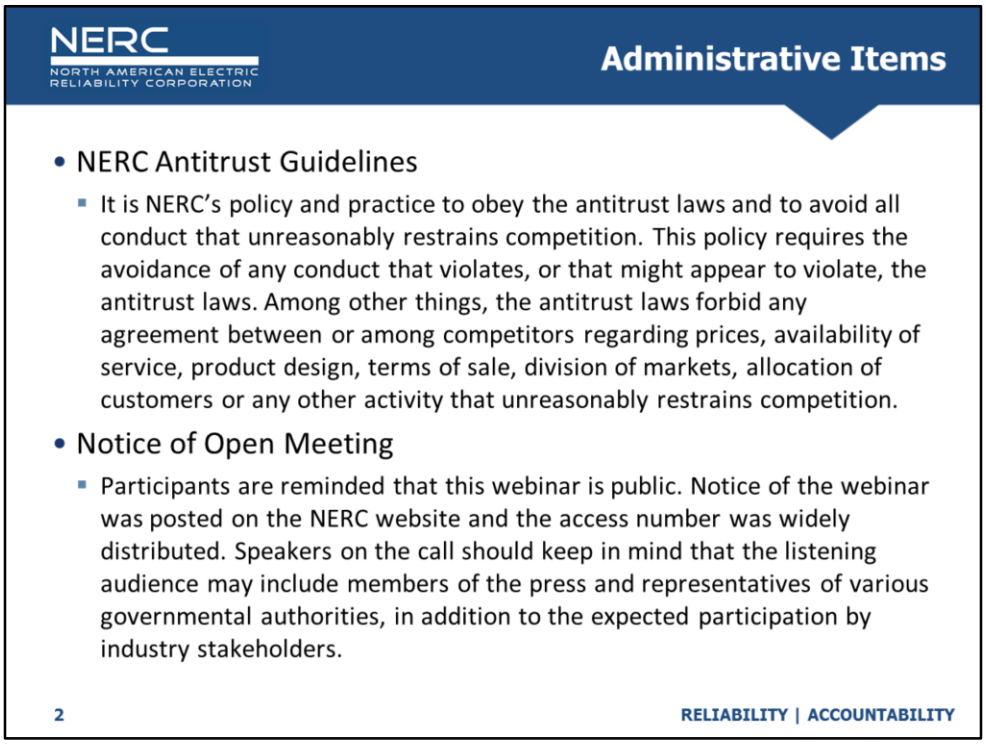
-Katherine Street-

Good morning everyone, and welcome to the Project 2016-02 Modifications to CIP Standards posting webinar.

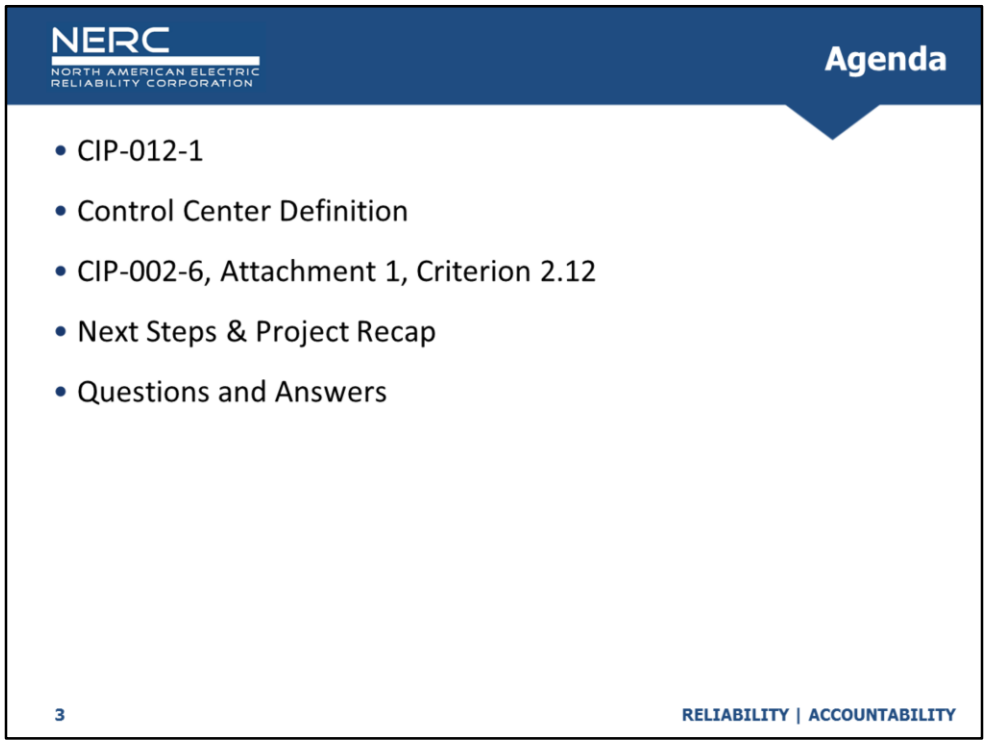
Let's get started with the antitrust guidelines and administrative items.



-Katherine Street-

Read slide above.

Now I am going to turn it over to our Co-chair, David Revill who will review the agenda and introduce the drafting team members.



-David Revill-

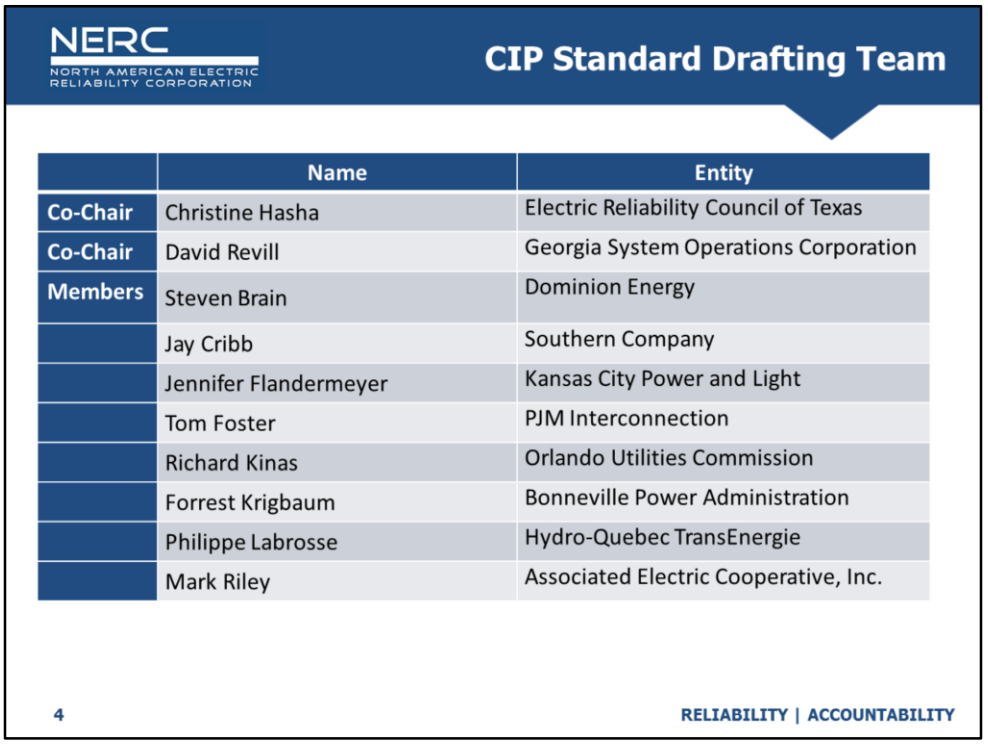
Thank you, Katherine.

Good morning from Vancouver, WA. My name is David Revill, one of the co-chairs for the CIP modifications Standard Drafting Team. Thank you for joining us for this webinar on the Standard Drafting Team's review of its current work. We first want to thank you for your attention and thoughtful comments that have been provided to the drafting team up to this time. Your feedback is a critical element to the development process.

Today, we would like to review the materials that the SDT has been working on. First, we will cover the new proposed standard CIP-012 that is out for formal comment and ballot. CIP-012 was developed to respond to FERC's directives in Order 822 on the protection of sensitive Bulk Electric System data that is communicated between Control Centers. Next, we will cover a potential revision to the Control Center definition. The SDT is looking for feedback through an informal comment form on modifications to the Control Center Definition. Then, we'll review some changes to CIP-002, Attachment 1, Criterion 2.12 that were developed in response to the issue identified by the Version 5 Transition Advisory Group (or V5TAG) on Transmission Owner Control Centers performing the functional obligations of a Transmission Operator. These CIP-002 changes are currently being submitted to the NERC standards committee seeking their authorization for formal posting. Finally, we'll review the team's next step and do a brief project recap.

There will be a question and answer period at the end of the session. If you have a question, please send your question through via the chat function. As a reminder, these slides and this webinar recording will be available on the NERC website within a few days.

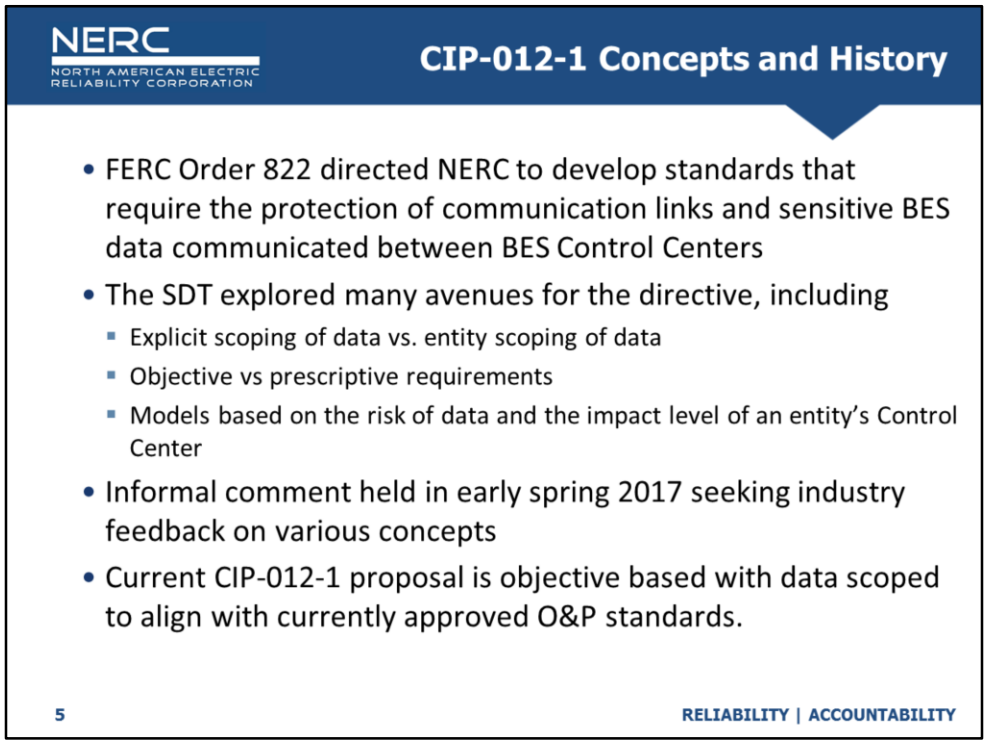
Next slide



-David Revill-

Before we get going, I'd like to take a moment to introduce the members of the Project 2016-02 CIP Modification Standards Drafting Team.
Co-Chair Christine Hasha from Ercot
Steve Brain – Dominion Energy
Jay Cribb – Southern Company
Jennifer Flandermeyer – KCP&L
Tom Foster – PJM
Rich Kinas – Orlando Utilities
Forrest Krigbaum, our host this week at Bonneville power Administration
Philippe Labrosse – Hydro Quebec TransEnergie
Mark Riley – Associated Electric Cooperative

As always, if you have any questions after this webinar, feel free to reach out to any of our team members. With that, I'll hand it over to Tom Foster from PJM to review the proposed CIP-012 standard.

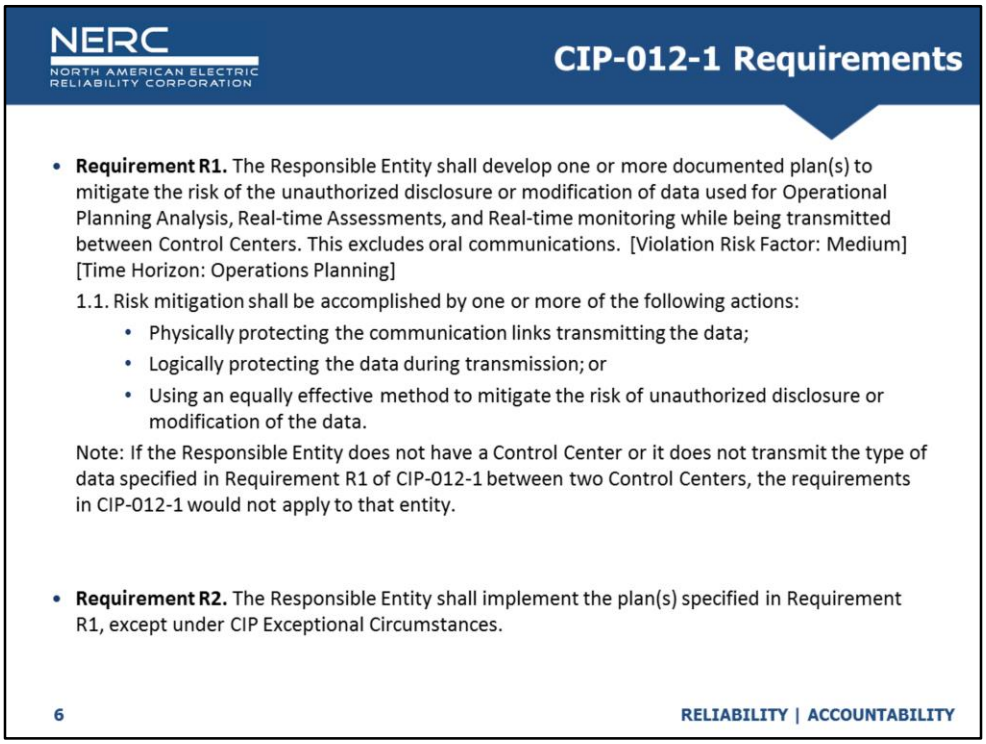


-Tom Foster-

Thanks David. To start the discussion on CIP-012-01, we first wanted to give a brief overview of the path the drafting team has taken to get us to where we are. As most of you know, in Order 822 the Commission directed NERC to develop standards that required the protection of communication links and sensitive bulk electric system data communicated between Control Centers. The Commission sought to ensure the confidentiality, integrity, and availability of these links and data were protected, and noted that entities could achieve this through physical means, logical means, or a combination of both.

Over the course of the past year or so, the SDT explored many options to satisfy the directive the Commission outlines in Order 822. Regarding the question of "what is sensitive bulk electric system data?" the team worked through formally defining the term sensitive bulk electric system data, scoping the data within the standards, and allowing an entity to define what needed to be protected as sensitive. We also looked at whether it would be best to have a prescriptive requirement that dictated the protection that needed to be employed, or allowing an entity to define adequate protections based on their environment. Lastly, the SDT explored different ways to associate risk, be it of the data or the impact level of Control Center, with the protection an entity would need to apply to satisfy the requirement.

Prior to a formal comment period and balloting, the SDT sought informal feedback on some of the concepts outlined above in early Spring. The feedback we received has since been incorporated and helped us in our first draft of the requirements to address the Commission's order. The current CIP-012-1 proposal is objective based and scopes the data based on currently approved Operations and Planning Standards. In addition, you will notice that the SDT is proposing explicitly handling the confidentiality and integrity concerns raised by the Commission in its order. As noted in the informal comment period and supported by the feedback we received, we did not explicitly handle the availability piece as it is adequately covered in various other standards.



-Tom Foster-

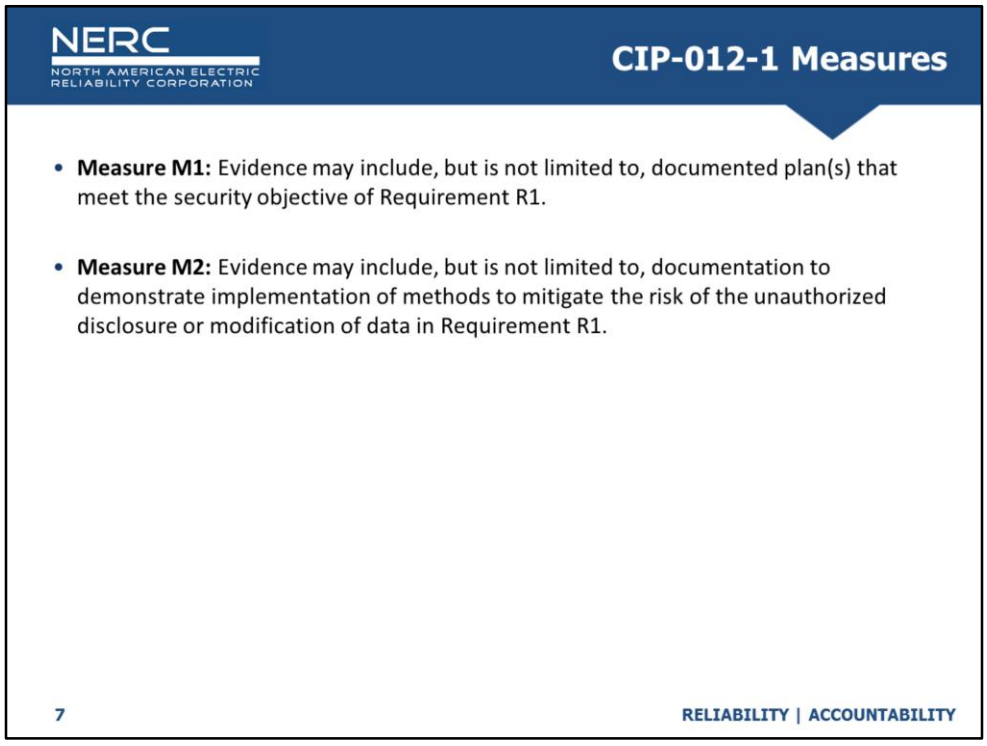
Now that we have some background information covered, the proposed requirements are:
Requirement R1. The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers. This excludes oral communications. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]
1.1. Risk mitigation shall be accomplished by one or more of the following actions:

Physically protecting the communication links transmitting the data;
Logically protecting the data during transmission; or
Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data.

Requirement R2. The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.

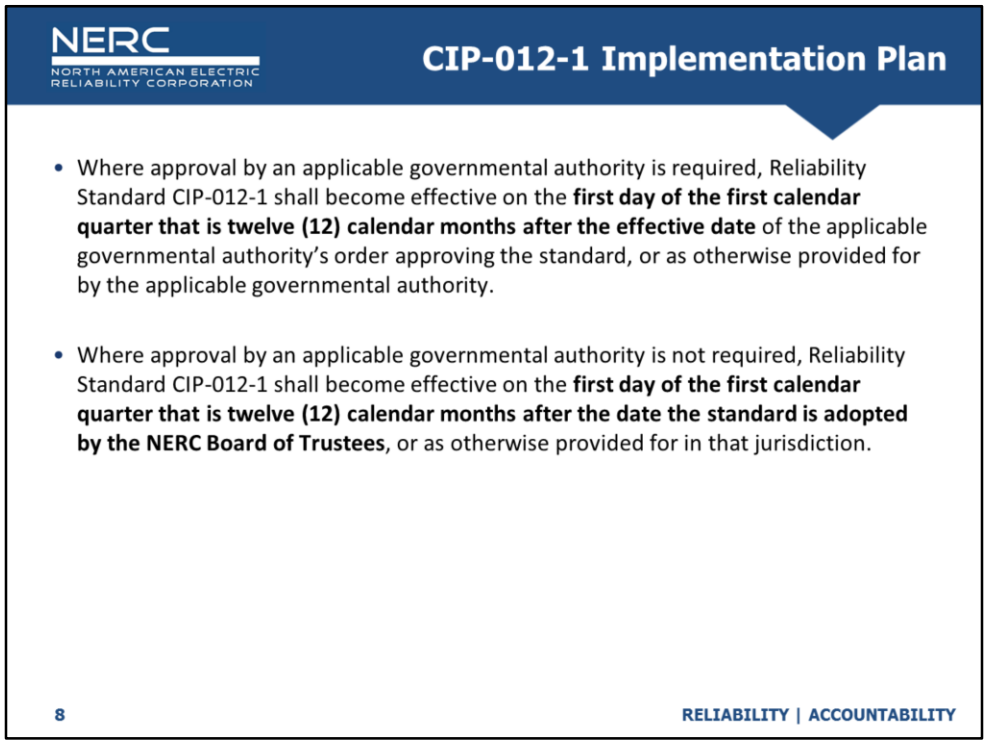
FERC Order No. 822 directed NERC to develop modifications to the CIP Reliability Standards to require Responsible Entities to implement controls to protect communication links and sensitive Bulk Electric System (BES) data communicated between BES Control Centers. Reliability Standard CIP-012-1 responds to that directive, requiring Responsible Entities to develop a plan to protect the confidentiality and integrity of sensitive data while being transmitted between Control Centers. Responsible Entities use various means to communicate information between Control Centers. The plan for protecting these communications is required for all impact levels due to the inter-dependency of multiple impact levels.

The type of data in scope of CIP-012-1 is data used for Operational Planning Analyses, Real-time Assessments, and Real-time monitoring. The terms Operational Planning Analyses, Real-time Assessments, and Real-time used are defined in the Glossary of Terms Used in NERC Reliability Standards and used in TOP-003 and IRO-010, among other Reliability Standards.
There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two geographically 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 contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.



-Tom Foster-

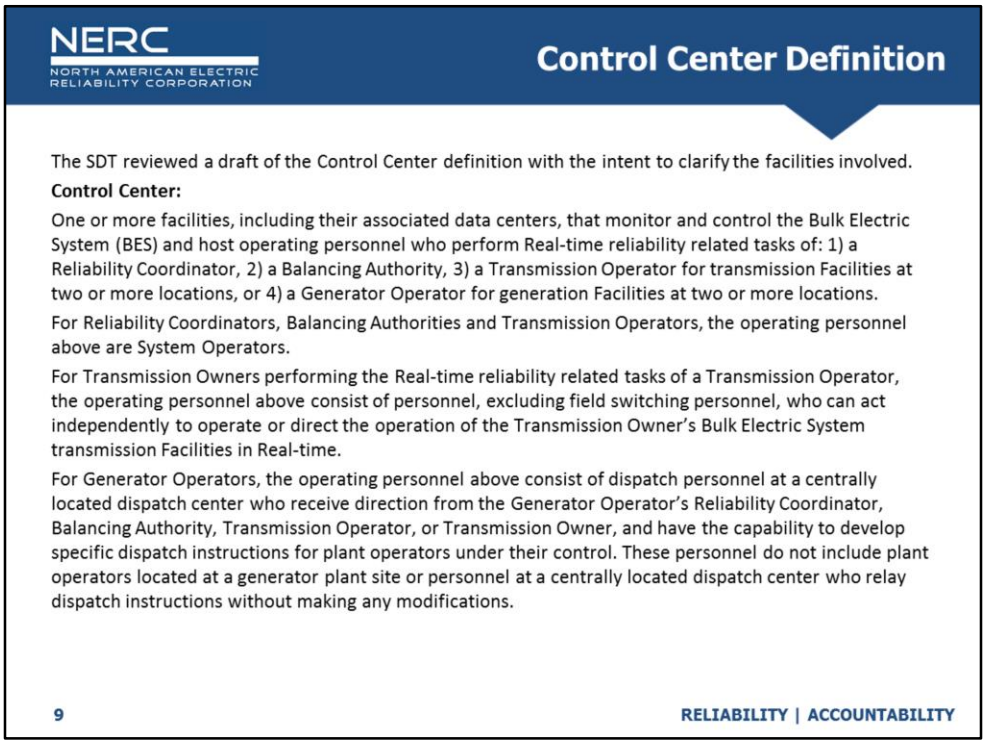
The measures associated with the proposed requirement are self-explanatory. A Responsible Entity must be able to provide the documented plan or plans developed for CIP-012-1 in order to evidence compliance with Requirement R1. Similarly, the Responsible Entity would then need to provide evidence that the developed plan or plans were implemented as documented. The draft measures do not include explicit evidence examples as this is dependent on the protection that the entity chooses to implement to protect the confidentiality and integrity of the data noted in the proposal.



-Tom Foster-

Lastly for the implementation plan, the SDT is proposing an effective date on first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the approval of the standard. Each entity with a Control Center, as defined in the Glossary of Terms, that transmits the data specified in Requirement R1 of CIP-012-1 would have 12 months to ensure both the development of a plan or plans is completed for CIP-012-1, as well as the implementation of that plan or plans.

That wraps up what we have for CIP-012-1. I'll now pass it over to Christine to talk about the work around the Control Center definition.

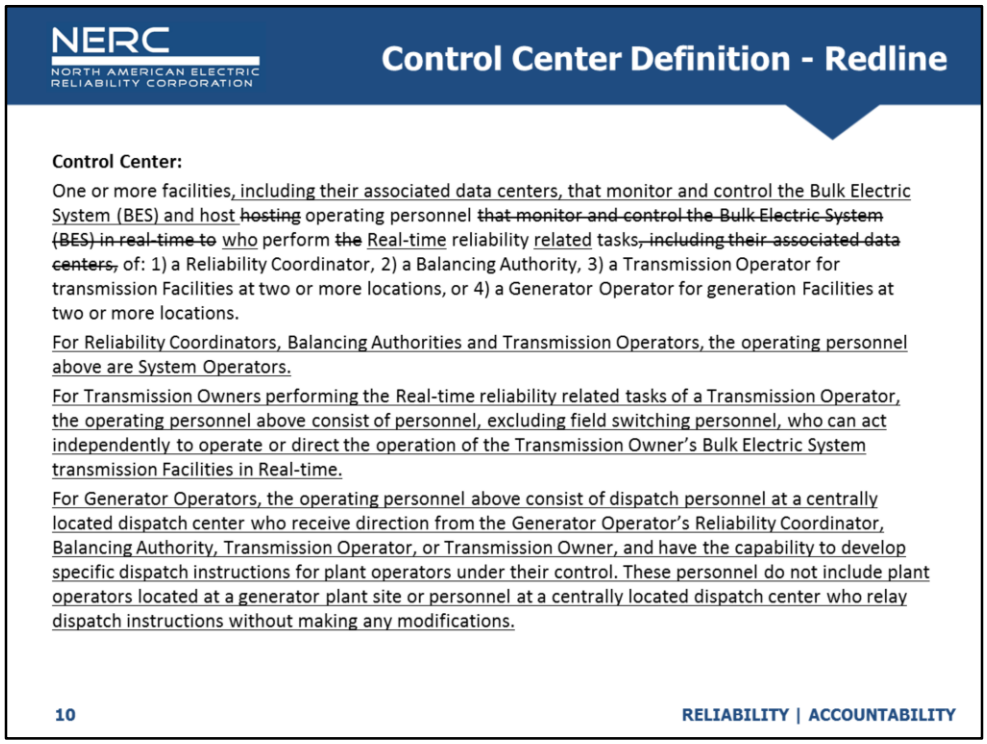


-Christine Hasha-

The Standard Authorization Request or SAR for this Drafting Team contains multiple issue areas that impact Control Centers. These areas include the CIP-012 changes we just discussed as well as the Transmission Owner Control Center issue that we will cover next. As we worked on these issues, the SDT identified potential improvements to the Control Center definition.

For a little history, while working on the Control Center definition we have now, the Version 5 CIP Standards Standard Drafting Team received comments stating that the scope of the Control Center definition did not adequately identify control centers. The comments noted that the defined term Control Center could inaccurately apply to some generator plant control rooms. In response, the Project 2008-06 SDT created criteria in CIP-002 that would categorize BES Cyber Systems associated with these control room facilities as low impact. Since there were no low impact requirements specific to Control Centers, this temporarily mitigated the issue.

Our current drafting team is now introducing new requirements that apply to low impact Control Centers in its draft of the CIP-012 standard.



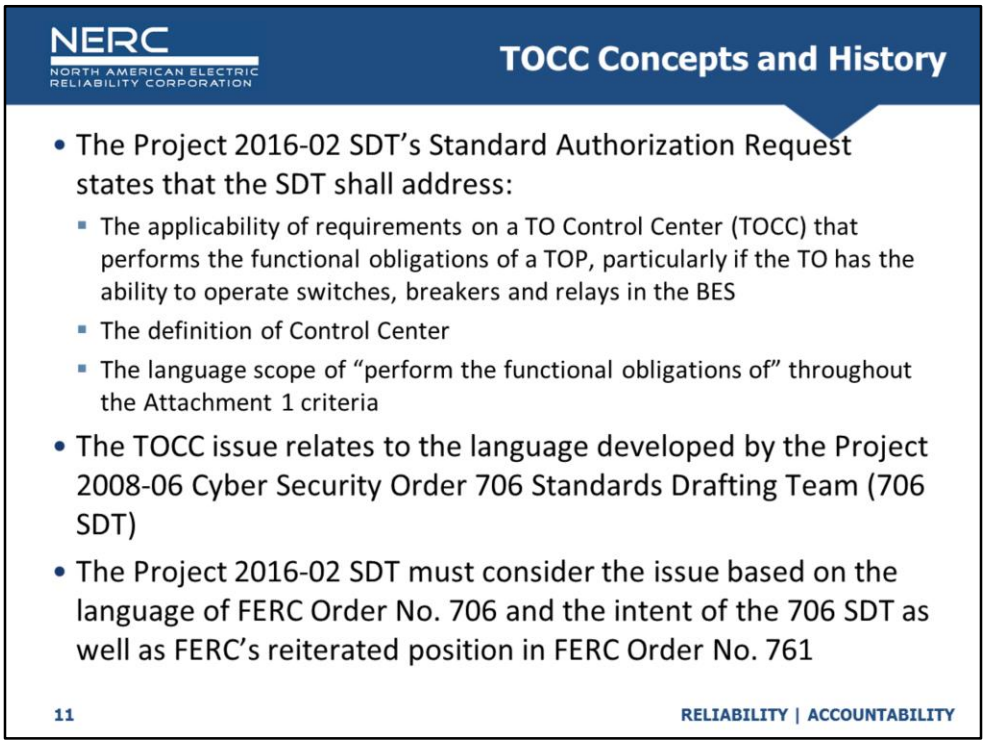
-Christine Hasha-

The drafting team is seeking comments on potential modifications to the Control Center definition to provide further clarification of the term "operating personnel." The proposed Control Center definition identifies facilities that have two characteristics. The first characteristic is that the facility hosts operating personnel that perform Real-time reliability-related tasks to operate the Bulk Electric System. The second characteristic is that the facility contains BES Cyber Systems that are used by operating personnel to monitor and control the BES.

We believe that operating personnel in this definition should align with personnel already identified in Reliability Standard PER-005-2. The purpose of Reliability Standard PER-005-2 is, "[t]o ensure that personnel performing or supporting Real-time operations on the Bulk Electric System are trained using a systematic approach." The proposed revisions to the Control Center definition clarify that operating personnel perform Real-time reliability-related tasks and lists functional entities that perform those tasks as identified in the applicability section of PER-005-2.

Along with comments on the possible definition, we are also seeking your input on the potential impact on scope or intent of any current standards such as COM-001-3; TOP-001-4; and IRO-002-5, as well as any pending Reliability Standard(s).

Now will turn it over to **Jennifer Flandermeyer** who will give an overview of the TOCC issue.

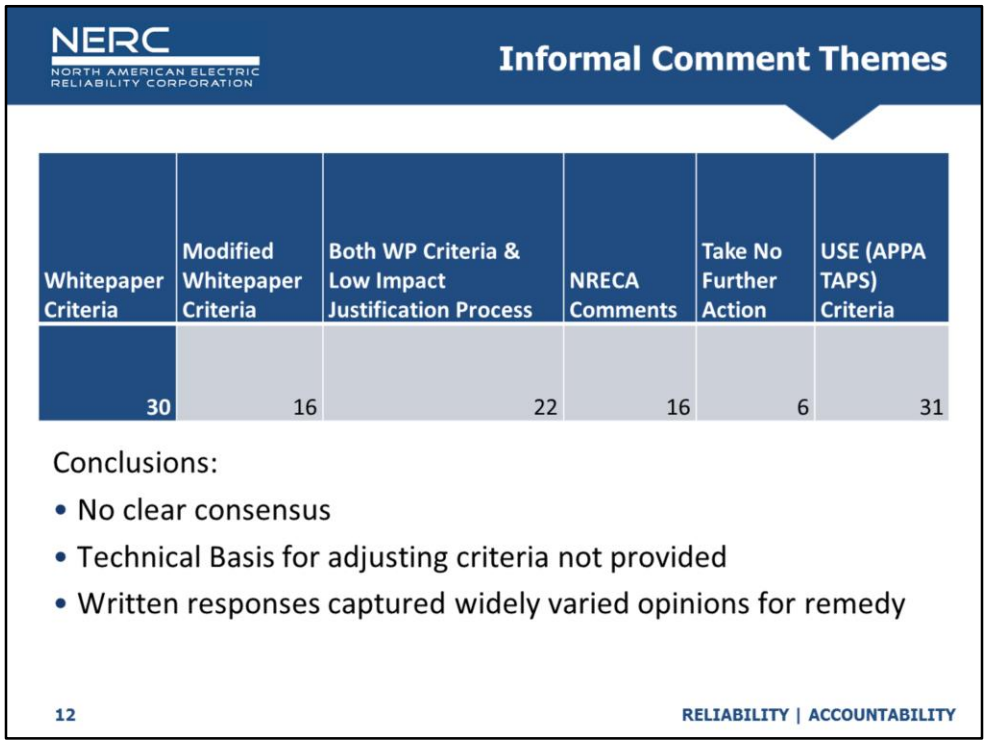


-Jennifer Flandermeyer-

Thank you, **Christine**. As a reminder, the NERC Project 2016-02 Standards Drafting Team's Standards Authorization Request encompassed items that were transferred to the SDT in a document from the Version 5 Transition Advisory Group. The transfer document stated there were multiple readings of the language "used to perform the functional obligation of" in CIP-002-5.1a, Attachment 1, criterion 2.12. In addition, the V5TAG suggested that the SDT consider three additional potential options or recommendations:

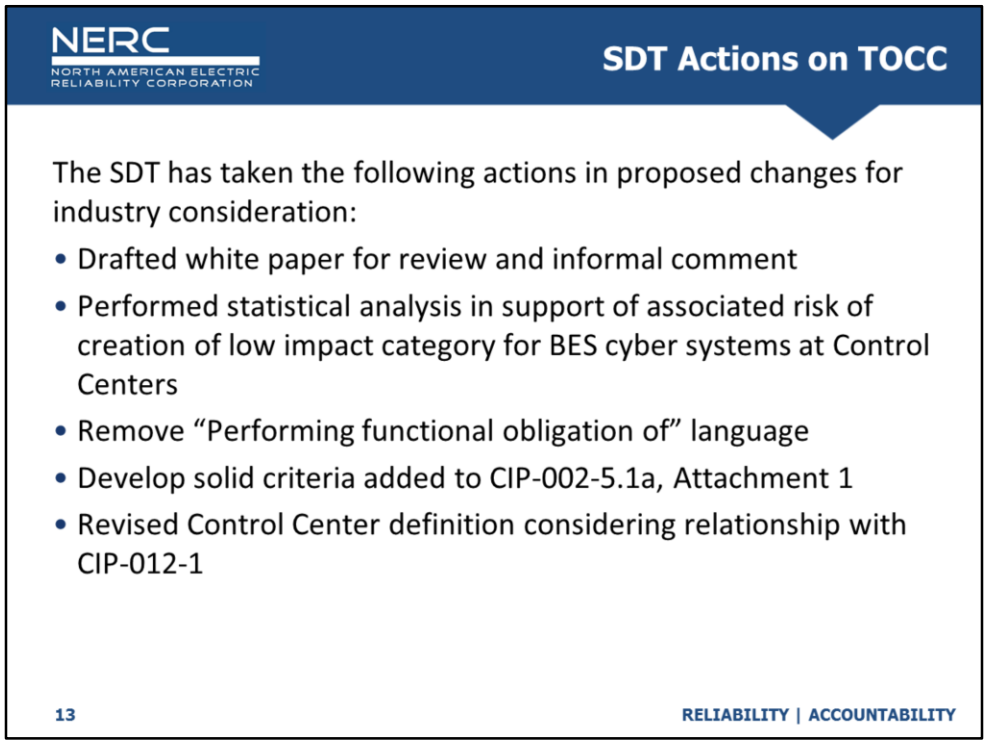
- Provide additional clarity or revisions to CIP-002-5.1a, Attachment 1. Specifically around Transmission Owner Control Centers performing the functional obligations of a Transmission Operator, in particular for entities with small or lower-risk Cyber Asset risks,
- Clarify applicability of requirements on a TOCC that perform the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES. CIP-002-5.1a indicates that any Control Center performing the actions noted above is to be considered as having BES Cyber Systems categorized as medium impact, if not already identified as high impact. Currently, there is no allowance for a low-risk entity performing TOP functions to identify their assets as containing only low impact BES Cyber Systems, or
- Revise the definition of Control Center if additional clarity will improve consistency in implementation, compliance and enforcement, and determination of applicability.

It is important to remember that the V5TAG issues relate to the language developed by the Project 2008-06 Cyber Security Order 706 Standards Drafting Team (706 SDT) as directed in FERC Order No. 706. The NERC Board of Trustees adopted the stakeholder-approved CIP Version 5 standards and FERC approved the standards on January 18, 2006. The Project 2016-02 SDT must consider the V5TAG issues based on the language of FERC Order No. 706 and the intent of the 706 SDT. In addition to FERC Order No. 706, FERC reiterated its position on April 19, 2012 in FERC Order No. 761 and that language must also be considered by the SDT related to concerns about misuse and Control Centers.



-Jennifer Flandermeyer-

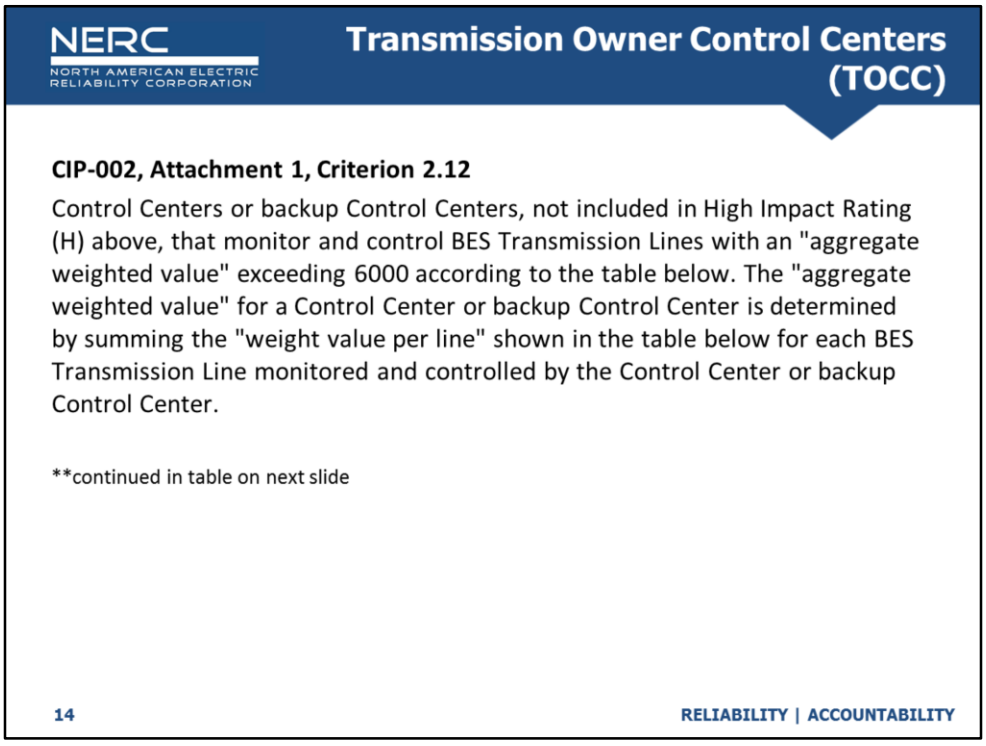
In March 2017, the SDT posted the TOCC materials for informal comment. Most of the commenters agreed with the TOCC whitepaper assumptions about authority and capability. A number of comments requested the consideration be expanded to the TOP functions as well. Industry comments reflected a focus on risk to the BES presented by the capability of the Control Centers in question. However, with the comments received the comments did not define a clear consensus, provide further technical basis for adjusted criteria or suggest additional reasons for decreased risk.



-Jennifer Flandermeyer-

Based on informal comments from industry and risk analysis of the SDT, and to address the issues captured in the SAR, the SDT proposes to take several actions. To capture these at a high level, these actions are as follows: (1) Remove "performing functional obligation of" language; (2) define specific criteria in CIP-002-5.1a, Attachment 1, criteria 2.12; and (3) revision of the definition of Control Center in collaboration with the work completed on communication networks in the proposed CIP-012-1.

Now, I will turn it over to Mark Riley to discuss the TOCC revisions in more detail.



-Mark Riley-

Thank you, Jennifer.

The SDT has submitted a request to the Standards Committee to post proposed modifications to CIP-002-5.1a, Attachment 1, Criterion 2.12 for industry ballot and comment. This revised criterion clarifies the applicability of requirements for a TO Control Center that performs the functional obligations of a TOP. The criterion establishes a minimum threshold for medium impact BES Cyber Systems associated with Control Centers that monitor and control BES Transmission Lines, regardless of a Responsible Entity's functional registration. This allows TOs and TOPs to identify their BES Cyber Systems associated with Control Centers as medium or low impact based on the BES Cyber System's span of control. This contrasts with the currently approved Criterion 2.12, which identifies BES Cyber Systems as medium impact when they are associated with a Control Center or backup Control Center used to perform the functional obligations of the TOP and not included in the high impact rating.

The proposed criterion aligns with CIP-002-5.1a, Attachment 1, Criterion 2.5. It establishes an average MVA line loading, based on voltage class, for BES Transmission Lines operated between 100 and 499 kV. The aggregate weighted value for applicable BES Cyber System must exceed 6000 to meet the minimum threshold established in Criterion 2.12 and can be calculated by summing the "weight value per line" for each BES Transmission Line that is monitored and controlled by the Control Center or backup Control Center (as shown in the table on the following slide). If the aggregate weight value of lines exceed 6000, the Control Center's associated BES Cyber System(s) must be identified as medium impact. If the aggregate weight value of lines does not exceed 6000, the Control Center's associated BES Cyber System(s) must be evaluated for classification as low impact pursuant to Criterion 3.1.

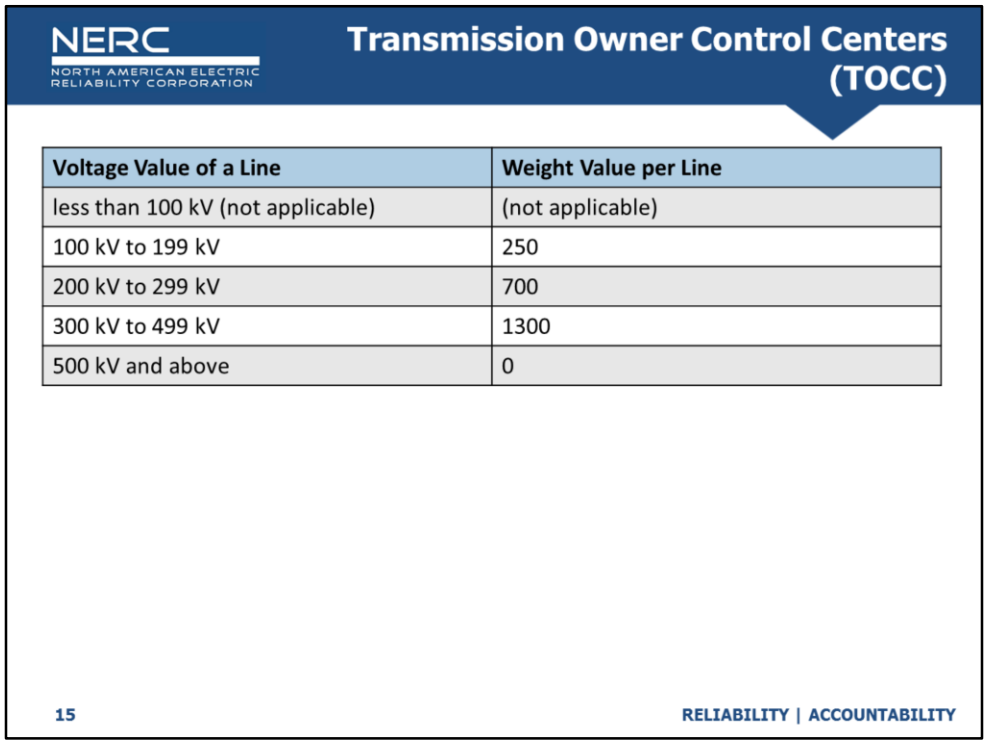
Additional Notes:

The SDT finalized documents for formal comment and ballot

Modifications to clarify CIP-002-5.1a, Attachment 1, Criterion 2.12
Aligns to CIP-002-5.1a, Attachment 1, Criterion 2.5
Implementation Plan to be effective the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the standard.

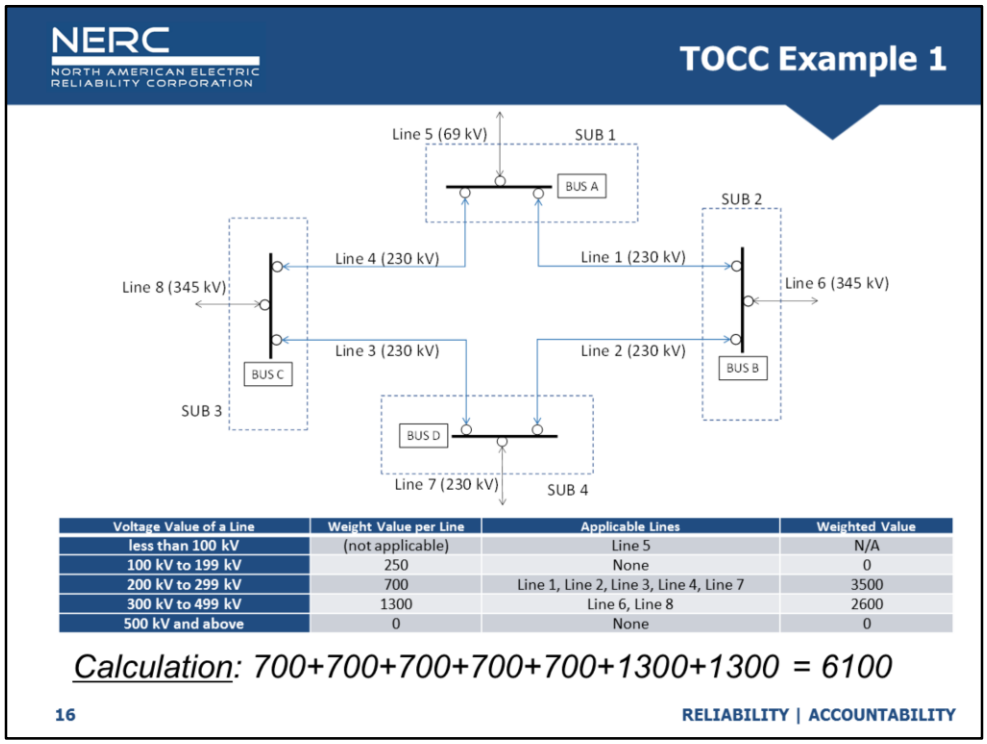
The SDT will post a request for comment on the following:

The potential modification clarifies CIP-002-5.1a Attachment 1, Criterion 2.12 as requested by the V5TAG Transfer Document.
The threshold of 6000 aggregate weighted value to establish the minimum threshold for medium impact BES Cyber Systems used by and located at Control Centers that monitor and control Transmission.



-Mark Riley-

The table in revised Criterion 2.12 establishes an average MVA line loading, based on voltage class, for BES Transmission Lines operated between 100 and 499 kV. Transmission Lines operated above 499 kV are excluded from this criterion because BES Cyber Systems used by and located at Control Centers that monitor and control BES Transmission Lines at 500 kV or higher are already categorized as high impact BES Cyber Systems pursuant to CIP-002-5.1a, Attachment 1, Criterion 1.3.

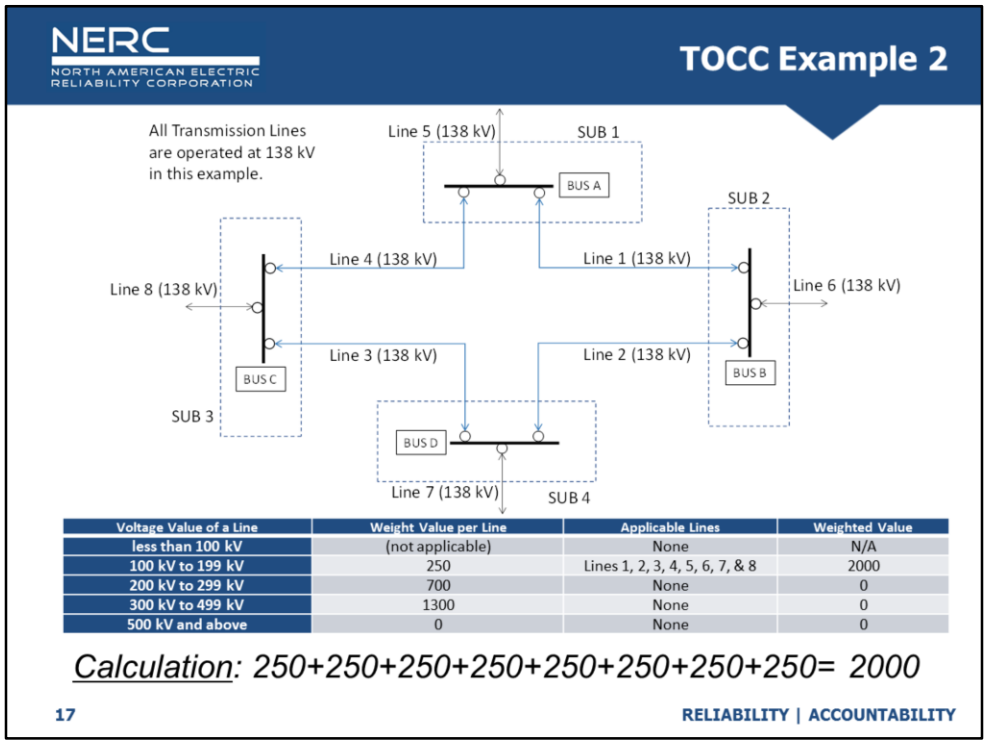


Voltage Value of a Line	Weight Value per Line	Applicable Lines	Weighted Value
less than 100 kV	(not applicable)	Line 5	N/A
100 kV to 199 kV	250	None	0
200 kV to 299 kV	700	Line 1, Line 2, Line 3, Line 4, Line 7	3500
300 kV to 499 kV	1300	Line 6, Line 8	2600
500 kV and above	0	None	0

-Mark Riley-

Next we will demonstrate the application of Criterion 2.12 by calculating the aggregate weighted value for an example BES Cyber System.

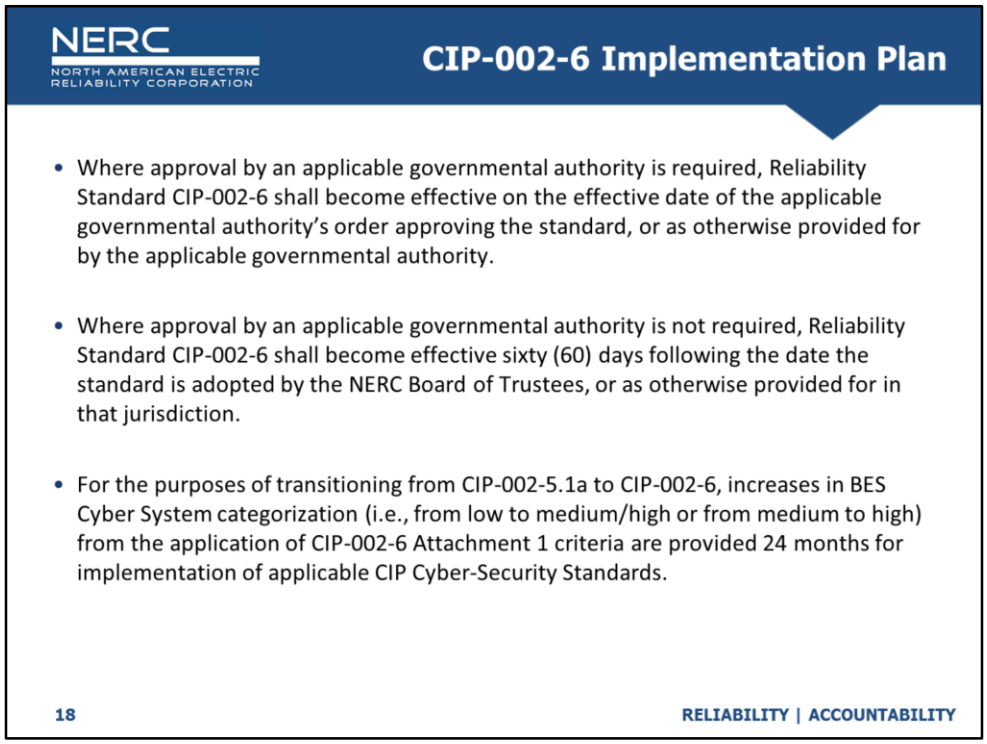
In this example, a BES Cyber System is associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line. The weighted value for each BES Transmission Line is identified in the table on this slide by voltage classification. The calculation of the weighted values is detailed in this slide and equates to an aggregate weighted value of 6100, which is above the minimum threshold for the medium impact rating required in Criterion 2.12. In accordance with this criterion, the BES Cyber System associated with this Control Center should be categorized as a medium impact BES Cyber System.



Voltage Value of a Line	Weight Value per Line	Applicable Lines	Weighted Value
less than 100 kV	(not applicable)	None	N/A
100 kV to 199 kV	250	Lines 1, 2, 3, 4, 5, 6, 7, & 8	2000
200 kV to 299 kV	700	None	0
300 kV to 499 kV	1300	None	0
500 kV and above	0	None	0

-Mark Riley-

In this additional example, a BES Cyber System is associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line. The weighted value for each BES Transmission Line is identified in the table on this slide by voltage classification. The calculation of the weighted values is detailed in this slide and equates to an aggregate weighted value of 2000, which is below the minimum threshold for a medium impact rating required in Criterion 2.12. The BES Cyber System associated with the Control Center in this example should be categorized as a low impact BES Cyber System, pursuant to Criterion 3.1.



-Mark Riley-

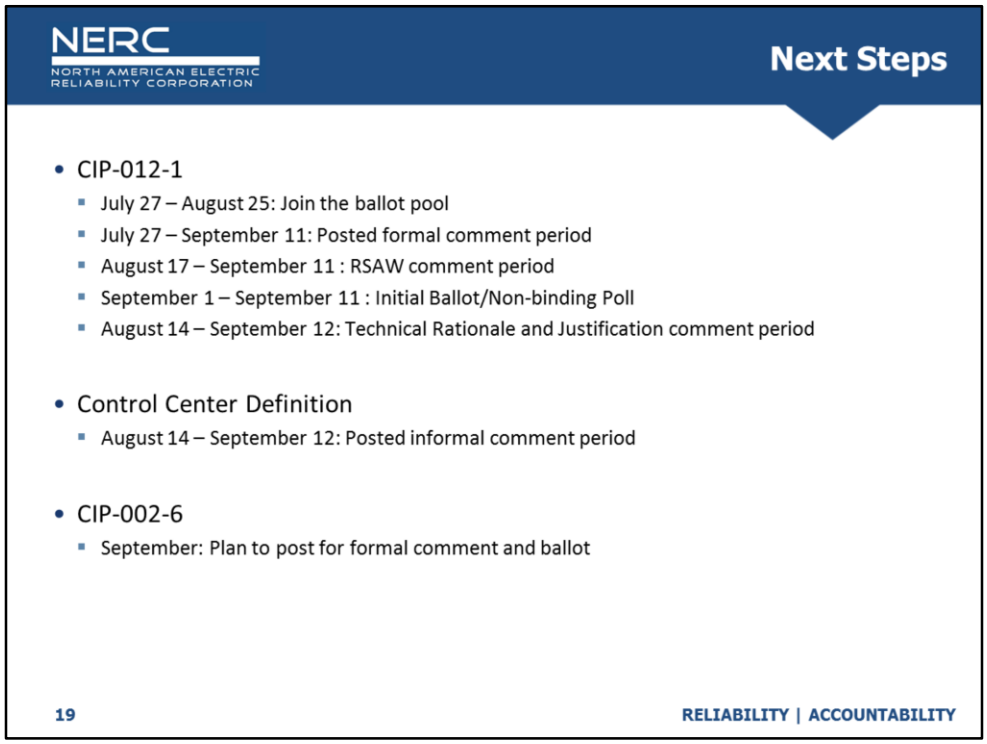
In addition to the revised standard, the SDT has submitted a proposed implementation plan for CIP-002-6. The plan details the following timelines:

Where approval by an applicable governmental authority is required, Reliability Standard CIP-002-6 shall become effective on the effective date of the applicable governmental authority's order approving the standard.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-002-6 shall become effective sixty (60) days following the date the standard is adopted by the NERC Board of Trustees.

Additionally, for the purposes of transitioning from CIP-002-5.1a to CIP-002-6, responsible entities that experience increases in BES Cyber System categorization (from low to medium/high or from medium to high) from the application of CIP-002-6 Attachment 1 criteria are provided 24 months for the implementation of applicable CIP Cyber-Security Standards.

Now will turn it over to Jay Crib who will review next steps for the projects.



-Jay Cribb-

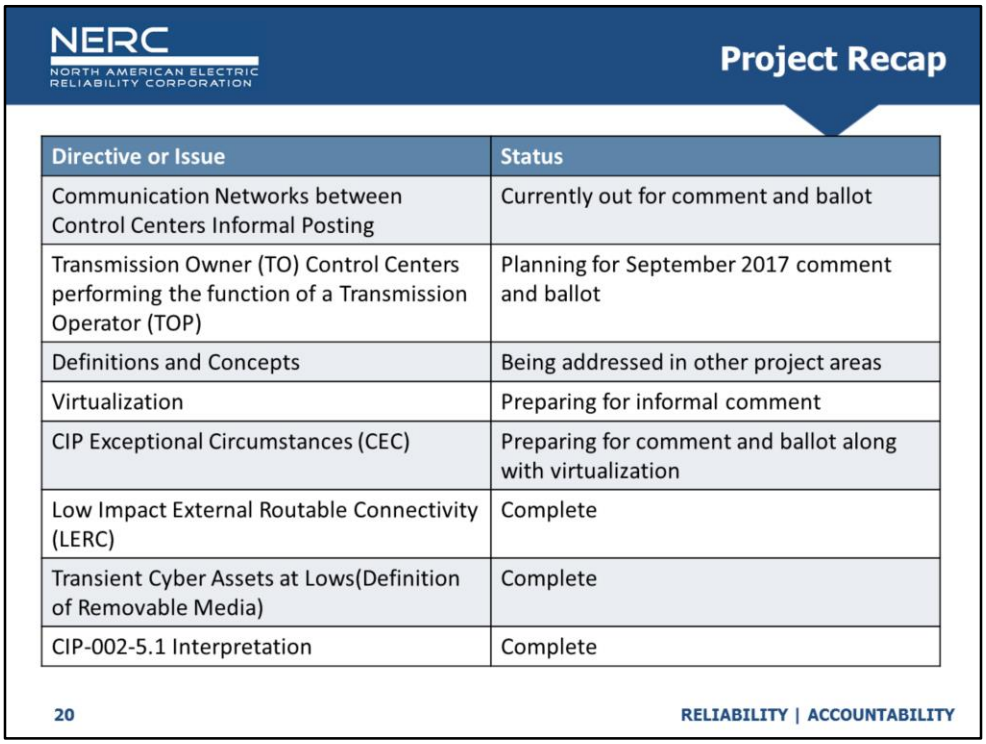
Thanks, Tom. First, a quick recap of what is out for comment now and coming in the near future with the dates to be aware of.

First is CIP-012-1, the new standard on Control Center Communications and protecting data while its being transmitted between them. That standard posted for formal comment and ballot on July 27 and you can join the ballot pool through August 25, which is this Friday and is the most immediate deadline. The next deadline is Monday, Sept 11 when the formal comments and ballots are due by 8 PM Eastern. The RSAW for CIP-012 has also been posted to the project page and those comments are due to the RSAWfeedback@nerc.net email address on Sept 11 as well.

Now concurrent with this are two *informal* comment periods; one is for the proposal to change the Control Center definition to clarify the operating personnel as discussed previously. The second one is not on the slide, but you'll notice that CIP-012-1 has no "Guidelines and Technical Basis" section per the new NERC format. That type of information is now in a separate document containing the Technical Rationale and Justification for CIP-012-1 and it is posted for informal comment separately from the standard. These two informal comment periods close the next day on Tues, Sept 12 at 8 PM Eastern. Since the control center definition and CIP-012 are highly related, the SDT plans to eventually bring them to final ballot concurrently.

So, three big dates coming up to have on your radar: this Friday for joining the ballot pool, then Monday Sept 11 for comments and ballot on CIP-012 and the RSAW, and Tues Sept 12 for the Control Center definition and CIP-012 technical rationale and justification document.

That is what's in play as we speak. Our plan for CIP-002-6 containing the new criteria for low impact Transmission control centers is to post a first draft for formal comment and ballot coming up in September, so be on the lookout for that.
Next slide please.



-Jay Cribb-

Finally let's look at a brief recap of the scope of this drafting team's work on its issues and directives - past, present, and yet future. For the present, we have CIP-012-1 concerning the communication networks between control centers out for comment and ballot.

For the Transmission Owner control centers performing the function of a Transmission Operator, we are planning on posting CIP-002-6 next month for comment and ballot.
Also in the V5TAG issues list were several clarifications regarding definitions and concepts. We are not addressing those as a standalone area but they are being addressed as we go through these other areas. For example, virtualization touches on several of these definitions are being handled within that body of work.

Speaking of virtualization, the SDT is continuing the work to determine what changes or new concepts may be needed in the standards to handle any issues brought about by virtualization technologies. For one example and to reminisce a bit for those who have been around this for a while, we know the core foundation for today's CIP standards was established back in the 2002/2003 timeframe with "Appendix G" and the "Urgent Action 1200" standards and they have a strong layer 3 routable protocol focus for security controls around communications. But 15 years later we know that within today's virtualization technologies these types of security controls can be and are implemented at various levels and not just at layer 3 routing. So we're thinking through concepts that we may need to modify or introduce so that we as industry can use virtualization technologies and take credit for good security controls that may not happen to be at layer 3. These are the kinds of things at the core of the team's virtualization work. The team has already produced three technical NERC webinars on virtualization pertaining to virtual hosts, networking, and storage that are available on the NERC website. As we look into these areas with an eye towards future proofing the standards, next on the agenda is an informal comment period to get your feedback on our current thinking in regards to some proposed new and modified definitions and requirements.

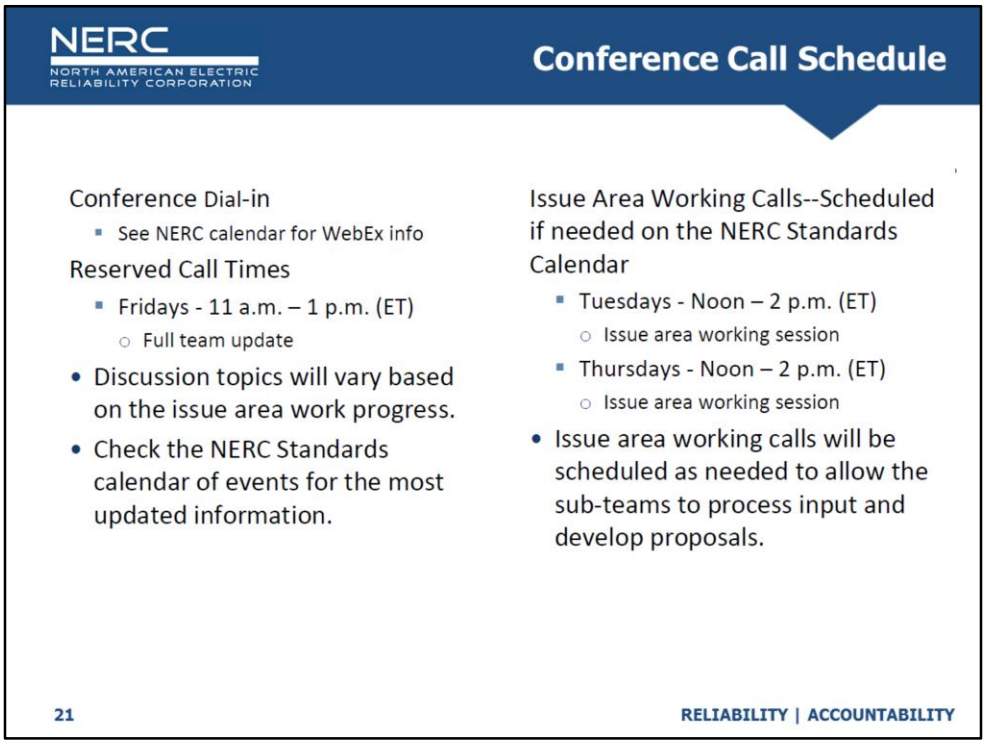
We are also looking to post at the same time as virtualization the new CIP Exceptional Circumstances additions. This issue was added to our team's scope during the SAR comment period and was added because there are instances of requirements that are heavily dependent on one another where one is eligible for a CEC but the other is not. The SDT has performed an extensive review of where CEC is or should be available in the standards and will be posting those for comment and ballot shortly.

For a brief recap of what the team has already accomplished, remember we have CIP-003-7 that passed industry ballot and is currently filed with FERC awaiting approval. That work covered two areas. First is the clarifications to low impact external routable connectivity or LERC as directed by the FERC order. This work resulted in a simplified rewrite of the 'electronic access controls' section of the cyber security plan required in Appendix 1 for assets containing low impact BES Cyber Systems and some conforming changes to the examples in the guidelines and technical basis.

The second issue we addressed in CIP-003-7 was also from the FERC order and covered the addition of section 5 to that same Appendix 1 cyber security plan. This section was added to mitigate the risks of introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media.

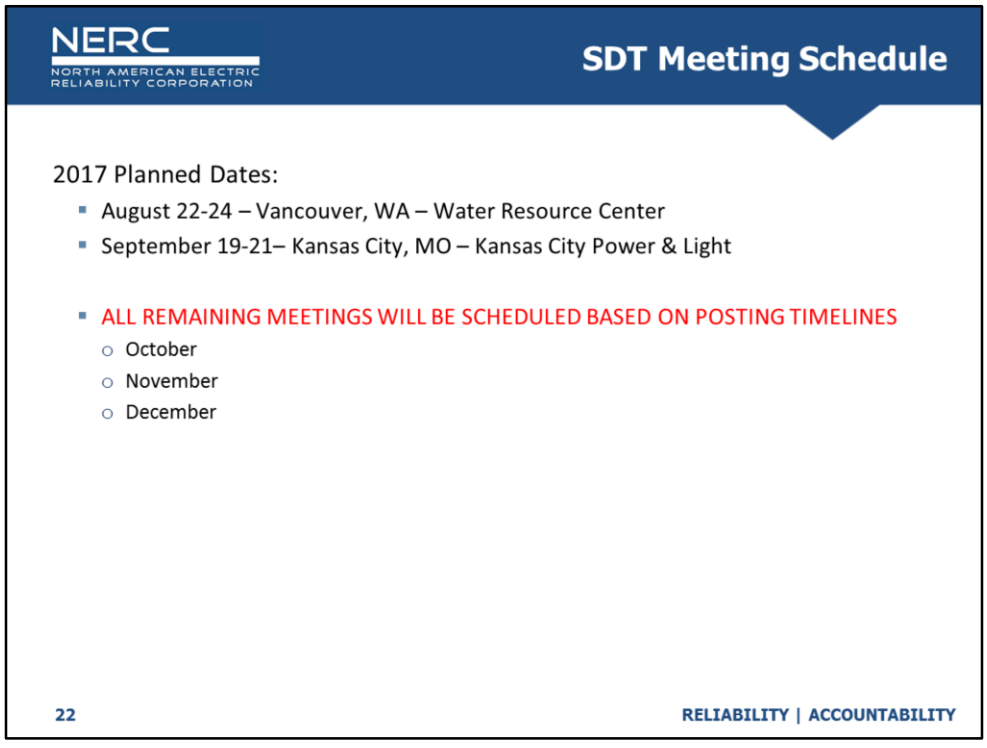
And finally in our recap, one of the first things the team accomplished was to answer a request for interpretation regarding three questions clarifying the term "Shared BES Cyber Systems" that resulted in version CIP-002-5.1a that has been approved by FERC.

Rarely a dull moment on a CIP drafting team. With that, I'll turn it back over to David.



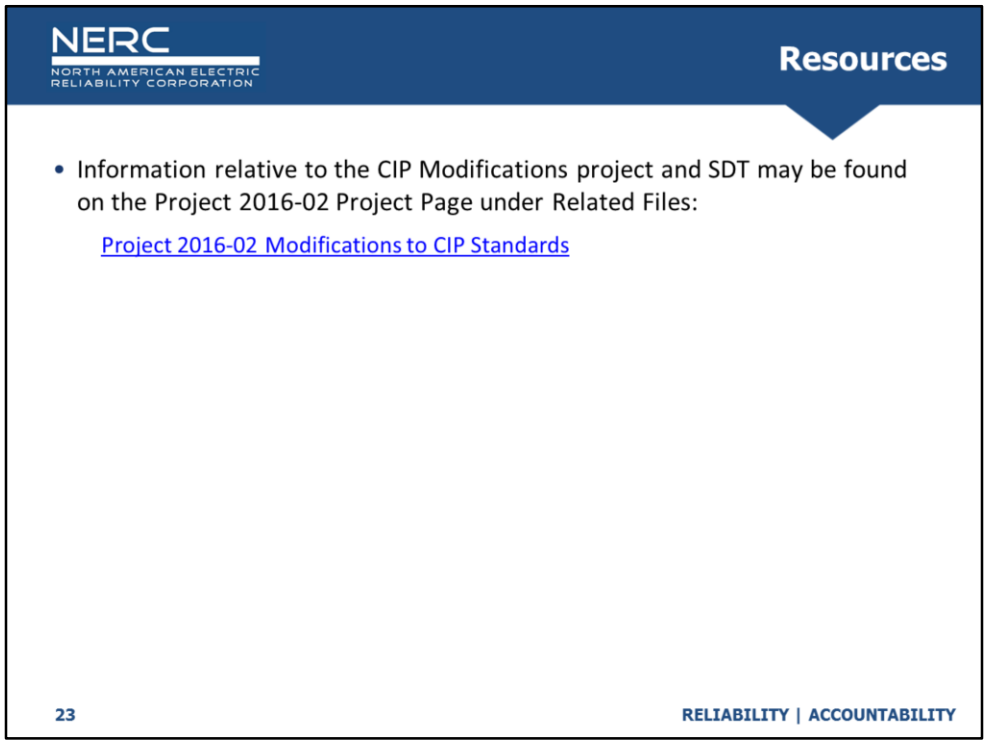
-Jay Cribb-

We do have weekly calls to work on further developing the standards in response to our SAR. We also have a full team meeting to recap the week's work. All of the meetings are scheduled on the NERC calendar. Please see calendar for details.



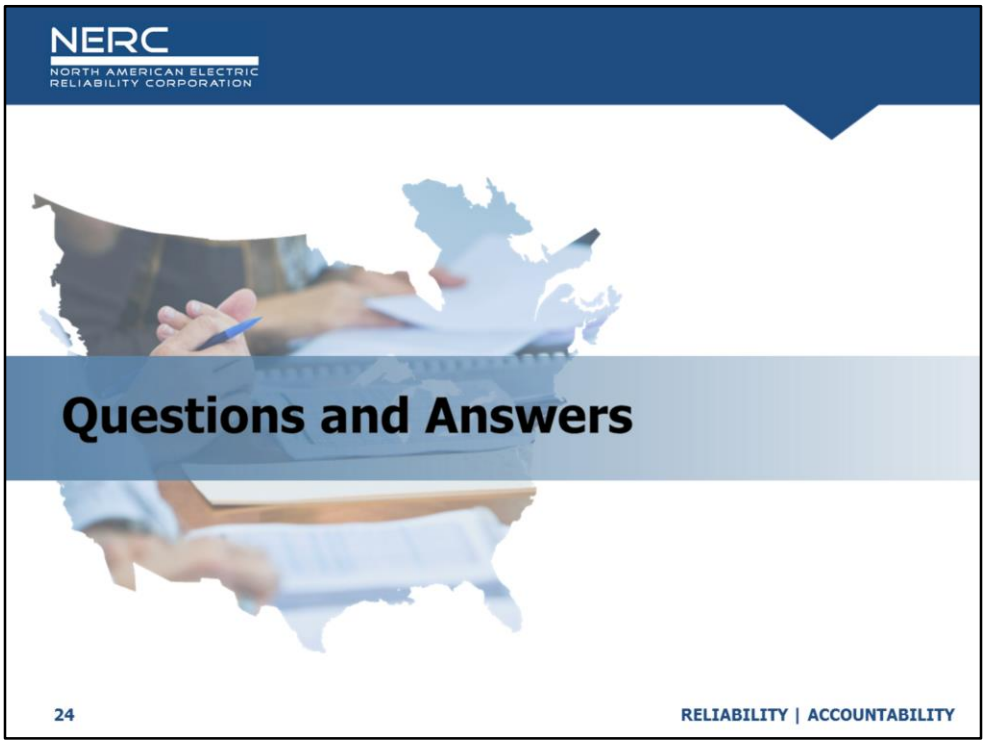
-Jay Cribb-

Note that ALL REMAINING MEETINGS WILL BE SCHEDULED BASED ON POSTING TIMELINES



-Jay Cribb-

We have provided a link to the project page for you.
We will now go into the question and answer portion of the webinar. Please be sure to use the chat feature to submit a question for the team's review. Please give us a moment to get things ready.



-Forrest Krigbaum-

(AFTER Q&A)

This concludes today's webinar. We would like to thank our presenters and thank you for joining us. We hope that you have found the presentation helpful in your preparation of comments. Please keep in mind the comment and ballot deadlines. The materials will be posted on the Project 2016-02 project site. Have a great day.