP-012, Requirement R1 does not provide guidance on what are acceptable measures for a Registered Entity to take to meet the requirement. There are not sufficient measures, guidelines, or technical rationale documented in the draft for a Registered Entity to design a solution that meets security goals and is cost effective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team has revised the measures in the latest CIP-012 draft to include more examples in order to provide additional clarity regarding availability and example controls around it. Please see the revised Implementation Guidance regarding carriers, diversity, recovery of links, and other topics. Additionally, the revised language is focused now on identification of methods for recovery and examples of those methods are now in the Measures section of the draft Standard.	
Joseph Amato - Joseph Amato On Behalf of: Terry Harbour, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	No
Document Name	
Comment	
Where new technology will be required to support availability, we have no basis to determine the cost effectiveness of implementing this standard.	

Likes 0	
Dislikes 0	

Response

While the standard does not impose a requirement for new technology to meet its objectives, some entities may choose to use new technology to meet the requirements. The standard drafting team recommends entities consider the cost of any new equipment to be balanced against the cost of the risk of loss of availability.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST believes that as written, the draft Implementation Guidance document strongly implies that Responsible Entities should employ redundant communication links between Control Centers to address availability, even while noting FERC's acknowledgement that in some suburban and rural areas, this could be prohibitively expensive, of only marginal incremental benefit to availability (no options for path diversity), or both. While we agree that redundant links should be considered, we recommend the document be revised to acknowledge this may not be a viable approach to mitigating availability risks in all cases. The SDT might also consider adding some examples of emergency back-up communications links an Entity might be able to utilize if its primary communications link is down or otherwise unavailable.

N&ST notes, further, that while FERC Order 866 suggests it might be possible for a Responsible Entity to establish availability-related service level agreements with one or more network service providers, the Implementation Guidance document makes no mention of this option.

Finally, N&ST believes the scope of CIP-012's proposed availability requirements is unclear and open to interpretation, which has the potential to have significant cost implications for some entities, especially those without fully redundant Control Center network and computing infrastructures.

Likes 0	
Dislikes 0	

Response

While the standard does not impose a requirement for redundancy to meet its objectives, some entities may choose to use redun dancy to meet the requirements. The standard drafting team recommends entities consider the cost of this method to be balanced against the cost of alternative methods to mitigate the risk of loss of availability. The revised language is focused now on identification of methods for recovery and examples of those methods are now in the Measures section of the draft Standard. The SDT notes that Implementation Guidance is not all inclusive and is only one way in which to comply, not the only way.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Please refer to BC Hydro's comments on Question #2. CIP-012-1 is not yet in effect in British Columbia and BC Hydro has not implemented a solution to comply with CIP-012-1 yet; therefore, it is not yet feasible to identify the additional costs related to the Project 2020-04 CIP-012-2 changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	

No: NCPA does not agree the proposed language is considered cost effective until there is expectation of what availability would be defined as with regards to the standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. There is currently a NIST based definition of *availability* within the included Implementation Guidance. The SDT has refined this definition to better reflect industry feedback. Additionally, the word availability has been removed from the Standard language which now reflects the concept of availability rather than a direct reference to availability. Additionally, the revised language is focused now on identification of methods for recovery and examples of those methods are now in the Measures section of the draft Standard.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment

Where new technology will be required to support availability, we have no basis to determine the cost effectiveness of implementing this standard.

Likes 0	
Dislikes 0	

Response

While the standard does not impose a requirement for new technology to meet its objectives, some entities may choose to use new technology to meet the requirements. The standard drafting team recommends entities consider the cost of any new equipment to be balanced against the cost of the risk of loss of availability.

James Baldwin - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

LCRA is unclear exactly what these modifications will entail and is unsure what will constitute as sufficient availability.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. There is currently a NIST based definition of *availability* within the included Implementation Guidance. The SDT has refined this definition to better reflect industry feedback. Additionally, the word availability has been removed from the Standard language which now reflects the concept of availability rather than a direct reference to availability. Additionally, the revised language is focused now on identification of methods for recovery and examples of those methods are now in the Measures section of the draft Standard.

Teresa Krabe - Lower Colorado River Authority - 1,5

Answer	No
Document Name	
Comment	
LCRA is unclear exactly what these modifications will entail and is unsure what will constitute as sufficient availability.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. There is currently a NIST based definition of *availability* within the included Implementation Guidance. The SDT has refined this definition to better reflect industry feedback. Additionally, the word availability has been rem oved from the Standard language which now reflects the concept of availability rather than a direct reference to availability. Additionally, the rev ised language is focused now on identification of methods for recovery and examples of those methods are now in the Measures section of the draft Standard.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
At this time PG&E cannot determine if the proposed modifications are cost-effective in meeting the FERC directive.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
I support the comments submitted by Sean Erickson (WAPA).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to WAPA.	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
Implementation will increase costs for Responsible Entities. The changes will have unforeseen consequences. For responsible entities these consequences will be incurred in terms of additional equipment,software licensing, contract modifications and man hours involved in planning, implementation,processes, maintenance and monitoring.	
Likes 0	
Dislikes 0	
Response	
While the standard does not impose a requirement for new technology to meet its objectives, some entities may choose to use new technology to meet the requirements. The standard drafting team recommends entities consider the cost of any new equipment to be balanced against the cost of the risk of loss of availability.	

Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Black Hills Corporation does not anticipate a significant expense to achieve compliance.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
The NSRF suggests the SDT identify which TOP and IRO O&P Standards are referenced in the Implementation plan at **Identification of Methods Used for the Recovery of Communication Links (R1.2)**. If the objectives are consistent, identification may help with cost effectiveness by allowing an entity to leverage current practices of compliance with those standards.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Thank you for your support. Please see the updated Technical Rationale and Implementation Guidance.	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	

The NSRF suggests the SDT identify which TOP and IRO O&P Standards that are referenced in the Implementation plan at **Identification of Methods Used for the Recovery of Communication Links (R1.2)**. If the objectives are consistent, identification may help with cost effectiveness by allowing an entity to leverage current practices of compliance with those standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see the updated Technical Rationale and Implementation Guidance.	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to comments submitted by the MRO Standards Review Forum.	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	

It depends on the final version of this standard. PNMR is concerned that this feels like an all or nothing requirement. What are the restoration requirements? What if we lose connection and ability to transmit RTA and RTm data for 10 seconds, 30 seconds, 30 minutes? Do we have a potential non compliance? There should be some timedriven measure. Availability, like confidentiality and integrity, is a risk and methods to address the risk should be implemented.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the revised draft language which states "Identification of method(s) used to mitigate the risks". Please see the revised measure regarding time driven measures. Additionally, the word availability has been removed from the Standard language which now reflects the concept of availability rather than a direct reference to availability. Additionally, the revised language is focused now on identification of methods for recovery and examples of those methods are now in the Measures section of the draft Standard.	
Adrian Raducea - DTE Energy - Detroit Edison Company - 5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Matthew Jaramilla - Salt River Project - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joyce Gundry - Public Utility District No. 1 of Chelan County - 3, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Watt - Lakeland Electric - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Neville Bowen, Ocala Utility Services, 3; - LaKenya VanNorman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Benjamin Winslett - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	

Answer	
Document Name	
Comment	
Dominion Energy does not have enough information to make a determination.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	

4. The last ballot showed industry approval of the proposed 24-month implementation plan. Do you still agree the proposed timeframe is appropriate in light of the proposed revisions to the standard language? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee no NGrid's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to NGrid's comments.	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
We do not believe the implementation time frame is adequate because it is unclear whether encryption is or is not required, nor can we predicte the length of time to it will take to plan necessary changes, implementation of the changes, management and development of processes and procideures.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The revised draft language is focused upon the availability component of CIP-012. Confidentiality and integrity of the data are already covered in the approved CIP-012-1. The SDT does not endorse a specific technology.	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
I support the comments submitted by Sean Erickson (WAPA).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to WAPA's comments.	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
PNMR recommends 36 month implementation guidance due to supply chain challenges	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Industry was supportive of the 24-month timeframe in the previous ballot.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee no NGrid	
Answer	No
Document Name	
Comment	
We cannot answer until we understand what "availability" means and the availability's scope. Scope refers to how deeply an entity must depend on other companies. We request clarification on 1) what availability means and 2) what is availability's scope.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of availability to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. Doing this has allowed the SDT emphasize a focus on controls and measures to achieve availability rather than a measurement for availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Teresa Krabe - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
This standard involves technology and protocol changes. More time is warranted to effectively implement these changes.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Industry was supportive of the 24-month timeframe in the previous ballot.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
This standard involves technology and protocol changes. More time is warranted to effectively implement these changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Industry was supportive of the 24-month timeframe in the previous ballot.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No: NCPA does not agree that 24 months is long enough to implement other solutions. Many of these implementations require 3rd party ISPs to install circuits. In many cases it can take 6 months or more to get a circuit installed when it is available, however depending on location it can be years before circuitry is locally available.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Industry was supportive of the 24-month timeframe in the previous ballot.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
As identified in answers to Questions above, at this time BC Hydro does not have sufficient information to affirm whether 24 months will be adequate to implement the solutions to comply with the changes proposed in Project 2020-04 for CIP-012.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Industry was supportive of the 24-month timeframe in the previous ballot.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
WECC proposes the SDT consider changing to a 12 or 18-month Implementation Plan.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Industry was supportive of the 24-month timeframe in the previous ballot.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
We do not recommend adding availability to the scope of CIP-012, since availability of operational data is already addressed in other NERC Reliability Standards, specifically the provisions of TOP-001 and IRO-002, which require redundant and diversely routed data exchange infrastructure implementation and testing.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. 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.”	
Adrian Raducea - DTE Energy - Detroit Edison Company - 5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
Compliance with the availability requirement may involve the installation of back-up communications. We are current experiencing delays in obtaining equipment necessary to install a dedicated line (six months from time of order). This type of delivery challenge may necessitate an extension in the enforcement date for CIP-012-2.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Industry was supportive of the 24-month timeframe in the previous ballot.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the 24-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment, please see response to MRO NSRF.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Consider current supply chain landscape impacts to procuring technology to support this implementation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Industry was supportive of the 24-month timeframe in the previous ballot.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAFG supports the proposed implementation plan timeframe. GO/GOPs needing to procure equipment to demonstrate compliance must navigate both organizational system development life cycle processes and national supply chain constraints.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Consider current supply chain landscape impacts to procuring technology to support this implementation	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Industry was supportive of the 24-month timeframe in the previous ballot.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
The need for a 24 month implementation plan is paramount to reliably and securely implement this standard. If the standard is implemented as written, 24 months will be needed to apply the recovery procedures as outlined. Registered Entities will need to work with their neighbors on the development of recovery plans; for example, an RTO/ISO will need to ensure recovery plans are in place for the availability of communications links with each of its members. Also, this standard involves more than just developing a recovery plan. Since these assets are not owned by Functional Entities subject to CIP-002, the utilization of CIP-008 and CIP-009 plans may not be relevant, and entities will have to develop their own recovery plans from scratch. Entities will have to work with telecommunication providers to set up new links and test them for recovery if they have not already done so. Finally, if supply chain issues cause delays in obtaining the required components needed for industry to fully implement V1 of this standard, then extra time will be needed for implementation until the supply chain issues are mitigated and resources are available.	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Eversource supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see response to EEI's comments.	
Jennifer Malon - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees that a 24 month implementation time is reasonable, however where vendors are involved that timeframe could become challenging.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Benjamin Winslett - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dana Showalter - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Neville Bowen, Ocala Utility Services, 3; - LaKenya VanNorman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Watt - Lakeland Electric - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joseph Amato - Joseph Amato On Behalf of: Terry Harbour, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joyce Gundry - Public Utility District No. 1 of Chelan County - 3, Group Name CHPD	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Daniela Hammons - CenterPoint Energy Houston Electric, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF, Group Name Consumers Energy Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Matthew Jaramilla - Salt River Project - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

5. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale and implementation guidance document, if desired.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	
Document Name	
Comment	
Please see comments provided above	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to your previous comments.	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	
Document Name	
Comment	
Following is Duke Energy's suggested rewording of the SDT's proposed draft sub requirements for R1. We appreciate the effort that went into consolidating R2 into R1 and the opportunity to provide feedback. 1.1 Identification of security protection(s), the Responsible Entity applied to mitigate the risks posed by unauthorized disclosure or unauthorized modification of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers.	

1.2 Identification of controls, the Responsible Entity implemented to protect the availability of communication links used to transmit data between Control Centers for Real-time Assessment and Real-time monitoring as to ensure timely and accurate data communication.

1.3 Identification of methods by the Responsible Entity, to be used for the recovery of communication links to transmit Real-time Assessment and Real-time monitoring data between Control Centers.

1.4 Identification of where the Responsible Entity has applied the protections and controls identified in Parts 1.1 and 1.2; and

1.5 If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying protections and controls to data being transmitted between Control Centers as required in Parts 1.1 and 1.2.

FERC Order No. 866 spoke directly to recovery. Recovery in the standard aligns with this; however, restoration and recovery are both used in the Implementation Guidance. We are requesting clarification if “recovery and restoration” are meant to be interchangeable. We recommend that the Implementation Guidance solely reference the term recovery, since recovery and restoration have different technical implications

Likes 1	PNM Resources - Public Service Company of New Mexico, 3, Bratkovic Amy
Dislikes 0	

Response

Thank you for your comment. The SDT appreciates the inclusion of suggested language above and has revised the R1 subpart language to focus upon “Identification of method(s) used to mitigate the risk” to better reflect the requirement for availability controls based on industry feedback.

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	
Document Name	

Comment

Thank you for the opportunity to comment.

Likes 0	

Dislikes 0	
Response	
Thank you for your response.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	
Document Name	
Comment	
ATC supports the SDT's approach to permit each Registered Entity to define availability within a CIP-012 plan, as opposed to having this term defined in the glossary of terms. Defining "availability" in the glossary of terms would be too prescriptive an approach espe cially considering the prevalent use of this word is in other Reliability Standards, and the broad ranging impacts and unintended consequences t hat a definition could have on other mandatory regulations outside the scope of this SDT's SAR. ATC appreciates t he flexibility this draft provides entities and supports objective-based requirements that steer away from one-size-fits-all definitions.	
Likes 3	Nebraska Public Power District, 1, Cawley Jamison; Nebraska Public Power District, 3, Eddleman Tony; Nebraska Public Power District, 5, Bender Ronald
Dislikes 0	
Response	
Thank you for your support.	
Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4	
Answer	
Document Name	
Comment	
NONE	

Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Ronald Bender - Nebraska Public Power District - 5	
Answer	
Document Name	
Comment	
NPPD supports the SDT's approach to permit each Registered Entity to define availability within a CIP-012 plan, as opposed to having this term defined in the glossary of terms. Defining "availability" in the glossary of terms would be too prescriptive an approach. NPPD appreciates the flexibility this draft provides entities and supports objective-based requirements that steer away from one-size-fits-all definitions.	
Likes 2	Nebraska Public Power District, 3, Eddleman Tony; Nebraska Public Power District, 1, Cawley Jamison
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	
Comment	
The terminology continues to be confusing, especially for those unfamiliar with the underlying FERC Order. The concepts could be explained in R1 using simple, plain language.	

The changes proposed are a significant increase in the scope of the standard, which will have a substantial impact on affected entities and should not be taken without appropriate consideration. Some communications paths are already covered under other NERC standards. Proposed R1.2 recovery plans should be included under CIP-009 instead of CIP-012-2. To minimize churn among standard versions, Reclamation recommends the SDT fully scope each project before developing proposed modifications to ensure all of FERC's desired requirements are included, thereby precluding the need for FERC to order approval with additional modifications. For CIP-012, Reclamation recommends the SDT coordinate changes with Projects 2016-02 and Project 2019-03. This will reduce the chance that standards conflict with one another and will better align related standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of availability to better reflect the cyber security objective of the Requirement. There may be elements of your CIP-012 components that logically lay outside of the other CIP standards. Entities may use CIP-009 plans in support of meeting the regulatory requirements within CIP-012, but Entities must ensure that all of the appropriate components for CIP-012 are covered in the restoration plans. The SDT continues to collaborate with Projects 2016-02 and 2019-03.	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	
Eversource supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see response to EEI’s comments.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE noticed a potential reliability gap between proposed CIP-012-2 and CIP-008-6. CIP-008-6 seeks to “mitigate the risk to the reliable operation of the BES as a result of a Cyber Security Incident by specifying incident response requirements” (CIP-008-6 Purpose Statement). The definitions of Cyber Security Incident and Reportable Cyber Security Incident may not cover cyberattacks targeted toward disrupting the confidentiality, integrity, or availability of Control Center communications. Texas RE recommends the definitions of Cyber Security Incident, Reportable Cyber Security Incident, and the applicable systems column of CIP-008-6 be modified to explicitly include situations where the confidentiality, integrity, or availability of Control Center communications is targeted.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Modification of these definitions would be outside the scope of the 2020-04 SAR, and team recommends this comment be submitted during any future CIP-008 standards development activity.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
There is nothing in Guidance Document that provides information on protections for availability of data. The guidance deals with confidentially and integrity of data.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	
Document Name	
Comment	
As mentioned above, Dominion Energy supports EEIs comments. In addition, Dominion Energy has the following suggestion for language in R1.2 that would allow this requirement to be actionable by industry: Identification of methods to be used for the recovery of communication **link components controlled by each Responsible Entity and response plans used for the recovery of communication links not controlled by the Responsible Entity** used to transmit Real-Time Assessment and Real-time monitoring data between Control Centers.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI's comments. The SDT has modified the Measures to include language suggesting ways in which the Responsible Entity may affect recovery of links.	
Joyce Gundry - Public Utility District No. 1 of Chelan County - 3, Group Name CHPD	
Answer	
Document Name	
Comment	

With the content of the previous R1.2 moved to R1.3, the updated R1.2 deals with recovery methods that appear to go beyond the FERC Order No. 866 directive and aren't applicable to many Registered Entities. Communications links between Control Centers operated by different Registered Entities are dependent on telecommunication companies. For many Registered Entities, the method to recover a link is a support call to their region's contracted telecommunication provider.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see response to EEI's comments. The SDT has modified the Measures to include language suggesting ways in which the Responsible Entity may affect recovery of links.

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	
Document Name	

Comment

The Implmentation Guidance and Technical Rationale appear to infer encryption is the only method to meet the security objectives to mitigate the risks posed by unauthorized disclosure, unauthorized modification of applicable data. Consider providing examples an entity could altnatively consider to also meet the security objectives.

For example:

1. An entity owned, operated and managed communication link.

2. Monitoring, detecting, alerting and response to any possible unauthorized disclosure or unauthorized modification of applicable data transmitted on a ---communication link between Control Centers.

Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The revised draft language is focused upon the availability component of CIP-012. Confidentiality and integrity of the data are already covered in the approved CIP-012-1. The SDT does not endorse a specific technology.	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	
Document Name	
Comment	
None at this time.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
The current wording of the proposed standard gives IESO the flexibility to address the availability controls of the data itself in addition to the just the availability controls associated with solely with the communications link.	

IESO recommends that that the definition of term “availability” be futher clarified with the addition of the wording “as determined by the Responsible Entity”	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see the revised Implementation Guidance and Technical Rationale.	
JT Kuehne - AEP - 6	
Answer	
Document Name	
Comment	
AEP appreciates the efforts of the SDT on this project. Please see below for additional comments. While AEP agrees that creating a plan to account for the security and availability of Real-time Assessment and Real-time monitoring data is crucial as part of FERC Order No. 866, we believe the revisions to CIP-012-2 need to be more prescriptive to capture the expected contents of the plan. For example, page 4 of the Technical Rationale document lays out an expectation and relationship with CIP-008 and CIP-009 plans, “The SDT recognized that Responsible Entities may already have plans to address these contingencies in their CIP-008 and CIP-009 plan(s) and these could be referenced as part of their CIP-012 plan to meet the requirement and avoid duplication of effort.” However, the applicable systems for CIP-008 and CIP-009 are different than the devices that would receive protections for CIP-012. With that in mind, AEP suggests that NERC take either of the following action: (1) Create the desired components of CIP-008 and CIP-009 as explicit requirements and sub-requirements within CIP-012; or (2) Create a new classification for CIP-012 devices (e.g., “associated networking equipment”) and determine the specific requirements within the other CIP standards that apply to that classification.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts. Please see the revised Implementation Guidance and Technical Rationale.	
Joseph Amato - Joseph Amato On Behalf of: Terry Harbour, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
N&ST believes that both the proposed availability language of CIP-012 R1 and the accompanying draft Implementation Guidance lack sufficient clarity regarding the scope of a Responsible Entity's CIP-012 availability obligations: Where do they begin and end? The Implementation Guidance document seems to suggest that inter- Control Center communications channels subject to CIP-012 should include literally everything either utilizing or comprising those channels, including the sending and receiving hosts. Evide nce supporting this opinion includes the statement, "The SDT also recognizes that the availability components within the plan may or may not be applied t o Cyber Assets identified as BES Cyber Assets." Should Entities include ICCP servers, which are almost always identified as BES Cyber Systems and, for High	

and Medium Impact, located within Electronic Security Perimeters, in their CIP-012 availability plans? If so, will Entities with only single ICCP servers be expected to procure additional ones for redundancy? N&ST is concerned that by discussing endpoint hosts, the SDT may be expanding the scope of CIP-012 beyond FERC's mandate. At the very least, the draft Implementation Guidance raises questions we believe the SDT should answer. If it does not, experience suggests to us that NERC and/or the Regions will.

Additional Guidance document statements and phrases that N&ST believes need clarification include:

"Availability protection can be shown with network diagrams showing multiple circuits, redundant systems, application details or other documentation describing the protections used."

What kind of systems? Switches? Routers? Endpoint hosts? The SDT should provide examples.

The phrase, "entire communications link" is used several times. The SDT should define what this means, as well as whether or not endpoints are subject to CIP-012.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Based on industry feedback, the SDT has refined the requirement language of R1, the subparts, and the Measures. Please see the revised Implementation Guidance and Technical Rationale. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG. Please see the updated Technical Rationale and Implementation Guidance regarding carriers, diversity of links, and similar topics. Regarding the phrase "entire communications link", the SDT has reviewed the language within the context of the complete statement containing these words. This language has been part of the Implementation Guidance since CIP-012-1 as "Where the operational obligations of an entire communication link, including both endpoints…".

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	
Document Name	

Comment

BC Hydro suggests adding more clarity to term 'availability' by providing a more detailed definition. Although the SDT has proposed the use of the NIST definition of "Ensuring timely and reliable access to and use of information" for defining the term 'availability' in the Technical Rationale document, a more detailed and specific definition concerning the application and use, specifically at NERC entities, will help improve a clear understanding and easier implementation. BC Hydro also suggests including some pertinent use cases and examples.

Likes 0

Dislikes 0

Response

Thank you for your comment. Based on industry feedback, the SDT has refined the requirement language of R1, the subparts, and Measures, as well as provided additional context of availability to better reflect the cyber security objective of the Requirement. The revised language is focused now on “identification of methods to mitigate the risk of loss” of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement for availability.

Larry Watt - Lakeland Electric - 1

Answer

Document Name

Comment

This 'availability' requirement should be moved to the O&P standards.

Likes 0

Dislikes 0

Response

Thank you for your comment. 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.”	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	
Document Name	
Comment	
Thank you for your hard work and allowing Entities to provide feedback.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI’s comments.	
Kinte Whitehead - Exelon - 3	

Answer	
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI’s comments.	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI’s comments.	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	

Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI's comments.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	
Document Name	
Comment	
N/A	

Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
The phrase “and components used to provide availability protections” was added to both the technical rationale document and the implementation guidance for R1.3. As mentioned in our comment to question 2, if we contract with a 3rd party for security and availability (such as CAISO's AT&T DMVPN solution), we may not be privy to the specific component(s) where the availability protection is being applied. Additionally, this seems to be unnecessarily prescriptive. We recommend this phrase be removed from both documents. Also, the implementation guidance doesn’t acknowledge that not all entities involved are Registered Entities (such as a common carrier like AT&T). We recommend adding language to acknowledge those situations may exist, at a minimum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of availability to better reflect the cyber security objective of the Requirement. The former R1.1 has been separated into R1.1 and R1.2 so that availability could be addressed separately. Please see the revised Implementation Guidance and Technical Rationale.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	

Document Name	
Comment	
None at this time.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	
Document Name	
Comment	

Is this not an overlap with TOP-001-5 R20, R23? Or is the gap due to the communication links between control centers / data centers?

TOP-001-5 R20. Each Transmission Operator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and Real-time Assessments.

Same question but in regards to EOP-008-2. Would this not fall under "Loss of Control Center Functionality"? Or is FERC / NERC focused on the dealing with impacts to the specific processes associated with the Real-time Assessment and Real-time Monitoring tasks?

Finally – how far does this extend? Is this limited to the loss of availabliity of data associated with the security protections applied between control centers/ data centers? Or would it also stretch to wider data losses, such as external measurements sourced via ICCP, substation data sourced via RTU, or system-to-system communications within a control center / data center? The requirement as written, seems overly broad in scope when accounting for all of the data required to perform Real-time monitoring and Real-time Assessments.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. 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 and not so much about the use or ability to use that data.

Regarding your last comment, the intended scope of CIP-012-2 is the movement of data between in-scope Control Centers. Data at rest is covered in other CIP standards. The scope of the data covered by CIP-012-2 remains the same as the already approved CIP-012-1.

James Baldwin - Lower Colorado River Authority - 1	
Answer	
Document Name	
Comment	
Throughout the supporting documentation there are references to CIP-008 and CIP-009; however, these standards are not applicable to communication between control centers. By including CIP-008 and CIP-009 in the implementation of CIP-012, there may be unintended scope creep of CIP-008 and CIP-009.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The reference to CIP-008 and CIP-009 within the supporting documentation represents one way in which a responsible entity may address recovery of links. It is not a requirement to do so in this way, but it is suggested so that existing recovery plans may be used to facilitate this restoration. Please see the Technical Rationale and Implementation Guidance regarding the SDTs thought that went into recovery as well as additional examples of ways in which this can be achieved.	
Teresa Krabe - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
Throughout the supporting documentation there are references to CIP-008 and CIP-009; however, these standards are not applicable to communication between control centers. By including CIP-008 and CIP-009 in the implementation of CIP-012, there may be unintended scope creep of CIP-008 and CIP-009.	
Likes 0	
Dislikes 0	

Response	
Thank you for your response. The reference to CIP-008 and CIP-009 within the supporting documentation represents one way in which a responsible entity may address recovery of links. It is not a requirement to do so in this way, but it is suggested so that existing recovery plans may be used to facilitate this restoration. Please see the Technical Rationale and Implementation Guidance regarding the SDTs thought that went into recovery as well as additional examples of ways in which this can be achieved.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
We would like to thank the SDT for all their hard work and allowing us to provide feedback.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee no NGrid	
Answer	
Document Name	
Comment	
We request that future posting of all CIP Standards include a redline to the last approved. This redline will help SMEs determine the change and thereby complete comment forms faster.	

The Implementation Guidance refers to a NIST definition of availability. NIST could change its definition without notifying entities. NIST's definition is generic. We request clarification of CIP-012 availability. In the fourth paragraph of the introduction in the Technical Rational, the following sentence needs to be corrected as there is no R2 in CIP-012-1. "CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers.". We believe the text should read R1 and R1.2.	
Likes 1	PNM Resources - Public Service Company of New Mexico, 3, Bratkovic Amy
Dislikes 0	
Response	
Thank you for your comment. The SDT will draft redline to last approved for the next ballot and comment period if time allows. Regarding the NIST definition within IG, the previously approved version of CIP-012 used NIST definitions for confidentiality and integrity, but also spelled out those definitions in the IG. In the current draft, the SDT has used the NIST definition as a starting point for defining availability. The SDT has further modified the listed definition within the IG to better reflect the scope and purpose of CIP-012. Regardless of the definition used by NIST, the version provided in the IG by the SDT would still stand should the IG be ERO endorsed. Please see the updated language within the Technical Rationale with regards to the modified Requirement language from R2 to R1.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Neville Bowen, Ocala Utility Services, 3; - LaKenya VanNorman	
Answer	
Document Name	
Comment	
This 'availability' requirement should be moved to the O&P standards.	
Likes 0	

Dislikes 0	
Response	
Thank you for your response. 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.”	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	
Document Name	
Comment	
PG&E agrees with the Edison Electric Institute (EEI) comments related to the Introduction section having a reference to R2 that was removed in the most recent draft – the sections should be updated with the removal of R2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDTs response to EEI.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	
Document Name	
Comment	
GTC is concerned that the revisions to the technical rationale significantly alter the potential flexibility intended to be offered in requirements such as requirement 1.3. In addition, the inclusion of infeasible alternatives to availability such as backing up ICCP data with DNP3 is	

problematic, and GTC recommends that the SDT review the proposed revisions to the technical rationale and implement revisions to retain the original flexibility of implementation and to better ensure that suggested methods for compliance are actionable.

Likes 0	
Dislikes 0	

Response

Thank you for your comment, please see the revised Technical Rationale and Implementation Guidance.

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

The Introduction section has a reference to R2 that should be removed now that R2 has been deleted by the SDT (see below):

"Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate for securing the data. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 **and R2** protect the applicable data during transmission between two separate Control Centers. CIP-006 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection addressed in CIP-006 Requirement R1 Part 1.10 does not apply.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see the updated language within the Technical Rationale with regards to the modified Requirement language from R2 to R1.

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the SDTs response to EEI.	
Dana Showalter - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
The VSL table appears incomplete. ERCOT would encourage the drafting team to ensure there is consistency among standards with plans that are documented versus implemented, perhaps by identifying documentation versus implementation separately within the VSL matrix. Further, the VSLs refer to Requirement R2, which was removed in the Nov 2021 Draft.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT asserts that the proposed VSLs do have documentation and implementation separate in the V SL matrix. Any references to Requirement R2 have been removed.	

Benjamin Winslett - Georgia System Operations Corporation - 3,4	
Answer	
Document Name	
Comment	
GSOC is concerned that the revisions to the Technical Rationale significantly alter the potential flexibility intended to be offered in requirements such as Requirement 1.3. In addition, the inclusion of infeasible alternatives to availability such as backing up ICCP data with DNP3 is problematic, and GSOC recommends that the SDT review the proposed revisions to the Technical Rationale and implement additional revisions to retain the original flexibility of implementation and to better ensure that suggested methods for compliance are actionable.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the revised TR and IG.	
sean erickson - Western Area Power Administration - 1	
Answer	
Document Name	
Comment	
We do not agree with the draft language proposed. The standard purpose and requirements are to protect the confidentiality, availability and integrity (CIA) of Real-time Assessmentand Real-time monitoring data transmitted between Control Centers. While this language maps to the standard tenents of information assurance controls, the requirements and miigation of risk cannot be achieved unless an entity uses encryption and manages the encryption keys.	

Once data packets carrying RTA/RTm data have egressed the physical Control Center or associated data center equipment/technology, an entity is relying on non-entity controlled or maintained communicatition paths such as telecom carriers to transmit and route RTA/RTm data between Control Centers.

How is an entity able to "mitigate risks" of unauthorized disclosure and/or modification when RTA/RTm data is no longer in possession or control of the systems which transmit and carry such data?

Secondly, the phrase "while it is being transmitted" in context with availability requires an entity to only address entity owned and maintained equipment. This is because an entity cannot ensure the availability of RTA/RTm data beyond its possession. This phrase adds no value to the protection of data.

Because of this, industry and regulators alike will not be able to establish a clear understanding of what meets or what does not meet compliance, it may lead to additional administrative overhead, potential findings or self-reports or others issues. This position was also validated in the recent 12/8 Industry Webinar whereas the SDT's Lead related that an entity is not required to implement encryption, but an auditor would ask for it.

We ask the SDT to:

a. Remove or change the confidentiality and integrity language, and revise R1 to add the phrases "potential disclosure, potential modification and availability."

b. Remove the phrase "while being transmitted".

c. Remove the term "links." There is no such term and this may apply to many different things.

d. Clarify if RTA/RTm data is BES Cyber System Information.

e. Instead of relying on a one size fits all definition for the CIA triad the SDT would be better suited in defining a list of controls that responsibilities can implement and if used in concert with each other mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time Monitoring Data.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

a. This comment is focused on CIP-012-1. That is not within the SAR for this current version of the project.
b. "While it is being transmitted" helps define the scope of data to be protected by the other requirements of CIP-012.
c. The term "links" was copied from the FERC directive, which should provide a common understanding.
d. BCSI represents information that could be used to gain unauthorized access and pose a security threat to the BES. RTA/RTm represents data needed to run the BES. The focus of CIP-012-2 is about the cyber protections associated with the movement of RTA/RTm between control centers.
e. The SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of availability to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. The expansion of the Measures section also includes measures for confidentiality and integrity.

Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG. Confidentiality and integrity is already in the approved standard that went into effect on July 1, 2022.

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	
Document Name	

Comment	
Evergy supports and incorporates by reference Edison Electric Institute’s (EEI) response to Question 5.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT’s response to EEI.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports the NPCC Regional Standards Committee no NGrid‘s comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT’s response to the NPCC Regional Standards Committee.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	

If the SDT's intent was to point to Operations standards (TOP/IRO) to explain the "Availability timeframes" or server redundancy or site redundancy then our suggestion is that they spell that out or point to other standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the revised Technical Rationale and Implementation Guidance regarding availability timeframes.	

"Comments received from Jamie Monette – Minnesota Power, Inc."

Question 1
MP Comment: Minnesota Power opts to answer "No". Minnesota Power agrees with MRO's NERC Standards Review Forum (NSRF) comments. In addition, MP would like to see a definition for real time monitoring incorporated in the NERC Glossary of Terms for clarity.

SDT Response:
Thank you for your comment. Please see the SDT's response to NSRF. Regarding the definition for real time monitoring, creating a definition for this term is outside the scope of the Project 2020-04 SAR. The term is used throughout other standards with a common understanding in industry.

Question 2
MP Comments: Minnesota Power opts to answer "No". Minnesota Power agrees with MRO's NERC Standards Review Forum (NSRF) comments.
SDT Response: Thank you for your comment. Please see the SDT's response to NSRF.

Question 3

MP Comments: Minnesota Power opts to answer "No". Until the scope of the standard is more clearly defined it is difficult to determine co st effectiveness of implementation.
SDT Response:

Question 4

MP Comments: Minnesota Power opts to answer "Yes". Minnesota Power agrees with MRO's NERC Standards Review Forum (NSRF) comments.
SDT Response: Thank you for your comment. Please see the SDT's response to NSRF.

Question 5

MP Comments: Minnesota Power has no additional comment.

"Comments received from Darcy O'Connell – California ISO"

Question 1

☐ **Yes**
☒ **No**

Comments:

The definition of availability needs to be clarified.
The SRC generally agrees revised CIP-012-2 meets the FERC Order 866 directives; however, to be useful the term "availability" must be clarified in the requirements. While the SRC appreciates the NIST definition of "availability" contained in the proposed Implementation Guidance, it is not certain that the Implementation Guidance will be endorsed by the ERO. Therefore, the SRC recommends the SDT draft a formal definition of "Availability" for inclusion in the CIP-012-2 Standard, which could be the adoption of the NIST definition, or something similar. The SRC recognizes the challenges and unintended consequences associated with "availability" being added as a new definition to the NERC Glossary of Terms since "availability is used in other standards which could be impacted. In light of that, the SRC suggests a definition be added (and limited in scope) to the CIP -012 standard itself.

Additionally, clarification of "availability" could also be included in the Technical Rationale for CIP-012. The benefits of a definition include formalization within the Standard's vernacular, thereby reducing potential ambiguity and likelihood of different interpretations by registered entities and audit teams. The SRC also believes that the Measure M1 should provide examples of what types of evidence would meet the availability requirement (e.g., an entity executing plans in support of the recovery of compromised communications links and the use of back-up communications capability when primary communications are unavailable). This would provide additional clarity to the industry.

In addition, the SRC seeks clarification from the SDT whether availability only refers to the data links used for the transmittal of data, or if availability also refers to the data being provided by external systems flowing through the data links under CIP-012. The wording in the current revision makes the intended scope of what availability is ambiguous. There is concern that unintended interpretation of the standard could reach to include the external systems providing data through the data links; e.g. ICCP servers, in addition to the links themselves. Leaving this up to each entity to define for themselves can be problematic as the application of this standard relies on consistent interpretation across Registered Entities owning or operating Control Centers. Therefore, SRC requests the scope be clarified.

Similarly, while having the concepts of “diversity, redundancy, or a combination of both” in the Implementation Guidance is needed, the SRC recommends the SDT consider including the concepts in M1 to achieve a clearer measure of what constitutes meeting the requirement.

Proposed R1.2 requires identification of methods used for recovery, but the SDT fails to provide any examples of methods to recover a loss of a data link. The information currently contained in the Implementation Guidance is very broad and it would be helpful if examples are provided. Also, CIP-009 deals with CIP assets and restoration in the event of a loss but does not contain requirements regarding communications links and, therefore, is not applicable to CIP-012. The SRC recommends clarifying language be added to show the relation between CIP-012 and CIP-009.

The SRC recommends the SDT clarify within the Implementation Guidance at Identification of Methods Used for the Recovery of Communication Links (R1.2) the phrase “This objective is consistent with TOP and IRO O&P Standards” by identifying which standards are being referenced.

The term “recovery” as used in R1.1.2 is very broad, and, as many entities will be dependent on telecommunication companies to restore communications, the SRC recommends the SDT consider including a clause to mitigate compliance issues if a line goes down and it is not the entity’s fault.

Additionally, the task of restoring availability predominantly resides with the telecommunication provider. In the event a communication link goes down, electric reliability entities are reliant on telecommunication provider to restore service. The SRC requests the SDT add an exemption for links and equipment owned by telecommunication providers.

SDT Response:
Thank you for your comments. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on "identification of methods to mitigate the risk of loss" of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG.

Regarding the scope, the SDT notes that requirement R1 specifies data used for real-time assessment and real-time monitoring while such data is being transmitted between any applicable control centers.

The SDT has expanded the measures section of the draft standard to provide more details on what types of evidence would meet the availability requirement. The SDT has updated the Technical Rationale and Implementation Guidance references to CIP-008 and CIP-009 documentation. The SDT has also clarified in the Implementation Guidance the phrase Identification of Methods Used for the Recovery of Communication Links.

The SDT notes that the draft language is to have a documented plan to mitigate the risks. The draft language of the subparts was modified to include "identification of methods used to mitigate the risks" to provide additional clarity regarding the requirement.

Question 2
☐ **Yes**
☒ **No**
Comments:

The SRC requests the SDT add an exemption for the links and equipment owned by telecommunication providers. In many instances, availability resides with telecommunication providers; and in the event service is interrupted, Registered Entities are reliant on the telecommunication provider(s) to restore service. Similarly, in the event a telecommunication line or other piece of telecommunication equipment goes down, the Registered Entity is again reliant on the Telecommunication Provider(s) to address the issue(s).

The term “availability” is subjective and should be clearly defined prior to approving CIP-012-2.

SDT Response:
The SDT notes that the draft language is to have a documented plan to mitigate the risks. The draft language of the subparts was modified to include “identification of methods used to mitigate the risks” to provide additional clarity regarding the requirement.
Thank you for your comments. Based on industry feedback, the SDT has refined the requirement language of R1 and the subparts, as well as provided additional context of *availability* to better reflect the cyber security objective of the Requirement. The revised language is focused now on “identification of methods to mitigate the risk of loss” of availability and examples of those methods are now in the Measures section of the draft Standard. Doing so has allowed the SDT to emphasize a focus on controls and measures to achieve availability rather than a measurement *for* availability. Availability has a definition in the Implementation Guidance much like CIP-012-1 has definitions for confidentiality and integrity within the V1 IG. Please see the updated Technical Rationale and Implementation Guidance.

Question 3
☒ **Yes**
☐ **No**
Comments:
The SRC suggests the SDT identify which TOP and IRO O&P Standards are referenced in the Implementation plan at **Identification of Methods Used for the Recovery of Communication Links (R1.2)**. If the objectives are consistent, identification may help with cost effectiveness by allowing an entity to leverage current practices of compliance with those standards.

SDT Response:
Thank you for your comment. The SDT has made this reference more specific to TOP-003 and IRO-010.

Question 4
☒ **Yes**
☐ **No**
Comments:

The need for a 24-month implementation plan is paramount for reliably and securely implementing this standard. If the standard is implemented as written, 24 months will be needed to apply the recovery procedures as outlined. Registered Entities will need to work with their neighbors on the development of recovery plans; for example, an RTO/ISO will need to ensure recovery plans are in place for the availability of communications links with each of its members. Also, this standard involves more than just developing a recovery plan. Since these assets are not owned by Functional Entities subject to CIP-002, the utilization of CIP-008 and CIP-009 plans may not be relevant, and entities will have to develop their own recovery plans from scratch. Entities will have to work with telecommunication providers to set up new links and test them for recovery if they have not already done so. Finally, if supply chain issues cause delays in obtaining the required components needed for industry to fully implement V1 of this standard, then extra time will be needed for implementation until the supply chain issues are mitigated and resources are available.
SDT Response:
Thank you for your comment.

Question 5
Comments:

The SRC would prefer to have availability addressed as a separate requirement, e.g. R2, under CIP-012 and not as part of requirement R1 as encryption and availability are two separate functions. Inserting availability in with encryption merely serves to muddy the intent of R1.
SDT Response:
The SDT has separated availability into its own subpart to use clearer wording around what the requirement actually is.