NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Agenda
Reliability and Security Technical Committee

Virtual Meeting via WebEx

June 8, 2021 | 1:00–4:30 p.m. Eastern

Attendee WebEx Link: Join Meeting

Call to Order

NERC Antitrust Compliance Guidelines and Public Announcement

Introductions and Chair's Remarks

1. **Administrative items**
    a. Arrangements
    b. Announcement of Quorum
    c. Reliability and Security Technical Committee (RSTC) Membership 2020-2023*
        i. RSTC Roster
        ii. RSTC Organization
        iii. RSTC Charter
        iv. Participant Conduct Policy

Consent Agenda

2. **Minutes - Approve**
    a. March 2-3, 2021 RSTC Meeting*
3. **RSTC Executive Committee Action – Affirm**
    a. Security Working Group - Appoint Katherine Street (Duke Energy) as Co-chair
    b. Electric Gas Working Group - Appoint Mike Knowland (ISO New England) as Chair and Daniel Farmer (Entergy) as Vice-Chair

Regular Agenda

4. **Remarks and Reports**
    a. Remarks – Greg Ford, RSTC Chair
        i. Subcommittee Reports*
        ii. RSTC Work Plan
    b. Report of May 13, 2021 Member Representatives Committee (MRC) Meeting and Board of Trustees Meeting – Chair Ford

5. **Resources Subcommittee (RS) Documents – Approve** – Greg Park, RS Chair | Rich Hydzik, Sponsor

   a. *Reliability Guideline: ACE Diversity Interchange** is a three-year review of an existing, posted document. This document was posted for a 45-day comment period and conforming revisions made to it based on comments received. A clean and redline version were included in the agenda package along with a response to comments. The RS is requesting that this document be approved.

   b. *Reliability Guideline: Operating Reserve Management** is also a three-year review of an existing, posted document. This document was posted for a 45-day comment period and conforming revisions made to it based on comments received. A clean and redline version were included in the agenda package along with a response to comments. The RS is requesting that this document be approved.

   c. *Balancing and Frequency Control Reference Document** is also a three-year review of an existing, posted document. This document was posted for a 45-day comment period and conforming revisions made to it based on comments received. A clean and redline version were included in the agenda package along with a response to comments. The RS is requesting that this document be approved.

6. **Reliability Guideline: Inadvertent Interchange* – Accept to Post Document for 45-day Comment Period -** Greg Park, RS Chair | Rich Hydzik, Sponsor
   The Reliability Guideline: Inadvertent Interchange is a three-year review of an existing guideline that has been updated. Guideline Metrics section has been added in addition to the content update. The RS is requesting that this document be accepted to post for a 45-day comment period.

7. **Reliability Guideline: Gas and Electrical Operational Coordination Considerations*** – **Approve** – Chris Pilong, RTOS Chair | Todd Lucas, Sponsor

   The Reliability Guideline: Gas and Electrical Operational Coordination Considerations was revised by the Real Time Operating Subcommittee and the Electric Gas Working Group. This document was posted for a 45-day comment period and conforming revisions made to it based on comments received. A clean and redline version were included in the agenda package along with a response to comments.

8. **Security Guideline for the Electricity Sector: Assessing and Reducing Risk* – Approve** – Brent Sessions, SWG Co-Chair | Christine Hasha, Sponsor

   The purpose of this Guideline is to help organizations determine their current security and compliance posture and develop an improvement plan for addressing any gaps that are identified. The tool for that analysis maps requirements of the CIP Reliability Standards to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (hereafter referred to as “the framework”), and it can help a responsible entity identify areas that may require further action. This document was posted for a 45-day comment period and conforming revisions made to it based on comments received. A clean and redline version were included in the agenda package along with a response to comments.

9. **Implementation Guidance: Cloud Solutions and Encrypting BES Cyber System Information* – Endorse** – Brent Sessions, SWG Co-Chair | Christine Hasha, Sponsor

   The purpose of this Compliance Implementation Guidance is to provide examples for how encryption can be utilized to secure and restrict access to BES Cyber System Information in various commonly used cloud services. The RSTC endorsed this Compliance Implementation Guidance in June of 2020 and it was submitted to the ERO for approval. The ERO Enterprise identified some concerns with the guidance document and provided feedback to the team. The SWG made revisions to the document to address the ERO Enterprise's concerns and are seeking RSTC endorsement to submit the document to the ERO for endorsement as Compliance Implementation Guidance.

10. **MOD-032 Technical Reference Document* – Approve -** Shawn Patterson, PPMVTF Chair

    a. This technical reference document provides useful information and materials for entities regarding the development of models for interconnection-wide base case creation. The reference document focuses specifically on the provision of data and models by generator owners to the transmission planner and planning coordinator following MOD-032 requirements. The document provides details regarding the types of information provided. This action completes the scope of work for the PPMVTF and the Chair requests RSTC approval.

    b. The Chair request that the RSTC approve to disband the PPMVTF.

11. **Security Integration and Technology Enablement Subcommittee (SITES) Update and Work Plan* – Approve –** Benny Naas, SITES Chair | Marc Child, Sponsor

    The SITES has begun implementing and updating their work plan. Chair Naas will provide a status update as well as a revised work plan for approval.

2:40 P.M. - BREAK – 15 MINS

12. **Inverter-based Resources Performance Working Group (IRPWG) San Fernando Disturbance Follow-Up White Paper* - Approve –** Al Schriver, IRPWG Chair | Jody Green, Sponsor

    This brief white paper was developed by the NERC Inverter-Based Resource Performance Working Group (IRPWG) as a follow-up to the July 2020 San Fernando Disturbance Report published by NERC. That report contained a set of key findings and recommendations. The IRPWG discussed each of the key findings and recommendations in detail, provides a brief technical discussion and basis for each item, and where appropriate recommends follow-up action items. Table 1 shows the key findings and recommendations from the NERC disturbance report on the left-hand column and the IRPWG follow-up and recommendations for each item in the right-hand column.

13. **IRPWG TPL-001-5 SAR for BPS-Connected Inverter-based Resources* - Endorse –** Al Schriver, IRPWG Chair | Jody Green, Sponsor

    Considering current trends, the NERC IRPWG undertook review of the TPL-001 standard for considering BPS-connected IBRs. This review is captured in the following RSTC-approved white paper:

    IRPTF/IRPWG: IRPTF Review of NERC Reliability Standards – March 2020 (here)

    This SAR proposes to update TPL-001-5.1 to address the issues identified in the white paper. The IRPWG is seeking endorsement of the SAR.

14. GADS Section 1600 Data Request* – Accept to post for a 45-day comment period – Donna Pratt, NERC Staff

As an addition to the existing Section 1600 Generator Availability Data System (GADS) data request, accept the posting for a 45-day public comment period on the proposed data collection:

- GADS Conventional – Additional design and event data.
- GADS Photovoltaic (PV) – Configuration, performance and event data as well as outage detail.
- GADS Wind – Configuration, performance and event data as well as outage detail. Clarify reporting requirements related to plant size and commissioning date.

15. 2021 State of Reliability Report* – Information – John Moura and Donna Pratt, NERC Staff

An embargoed version of the 2021 State of Reliability Report (SOR) will be provided to RSTC members for their review and comment. This presentation will provide information regarding the contents, commenting period and approval dates for the SOR.

16. Vice Chair Election – Approve – Jody Green, RSTC Nominating Subcommittee

Due to a member resignation, the RSTC's Nominating Subcommittee (NS) held a nomination period to fill the RSTC Vice Chair role. Per the RSTC Charter, "The NS proposes chair and vice-chair candidates. The full RSTC will elect the chair and vice chair. The chair and vice chair shall not be from the same sector. The elected chair and vice chair are approved by the NERC Board." Once approved by the NERC Board, the elected member will complete the remainder of the term for the vacated seat. The NS reviewed the nominees during a May 24, 2021 conference call and recommends Rich Hydzik (Avista) to be elected as the RSTC Vice Chair.

17. Chair's Closing Remarks and Adjournment

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

DRAFT Meeting Minutes
Reliability and Security Technical Committee

March 2-3, 2021

Virtual Meeting via WebEx

A regular meeting of the NERC Reliability and Security Technical Committee (RSTC) was held on March 2-3, 2021, via webinar. The meeting presentations are posted on the RSTC website here.

Chair Ford called the meeting to order, and thanked everyone for attending. Tina Buzzard reviewed the procedures for the meeting, reviewed the Antitrust Compliance Guidelines, and confirmed quorum, as well as provided an overview of the polling actions to be used for Committee actions during the meeting.

Introductions and Chair's Remarks

Chair Ford provided an overview of the agenda noting that due to the number of action items before the Committee it may be necessary to defer some non-action topics to the next meeting.

Chair Ford called on Nina Johnston to review the meeting governance guidelines which were included in the advance materials package.

Meeting Highlights

1. The RSTC voted to disband the Security and Reliability Training Working Group and the Geomagnetic Disturbance Task Force.
2. The RSTC approved scope documents for the Performance Analysis Subcommittee, Event Analysis Subcommittee and the Security Working Group.
3. The RSTC approved the scope and work plan of the Energy Reliability Assessment Task Force (ERATF).
4. The RSTC approved the RSTC Work Plan.
5. The RSTC Endorsed the *Special Assessment: NERC Energy Management System Performance Special Assessment (2018–2019)*.
6. The RSTC approved the *White Paper: Possible Misunderstandings of the Term "Load Loss"*.
7. The RSTC endorsed the Standing Committees Coordinating Group (SCCG) Scope.
8. The RSTC Approved the *Reliability Guideline: Model Verification of Aggregate DER Models used in Planning Studies* and the *Battery Energy Storage Systems (BESS) and Hybrid Power Plant Modeling and Performance Guideline.*

Consent Agenda

Chair Ford reviewed the Consent Agenda and asked RSTC members if they concurred with the items on it. Brian Evans Mongeon made a motion to approve the consent agenda. Upon motion duly made and seconded, the Committee approved the Consent Agenda.

Regular Agenda

Remarks and Reports

Chair Ford welcomed Jim Piro, NERC Board of Trustees, who has been assigned by Board Chair DeFontes, to act as the Board liaison to the RSTC and opened the floor for remarks from Trustee Piro.

Trustee Piro expressed his appreciation to RSTC leadership (Chair Ford and Vice Chair Zwergel) and thanked the RSTC on its work to improve efficiency and effectiveness of the RSTC. He noted that the Committee's future work should continue to focus on coordination with the RISC and addressing emerging risk issues like resource adequacy, wildfires, and changing resource mix.

Mark Lauby expressed his appreciation of the work of Tina Buzzard and Dan Hazelwood in making these virtual RSTC meetings successful. In addition, Mr. Lauby noted that the transforming grid is making us use new tools and all of the NERC standing committees are critical in ensuring the reliability, resilience and security of the bulk power system.

Chair Ford referenced the subgroup reports contained in the Agenda package and thanked the Sponsors for reports being submitted in the requested format. In addition, Chair Ford noted his appointment of Julia Matevosyan for IRPWG Vice Chair and advised that the RSTC Executive Committee voted on January 25, 2021 to have Chris Shepherd as the Sponsor for SCWG.

Lastly, Chair Ford provided highlights from the February 2021 Member Representatives Committee and Board of Trustees meetings.

Security and Reliability Training Working Group (SRTWG) Disposition
Motion was made to approve the disposition of the SRTWG. Vice Chair Zwergel provided background on the SRTWG and reviewed the recommendation for disposition of the working group. Comments were received that the SRTWG leadership and members were put in a tricky situation with the transition from the three standing committees to the RSTC and the SRTWG completed good works products including during the pandemic and recognition was given to the leadership of Erik Johnson and Neil Lundgren, in coordinating the SRTWG's efforts. Upon motion duly made and seconded, the Committee approved the disposition of the SRTWG.

Agenda Items 5-9
Chair Ford noted that four scope documents will be presented for approval plus the ERATF work plan and the overall work plan for the RSTC. With respect to these items, he updated the Committee that there were minor revisions to the PAS and EAS Scope, more significant revisions to the SWG scope and the ERATF is a new subgroup.

Performance Analysis Subcommittee (PAS) Scope
Motion was made to approve the PAS scope. Chair Brantley Tillis stated that a redline copy of the scope was included in the advance materials noting that most of the revisions reflect working with the RSTC rather than the PC and industry interaction. There were no significant changes to the scope. There was a brief discussion by RSTC members regarding the work of the Reliability Assessments Subcommittee and Performance Assessment Subcommittee diverging. It was suggested that we continue to coordinate with subgroups and get forward looking and backward looking groups closer together. Upon motion duly made and seconded, the Committee approved the PAS scope.

Event Analysis Subcommittee (EAS) Scope

Motion was made to approve the EAS scope. Chair Vinit Gupta stated that a redline copy of the scope was included in the advance materials and noting that there were minor revisions to the scope relating to RSTC transition planning activities, sponsors and Reliability Guidelines, and other documents to be submitted to the RSTC for approval. Upon motion duly made and seconded, the Committee approved the EAS scope.

Security Working Group (SWG) Draft Scope

Motion was made to approve the SWG draft scope. Chair Brent Sessions noted that the scope was developed in conjunction with SITES scope to be collaborative and avoid duplication, and that the SWG will develop a portfolio of technical expertise from industry and other willing participants who will conduct the activities as detailed in the draft scope included in the advance materials package. Upon motion duly made and seconded, the Committee approved the SWG scope.

Energy Reliability Assessment Task Force (ERATF) Scope and Work Plan

Motion was made to approve the ERATF scope and work plan. Peter Brandien reviewed that at the December, 2020 RSTC meeting, information was presented regarding the NERC/IRC Whitepaper on Ensuring Energy Adequacy which made a number of recommendations for mitigating risks to energy adequacy. The ERATF was formed to provide oversight and address the eleven issues identified in the report. Mr. Brandien provided an overview of the proposed scope and work plan, which were included in the advance materials package. Upon motion duly made and seconded, the Committee approved the ERATF scope and work plan. At the conclusion of the vote, Chair Ford appointed Pete Brandien as the ERATF Chair.

RSTC Work Plan

Motion was made to approve the RSTC work plan. Vice Chair Zwergel provided background on the development of the work plan and highlighted anticipated items for action between meetings as well as items for the June 2021 RSTC meeting. Several RSTC members noted that the work plan included in the agenda package should be modified to facilitate review. It was noted that the full work plan would be updated and posted in Excel on the RSTC webpage on a monthly basis allowing member and industry to easily review the work plan on an ongoing basis. In addition it was requested that a column be added to identify a target meeting date for deliverables. Upon motion duly made and seconded, the Committee approved the RSTC work plan.

Special Assessment: NERC Energy Management System Performance Special Assessment

Motion was made to endorse the Special Assessment: NERC Energy Management System Performance Special Assessment. EMSWG Chair Phil Hoffer stated that this document includes assessments for three factors (outage duration, EMS functions, and entity reliability functions), examining associated trends, event root causes, and contributing causes identified through the ERO Cause Code Assignment Process (CCAP) for the 2018–2019 period. In addition, Chair Hoffer presented on the key findings and recommendations from the assessment. It was noted that the recommendations are for both the ERO and industry. The EMWSG will clarify this in the report. NERC will publish the report, socialize the findings and recommendations with industry and post to the NERC website with notice to industry. Upon motion duly made and seconded, the Committee endorsed the Special Assessment: NERC Energy Management System Performance Special Assessment.

Geomagnetic Disturbance Research Work Plan Results and Recommendations

Motion was made to approve to disband the GMDTF. GMDTF Chair Emanuel Bernabeu stated The GMD Task Force (GMDTF) has supported NERC in establishing its GMD mitigation strategy and that its scope was updated in December 2016 to support NERC in meeting obligations of FERC Order No. 830. Chair Bernabeau than presented on the research results summary and the ERO recommendations noting that the two-year research effort with Electric Power Research Institute (EPRI) concluded in 2020, which promotes further knowledge of severe GMD event impacts and addresses FERC directives for research, that over 17 publications were produced, and the final EPRI white paper was published in August 2020. He further stated that the GMDTF has reviewed deliverables throughout the project, all EPRI reports and tools in this project are available to the public at no charge, and that NERC must file research results with FERC. Chair Bernabeau requested that the RSTC disband the GMDTF per the organizational structure and include GMD monitoring in the Real-time Operations Subcommittee (RTOS) scope. Mark Olson, NERC Staff, stated he will coordinate with the RTOS to assume the GMD monitoring activities. Upon motion duly made and seconded, the Committee approved to disband the GMDTF.

Data Collections Technical Reference Document | Approaches for Probabilistic Assessments and 2020 Probabilistic Assessment | Regional Risk Scenario Sensitivity Case Report

PAWG Chair Andreas Klaube provided an overview of the Data Collections Technical Reference document and the Regional Risk Scenario Sensitivity Case Report that were included in the advance materials package. Chair Klaube stated that the PAWG is seeking RSTC reviewers to review the two documents and provide feedback to the PAWG/RAS. Chair Ford opened to the Committee for volunteers and/or for members to send an email to Secretary Crutchfield and Secretary Crutchfield will coordinate the review process. RSTC members Carl Turner, Brian Evans-Mongeon, David Jacobson, Wayne Guttormson, David Mulcahy, and Robert Reinmuller offered to participate in the reviews.

Chair’s Closing Remarks and Adjournment

Chair Ford thank the members of the Committee for their support in the approval of the items on the day’s agenda and appreciated the good discussion. He called on Trustee Piro for any closing remarks, Trustee Piro thanked everyone and thought it was a good and productive meeting, all discussions were well done. Mr. Lauby noted that this was an informative meeting and he is very appreciative of the progress of both the RSTC and the GMDTF. There being no further business brought before the Committee the meeting was adjourned at 4:27 p.m. Eastern.

Wednesday, March 3, 2021

Chair Ford called the meeting to order, and thanked everyone for attending. Tina Buzzard reviewed the procedures for the meeting, reviewed the Antitrust Compliance Guidelines, and confirmed quorum, as well as provided an overview of the polling actions to be used for Committee actions during the meeting.

Introductions and Chair's Remarks

Chair Ford provided an overview of the agenda noting that due to the number of action items before the Committee it may be necessary to defer some non-action topics to the next meeting.

White Paper: Possible Misunderstandings of the Term "Load Loss"

Motion was made to approve the White Paper: Possible Misunderstandings of the Term "Load Loss". John Skeath presented that the System Analysis and Modeling Subcommittee developed a White Paper to address possible misunderstandings of the Term "Load Loss". The subcommittee received input from the Operating and Planning Committees and also requested input from RSTC members in October. The comments received have been addressed by an ad hoc team and conforming revisions made to the white paper. Some RSTC members expressed concerns regarding the priority of this White Paper and whether or not it addresses any reliability concerns. In response, Mr. Skeath provided an example of a scenario where a customer would transfer to another resource while the host utility would maintain voltage per TPL standard resulting in an extensive action plan. Upon motion duly made and seconded, the Committee approved the White Paper: Possible Misunderstandings of the Term "Load Loss".

Standing Committees Coordinating Group (SCCG) Scope

Chair Ford noted that the action for this item was listed incorrectly the item should be an acceptance item and not an endorsement. Motion was made to accept the Standing Committees Coordinating Group (SCCG) Scope. Vice Chair Zwergel provided an overview of the SCCG scope which was included in the advance materials package. He reviewed the group membership and noted that the SCCG has been in existence for a number of years as an informal means for the standing committees, reporting to the Board of Trustees, to coordinate their work plans and the SCCG is now seeking to formalize their scope and activities. Upon motion duly made and seconded, the Committee accepted the SCCG scope.

Reliability Guideline Metrics

Candice Castaneda, NERC Legal, provided a brief overview of Federal Energy Regulatory Commission approved process to review the effectiveness and efficiency of Reliability Guidelines as described in the agenda package. It was agreed that apart from the process to review Reliability Guidelines on a triennial basis and include metrics, the RSTC would assemble a team of RSTC members to define Reliability Guideline, Reference Document, Technical Reference Document, White Paper, etc. for further RSTC action/consideration. Chair Ford requested that anyone interested in participating in this effort should send an email to Secretary Crutchfield.

Reliability Guideline: Model Verification of Aggregate DER Models used in Planning Studies

Motion was made to approve the Reliability Guideline: Model Verification of Aggregate DER Models used in Planning Studies. SPIDERWG Chair Kun Zhu reviewed the focus of the guideline as well as its development process noting the SPIDERWG has responded to comments and made conforming revisions to the Guideline. After a brief discussion on metrics, upon motion duly made and seconded, the Committee approved the Reliability Guideline: Model Verification of Aggregate DER Models used in Planning Studies.

Battery Energy Storage Systems (BESS) and Hybrid Power Plant Modeling and Performance Guideline
Motion was made to approve the Battery Energy Storage Systems (BESS) and Hybrid Power Plant Modeling and Performance Guideline. IRPWG Vice Chair Julia Matevosyan reviewed the guideline and its development. Several RSTC members commented that the guideline is a very good document and they thanked the IRPWG for the excellent work. Upon motion duly made and seconded, the Committee approved the Battery Energy Storage Systems (BESS) and Hybrid Power Plant Modeling and Performance Guideline.

Standards Authorization Request (SAR) to revise TPL-001-5.1
Motion was made to endorse the Standards Authorization Request (SAR) to revise TPL-001-5.1. SPIDERWG Chair Zhu provided a summary of the SAR noting that considering current trends, the NERC SPIDERWG and NERC Inverter-Based Resource Performance Working Group (IRPWG) independently undertook a review of the TPL-001 standard for considering DERs and BPS-connected IBRs, respectively. These reviews are captured in the following RSTC-approved white papers:

SPIDERWG: Assessment of DER impacts on NERC Reliability Standard TPL-001 (here)

IRPTF/IRPWG: IRPTF Review of NERC Reliability Standards – March 2020 (here)

In addition, Mr. Zhu stated that the This SAR proposes to update TPL-001-5.1 to address the issues identified in both white papers. Several RSTC members expressed concerns about the SAR and thought that it was not ready for Standards Committee action. Mr. Zhu noted that the SAR would go through a comment period under the Standards Development Process. Upon motion duly made and seconded the motion did not meet the required passing rate and the motion failed. Chair Ford requested the Committee send their comments, concerns, recommended revisions on the SAR to Secretary Crutchfield and Jody Green for review by the SPIDERWG to allow resubmission to the RSTC at a future meeting.

Wildfire Mitigation Reference Guide
Al McMeekin, NERC Staff presented on the Wildfire Mitigation Reference Guide noting NERC and WECC developed this document with the goal of creating more awareness across all Interconnections of the knowledge and experience gained by western utilities on wildfire preparedness and mitigation. Research and development efforts by the Department of Energy (DOE) National Laboratories in partnership with electric utilities and other stakeholders on many facets of wildfire mitigation, situational awareness, and pre- and post-fire analyses are also highlighted in the document. In addition, the Reference Guide contains an extensive list of supplemental reference material.

Supply Chain Compromise Presentation
Jeff Jones, E-ISAC Staff, presented on the recent supply chain compromise and cyber threats to include a SolarWinds Resources, RDDoS & Ransomware, Ransomware Data Leaks and Florida Water Plant Incident

updates noting that security issues with a significant impact on critical infrastructures are unfortunately becoming more common.

Forum and Group Reports

NAGF
Allen Schriver provided an update on NAGF activities to include the NAGF Annual Meeting, NERC standards projects the NAGF is actively engaged in, collaboration efforts with the NATF and an update on the NAGF website redesign. In addition, he also noted that this is an appropriate time to stand up the ERATF and requested RSTC members to send him any suggestions for ways to enhance collaboration with the NAGF and industry to improve operations during extreme weather events.

NATF
Roman Carter provided an update on NATF activities to include its work on the response to COVID-19 challenges, conducting the well-attended webinar on the NERC Alert Regarding Supply Chain Compromises by Advanced Persistent Threat Actor, coordination with its members regarding the "Prohibition Order Securing Critical Defense Facilities" issued by U.S. Secretary of Energy Dan Brouillette on December 17, 2020, collaboration leadership meetings with NERC to discuss work and industry topics, and its efforts with respect to facility ratings and supply chain.

RSTC 2021 Calendar Review/Chair's Closing Remarks and Adjournment
Chair Ford referenced the future meeting schedule in the advance materials package stating that the September meeting will be fully virtual and the December meeting is still to be determined. He thanked all participants and expressed his appreciation to the Committee for their efforts, comments, and technical discussions over the past two days.

Chair Ford called on Trustee Piro for any closing comments. Trustee Piro noted the excellent work on two Reliability Guidelines and applauds the discussion on how to get Reliability Guidelines socialized with industry. He noted the Board's particular interest in the ERATF. Their work items (EA, gas delivery security, metrics and analysis) are important to the Board as the grid continues to change and the effort in determining how to handle the emerging risks, expressing the last presentation on the cyber events is really important.

There being no further business before the RSTC, Chair Ford adjourned the meeting on Wednesday, March 3, 2021 at 4:05 p.m. Eastern.

Stephen Crutchfield
Stephen Crutchfield
Secretary

RSTC Status Report – Security Working Group (SWG)

Chair: Brent Sessions
Vice-Chair: Katherine Street
June XX, 2021

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: Provides a formal input process to enhance collaboration between the ERO and industry with an ongoing working group. Provides technical expertise and feedback to the ERO with security compliance-related products.

Items for RSTC Approval/Discussion:

- **Approve**:
- Assessing and Reducing Risks Tool (Guideline)
- Final version of Encryption in the Cloud paper (Implementation Guideline)

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Update "Assess and Reducing Risks Tool" based on industry feedback	🟢	Ready for RSTC approval
Complete Encryption in the Cloud Compliance Implementation	🟢	Ready for RSTC approval
BCSI in the Cloud Tabletop Lessons Learned	🟢	Due Q2, 2021 for 1st RSTC review

Recent Activity

- Assessing and Reducing Risks Tool ready for RSTC Approval
- Encryption in the Cloud Compliance Implementation. Paper ready for RSTC Approval
  - Metrics survey
- BCSI in the Cloud tabletop lessons learned in SWG review – moving due date back due to review process with all stakeholders
- ERC Lessons Learned team formed
- SWG Co-Chair approved

Upcoming Activity

- Complete BCSI in the Cloud tabletop lessons learned
- CIP ERT commenting process
- SWG process/procedures
- External website set-up
- SITES requests process being developed
- Participation in SITES BES Operations in the Cloud groups

RSTC Status Report – Energy Reliability Assessment Task Force (ERATF)

Chair: Peter Brandien
June 8-9, 2021

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: The ERATF is tasked with assessing risks associated with unassured energy supplies stemming from the variability and uncertainty from renewable energy resources, limitations of the natural gas system and transportation procurement agreements, and other energy-limitations that inherently exist in the future resource mix.

Recent Activity:

- Reviewed the white paper, scope and work plan.
- Developed a Resource Map of RSTC subcommittees and working groups to assist in addressing the Focus Areas.
- Developed common worksheets to manage deliverables.
- Coordinated with the RSTC subcommittee and working group leadership.

Items for RSTC Approval/Discussion:

- **Discussion**: Update the RSTC on the coordination activities between the ERATF and RSTC subcommittees and working groups.

Upcoming Activity:

- Industry coordination on energy assessments, metrics, analysis, and unique considerations based on geography.
- Assist the RSTC subcommittee and working groups on their work plans and completion of the ERATF worksheets that facilitate coordination.

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Assemble the subject matter experts for Focus Areas.	🟡	On track.
The subject matter experts complete the deliverables as outlined in the work plan.	🟢	On track.
Engage industry research and development organizations to validate work from Focus Areas	🟢	On track.

RSTC Status Report – Event Analysis Subcommittee (EAS)

Chair: Vinit Gupta
Vice-Chair: Ralph Rufrano
June 7,2021

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: The EAS will support and maintain a cohesive and coordinated event analysis (EA) process across North America with industry stakeholders. EAS will develop lessons learned, promote industry-wide sharing of event causal factors and assist NERC in implementation of related initiatives to lessen reliability risks to the Bulk Electric System.

Recent Activity

- The EAS has published 4 new lesson learned since the December 2020 RSTC meeting.
- Webinar for the NERC EMS Performance Special Assessment was conducted April 28th.

Items for RSTC Approval/Discussion:

- None at this time.

Upcoming Activity

- Development of Lessons Learned
- 9th annual Monitoring and Situational Awareness Technical Conference.

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Pandemic Response lessons learned	🟢	EAS is coordinating development with RTOS .
EA Chapter of 2021 SOR	🟢	Coordinating development with PAS
EAS Scope Document	🟢	Approved March 2,2021
Events Analysis Process Review	🟢	On going.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Lessons Learned Summary

Rick Hackman, NERC
Update for May 6, 2021

NERC Lessons Learned Webpage

RELIABILITY | RESILIENCE | SECURITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Category of Lessons Learned Published to Date

- **8 NERC Lessons Learned published to date in 2021**
  - 2 - General Processes
  - 2 - Relaying and Protection Systems
  - 2 - Transmission Facilities
  - 2 - Bulk Power System Operations

- **11 NERC Lessons Learned were published in 2020**
  - 2 - Transmission Facilities
  - 3 - Relaying and Protection Systems
  - 2 - Relaying and Protection Systems, and Transmission Facilities
  - 2 – Communications
  - 2 - Bulk Power System Operations

Lessons Learned Submitted to NERC being currently worked

ERO Team*	1
MRO	0
NERC	0
NPCC	2
RF	0
SERC	0
TRE	0
WECC	0

*"ERO Team" means multiple Regions contributed

NPCC – "Salt Contaminated Bushings"

References to prior bushing coating LL and related issues will go into an attachment.

NPCC – "Multiple Faults in Rapid Succession Contribute to Relay Misoperations"

This is a 2nd LL from the event that gave us "Salt Contaminated Bushings"

The Review Team met on 5/4, and are choosing their next time

ERO Team – "Pandemic Response"

The Review Team met on 4/21 & 4/22 (in 2 groups). Their next meeting will be May 18.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lessons Learned Submitted to NERC still needing info

Lessons Learned ideas submitted to NERC for review, consideration and development of potential lessons learned waiting for draft or initial review of draft.

ERO Team*	**0**
MRO	**0**
NERC	**0**
NPCC	**0**
RF	**1**
SERC	**0**
TRE	**0**
WECC	**1**

***"ERO Team" means multiple Regions contributed**

WECC – "Islanding involving high amount of wind penetration and UFLS usage"

Needs a draft.

RF – "Questioning Attitude / Security Event"

Needs a draft.

Lessons Learned Metrics

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Total
ERO Team*	0	0	0	0	0	0	0	0	0	2	1	0	3
MRO	0	2	2	0	3	1	2	0	3	0	4	0	17
NERC	23	1	0	0	1	0	0	1	0	0	1	3	30
NPCC	0	5	2	5	4	10	6	2	4	3	2	3	46
RF	0	3	1	3	4	1	1	1	5	2	1	0	22
SERC	0	1	0	2	4	2	2	0	0	1	0	0	12
TRE	0	5	8	1	2	1	1	2	0	0	0	0	20
WECC	0	5	5	3	1	1	1	3	3	3	2	2	29
Total	23	22	18	14	19	16	13	9	15	11	11	8	179

***"ERO Team" means multiple Regions contributed**

NERC Lessons Learned Webpage

RSTC Status Report – System Protection and Control Working Group (SPCWG)

Chair: Jeff Iler
Vice-Chair: Bill Crossland
June 8,2021

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: The SPCWG will promote the reliable and efficient operation of the North American power system through technical excellence in protection and control system design, coordination, and practices.

Items for RSTC Approval/Discussion:

- **Approval**: SPCWG Scope Document
- **Approval**: To add Inter-Entity Short Circuit Model Outline to 2021 SPCWG work plan

Recent Activity

- Developing PRC-024-3 CIG
- Developing PRC-019-2 CIG
- IBR Impact on BPS Protection Technical Report

Upcoming Activity

- Developing 2021 Work plan
- Review roster to identify sector representatives, members, observers and verify contact information

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Revising Scope Document	🟢	On schedule
Developing 2021 Work plan	🟢	On schedule
Developing PRC-024-3 SAR	🟢	On schedule
Developing PRC- 019-2 CIG	🟢	On schedule

RSTC Status Report – Inverter-based resource Performance Working Group (IRPWG)

Chair: Al Schriver
Vice-Chair: Julia Matevosyan

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: To *explore the performance characteristics of utility-scale inverter-based resources (e.g., solar photovoltaic (PV) and wind power resources) directly connected to the bulk power system (BPS).*

Items for RSTC Approval/Discussion:

- **Approve:** San Fernando Disturbance Follow-Up White
- **Approve**: - TPL-001-5 SAR for BPS-Connected IBRs
- **Approve:** White Paper: BPS-Connected IBR and Hybrid Plant Capabilities

Recent Activity

- Reviewed latest draft white paper for Using BPS-Connected Inverter-Based Resources and Hybrid Plant Capabilities for Frequency Response
- Discussed latest draft of guideline: Reliability Guideline: EMT Modeling and Studies
- Developing Team for Reliability Guideline: Recommended Approach to Interconnection Studies for BPS-Connected Inverter-Based Resources

Upcoming Activity

- *White Paper: BPS-Connected IBR and Hybrid Plant Capabilities for Frequency Response* – Plan to request acceptance to post for 45 day comment period at third quarter RSTC meeting.

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Reliability Guideline: EMT Modeling and Studies	🟢	In progress
White Paper: BPS-Connected IBR and Hybrid Plant Capabilities for Frequency Response	🟢	In progress
White Paper: San Fernando Disturbance Follow-Up	🟢	In Progress
Reliability Guideline: Recommended Approach to Interconnection Studies for BPS-Connected Inverter-Based Resources	🟢	Team being developed

RSTC Status Report – Load Modeling Working Group (LMWG)

Chair: Kannan Sreenivasachar,
Vice-Chair:

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose:
The LMWG is transitioning utilities from the CLOD model to the CMLD Composite Load Model. The CLOD model lacks the capability to model events like FIDVR, which can have significant consequences on planning decisions.

Items for RSTC Approval/Discussion:

- **Approve**: LMWG *Work Plan*

Recent Activity

- Completed CMLD Phased Field Tests
- Update to Motor D base parameters
- EPRI initial test results on AC phasor model in PSLF

Upcoming Activity

- *CMLD Field Test Survey Summary*
- *CMLD Field Test Report*
- *Transient Voltage Response Whitepaper*
- *On-going testing by entities with updated Motor D parameters*

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Industry outreach - working with NERC MMWG on data management processes	🟢	In progress
Field Test survey Summary	🟢	In progress
Field Test Report	🟢	In progress
Transient Voltage Response Whitepaper	🟢	In progress

RSTC Status Report–Power Plant Model Verification Task Force (PPMVTF)

Chair: Shawn Patterson
June 8, 2021

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: PPMVTF develops technical guidance material related to power plant modeling, power plant model verification (PPMV), and generator testing procedures used for developing and certifying the simulation models used to reliably plan and operate the bulk power system (BPS).

Items for RSTC Approval/Discussion:

- **Approve or Accept to post for 45 day Comment period**: Reliability Guideline: MOD-032 guideline

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
MOD-032 Guideline Approval	🟢	

Recent Activity

- Preparing the MOD-32 guideline for RSTC Approval.

Upcoming Activity

- Review comments on the posted guideline.

RSTC Status Report – Reliability Assessments Subcommittee (RAS)

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Chair: Lewis De La Rosa (12/2019)
Vice-Chair: Anna Lafoyiannis (12/2019)
June 8, 2021

Purpose: The RAS reviews, assesses, and reports on the overall reliability (adequacy and security) of the BPS, both existing and as planned. Reliability assessment program is governed by NERC RoP Section 800.

Items for RSTC Approval/Discussion:

- 2021 SRA Report is under RSTC review until May 14.

Recent Activity

- RAS Meeting April 13-14: topics included updates from the Energy Assurance Task Force; discussion of findings for SRA; and planning for the 2021 LTRA and 2021-2022 WRA
- Endorsed *ProbA Regional Risk Scenarios Report* and *Data Collection Technical Reference Document* prepared by PAWG.

Upcoming Activity

- 2021 SRA Report planned publication is at the end of May.
- 2021 LTRA responses due back in June. RSTC Review planned for September 2021.
- 2021-2022 WRA input request will be sent to the regions in August.

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
2021 Summer Reliability Assessment	🟢	RSTC review ends May 14.
2021 Long-term Reliability Assessment	🟢	Assessment area information request responses received back in June.
2021-2022 Winter Reliability Assessment	🟢	Assessment area information request will be sent out to the regions in August.

RSTC Status Report – Resources Subcommittee (RS)

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Chair: Greg Park
Vice-Chair: Rodney O'Bryant
June 08, 2021

Purpose: The RS assists the NERC RSTC in enhancing Bulk Electric System reliability by implementing the goals and objectives of the RSTC Strategic Plan with respect to issues in the areas of balancing resources and demand, interconnection frequency, and control performance.

Recent Activity

- Review FRS Form 1 and Form 2 prior to OY2020 end of year posting deadline
- Continue to work on items to sunset the Inadvertent Interchange Working Group
- Quarterly review of interconnection performance
- EI High Frequency Webinar

Items for RSTC Approval/Discussion:

- **Approve**:
  - Balancing and Frequency Control Reference Document
  - ACE Diversity Interchange Guideline
  - Operating Reserve Management Guideline
- **Accept for 45 day Comment**:
  - Inadvertent Interchange Reliability Guideline

Upcoming Activity

- Begin engaging the Energy Reliability Task Force workplan

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Review and approval of the Annual Frequency Response Analysis	🟢	On Track
ACE Definition SAR	🟢	Due to delay, RS will bring SAR forward in October for RSTC review
RS M6 outreach to BAs indicating a year over year decline in performance.	🟢	RS leadership and regional representatives will be meeting with identified BAs during the upcoming quarter

RSTC Status Report – Performance Analysis Subcommittee (PAS)

Chair: Brantley Tillis
Vice-Chair: David Penney
September 16, 2020

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed
○ Not started

Purpose: The PAS reviews, assesses, and reports on reliability of the North American Bulk Power System (BPS) based on historic performance, risk and measures of resilience.

Items for RSTC Approval/Discussion:

- **Endorse**: State of Reliability Report
- **Approve:** Posting for public comment Generating Availability Data System (GADS) Data Request for Utility-Scale Solar Plants and Updates for GADS Wind and Conventional GADS

Recent Activity

- March:
  - RSTC: Approved the revised PAS scope
  - PAS: SOR kick off
- April:
  - PAS Endorsement of GADS Section 1600 Data Request
- May:
  - SOR preview to NERC Board

Upcoming Activity

- RSTC
  - June 22: Request for comments due on the SOR
  - June 30: Disposition of RSTC SOR comments webinar at 1 p.m. ET
  - July 7: Email SOR report accompanied with Email ballot for endorsement by the RSTC
- July 17: Electronic Voting Deadline for Report Endorsement by the RSTC

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
2021 State of Reliability Report	🟢	May – SOR in review
Section 1600 Data Request	🟢	NERC RoP GADS Section 1600 Data Reporting to collect and analyze conventional, wind and solar data.
Conduct annual metric review	○	2H 2021
Review proposed new metrics	○	2H 2021

RSTC Status Report – Supply Chain Working Group (SCWG)

Chair: Tony Eddleman | May 14, 2021
Vice-Chair: Charles Abell
Secretary: Tom Hofstetter
RSTC Sponsor: Chris Shepherd

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: Enhancing Bulk Electric System (BES) reliability by implementing the goals and objectives of the RSTC Strategic Plan with respect to issues in the area of supply chain risk management.

Recent Activity

- Met virtually on March 15th, April 19th and May 17th
- Working on a Supply Chain Standard Effectiveness Survey with NERC to be issued in the Fall of 2021
    - Voluntary survey to industry
    - NERC to use the results to brief the Board on the Supply Chain Standards
- Discussing the rapidly changing supply chain environment

Items for RSTC Approval/Discussion:

- **None**

Upcoming Activity

- Guidance documentation on supply chain risk management issues and topics
    - Monitoring FERC, Executive Orders, DOE, and CISA for future directions
- Input and feedback associated with the development of supply chain documents to NERC staff
    - Provide Supply Chain Standard Effectiveness Survey to NERC
    - Monitor NIC Controller pilot project
- Monitor Software Bill of Materials (SBoM) Project by NTIA

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Guidance documentation on supply chain risk management issues and topics	🟢	In progress
Input and feedback associated with the development of supply chain documents to NERC staff	🟢	In progress

RSTC Status Report – Probabilistic Assessment Working Group (PAWG)

Chair: Andreas Klaube
Vice-Chair: Alex Crawford
June 9, 2021

🟢	On Track
🟡	Schedule at risk
🔴	Milestone delayed

Purpose: *The primary function of the NERC Probabilistic Assessment Working Group (PAWG) is to advance and continually improve the probabilistic components of the resource adequacy work of the ERO Enterprise in assessing the reliability of the North American Bulk Power System.*

Items for RSTC Approval/Discussion:

- **Approval**: *Data Collection Approaches for Probabilistic Assessments Technical Reference Document*
- **Approval**: *2020 Probabilistic Assessment Scenario Case*

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
2021 NERC Probabilistic Analysis Forum	🟢	In progress, planned Q2 2021 announcement. Holding forum in October 2021

Recent Activity

- Presented draft of 2020 Probabilistic Assessment Scenario Case for RAS review.
- Continued planning of 2021 Probabilistic Analysis Forum
- Beginning scoping for request to work on new work documents
- Ongoing engagement with RAS with probabilistic components of their seasonal assessments.

Upcoming Activity

- *2021 Probabilistic Analysis Forum–* Plan to hold forum in October 2021

RSTC Status Report – System Planning Impacts from DER Working Group (SPIDERWG)

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Chair: Kun Zhu
Vice-Chair: Bill Quaintance
June 9, 2021

Purpose: *The NERC Planning Committee (PC) identified key points of interest that should be addressed related to a growing penetration of distributed energy resources (DER). The purpose of the System Planning Impacts from Distributed Energy Resources)SPIDERWG) is to address aspects of these key points of interest related to system planning, modeling, and reliability impacts to the Bulk Power System (BPS). This effort builds off of the work accomplished by the NERC Distributed Energy Resources Task Force (DERTF) and the NERC Essential Reliability Services Task Force/Working Group (ERSTF/ERSWG), and addresses some of the key goals in the ERO Enterprise Operating Plan.*

Recent Activity

- Met in April 2021 to update work products and refocus on high priority items.
- Beginning engagement on software vendors to enhance sub-group work products.
- Determined path forward to respond and enhance standard related efforts.

Items for RSTC Approval/Discussion:

- **Approval**: *DER Modeling Survey (Includes informative presentation)*
- **Accept to post**: *Reliability Guideline: Recommended Approaches for UFLS Program Design with Increasing Penetrations of DERs.*

Upcoming Activity

- *Many deliverables targeted for RSTC action in Q3 and Q4 of 2021. Currently consisting of:*
    - *Five White Papers for review/ approval*
    - *Two Reliability Guidelines to request posting for industry comment periods*
    - *One Reliability Guideline (UFLS) requesting approval*

Workplan Status *(6 month look-ahead)*

See next slide

Work Look Ahead

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Workplan Status (6 month look-ahead)

Milestone	Status	Comments
C6 – NERC Reliability Standards Review	🔴	Initial draft completed. Responding to various SPDIERWG reviews. Requesting RSTC review later in 2021.
O1 – White Paper FERC Order 2222 and BPS Reliability Perspectives	🟢	Initial draft of white paper complete and reviewing drafts. Lead author change.
S1 – Reliability Guideline: Bulk Power system Planning under Increasing Penetration of Distributed Energy Resources	🟢	Nearing completion of initial draft. Targeting RSTC request to post in Q4 2021.
V2 - Reliability Guideline: DER Forecasting Practices and Relationship to DER Modeling for Reliability Studies	🟢	Initial draft in review by SPIDERWG. Targeting RSTC request to post for industry comment in Q3 2021
S2a – SAR: Updates to TPL-001 Regrading DER Considerations	🟢	Targeting RSTC Q3 2021 for turnaround.
S3 – Recommended Simulation Improvements and Techniques	🟢	Beginning software vendor engagement.
S4b – Whitepaper: DER impacts to UVLS Programs	🟢	Initial draft underway.
S5 – Whitepaper: Beyond Positive Sequence RMS Simulations for High DER Penetration Conditions	🟢	Initial draft nearing completion. Targeting RSTC request for review in Q3 2021.

RSTC Status Report – Real Time Operating Subcommittee (RTOS)

Chair: Chris Pilong
Vice-Chair: Jimmy Hartmann
June 8-9, 2021

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: The RTOS assists in enhancing BES reliability by providing operational guidance to industry; oversight to the management of NERC-sponsored IT tools and services which support operational coordination, and providing technical support and advice as requested.

Items for RSTC Approval/Discussion:

- Reliability Guideline Gas and Electrical Operational Coordination Considerations

Recent Activity

- *Endorsed changes to the FRCC, SPP, SERC and PJM Reliability Plans:*
- Task Force developed to review GMD and Time Error Monitor procedures Q4 2020

Upcoming Activity

- Reliability Coordinator Plan Reference Document Q4 2021
- Reliability Guideline for Cyber Intrusion for System Operators Q4 2021

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Monitor development of common tools and act as point of contact for EIDSN.	🟢	In Progress
Frequency Monitor Reporting (Standing RTOS agenda item to discuss).	🟢	In Progress
Reliability Guideline: Cyber Intrusion Guide for System Operators (Approved by the Operating Committee on June 5, 2018)	🟢	In Progress
Reliability Coordinator Plan Reference Document	🟢	In Progress

RSTC Status Report – Security Integration & Technology Enablement Subcommittee (SITES)

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Chair: David Zwergel
Vice-Chair: Benny Naas | June 2021

Purpose: *To identify, assess, recommend, and support the integration of technologies on the Bulk Power System (BPS) in a secure, reliable, and effective manner.*

Items for RSTC Approval/Discussion:

- **Accept**: *None*
- **Approve**: *None*

Note: SITES has recommended a new subcommittee Chair for RSTC Chair approval

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
BES Operations in the Cloud	🟢	In progress Q4/2021
Zero-Trust Concepts	🟢	In progress Q4/2021
Security Integration	🟢	Planning phase Q1/2022
IT/OT Convergence	🟢	Planning phase Q1/2022
Reliability/Resilience/Security balance	🟢	Planning phase Q1/2022
Emerging Technologies	🟢	Planning phase Q1/2022
Risk Identification	🟢	Planning phase Q1/2022
Security Implementation	🟢	Planning phase Q1/2022

Recent Activity

- BES operations in the cloud whitepaper: Subgroup has been formed and initial working draft has been developed.
- Zero-trust whitepaper: Subgroup has been formed.

Upcoming Activity

- BES operations in the cloud whitepaper public comment period. Date TBD.
- Zero-trust whitepaper initial draft and prep for public comment period. Date TBD.

Agenda Item 5a
Reliability and Security
Technical Committee Meeting
June 8, 2021

Reference Document Review:
ACE Diversity Interchange Process Guideline

Action

Approve

Purpose

This Reliability Guideline, "ACE Diversity Interchange (ADI) Process Guideline" is up for the periodic 3-year review by the NERC Resources Subcommittee (RS). This document is intended as a tutorial for those new to ACE Diversity Interchange Process or as a reference for those consider implementing ADI.

Background

The RS drafted this Reliability Guideline at the request of the former NERC Operating Committee as part of a series on operating and planning reliability concepts. The document covers ACE Diversity Interchange Process concepts, issues, and recommendations with the goal to provide an understanding of the fundamentals.

Changes to the Updated Document

A sub-team of the RS has revised the ACE Diversity Interchange Process Guideline and vetted those changes through the full subcommittee. The major changes include:

- Numerous errata edits, re-wording and organizational changes
- Preamble section: Updated Committee Structure to reflect the recently formed Reliability and Security Technical Committee (RSTC)
- End of Hour Settlements section: Moved the section to after the Within Hour Assessments (Real Time) section and removed description of different methods of ADI settlement as they are not considered reliability issues.
- Within Hour Assessments (Real Time) section: Modified verbiage to provide better clarity
- Operating Principles section:
    - OP3: Clarified that both initial implementation and any subsequent modifications need to be reviewed and approved
    - OP4 and OP5 are combined into OP4
    - OP8: modified verbiage to reflect changes in BAL-002 (BAL-002-2 version)
    - OP9: added clarifying verbiage

On October 22, 2020 the RS approved the recommendation to move this technical reference document to the RSTC for approval and posting for 45-day industry comment.

Further Changes to the Posted Document:

Following the posting for comment period, a sub team of the RS has reviewed the comments received from the industry and made these further changes to the ACE Diversity Interchange Process Guideline Document:

- Purpose section: moved entire section up to before the Background section
- ADI Implementation Mechanics section: modified language to clarify the need for direct transmission connectivity
- Within Hour Assessments (Real Time) section: added several full terminologies to clarify their abbreviations, and modified language to clarify how the ADI adjustment term can be incorporated into ACE.
- Operating Principles section:
    - OP5: modified language to clarify the need for direct transmission connectivity
    - OP7: removed a vague and seemingly redundant sentence

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Guideline

Area Control Error Diversity Interchange Process – Version 3

Applicability

Balancing Authorities (BAs)

For Information

Transmission Operators (TOPs)
Reliability Coordinators (RCs)

Preamble

It is in the public interest for the North American Electric Reliability Corporation (NERC) to develop guidelines that are useful for maintaining or enhancing the reliability of the Bulk Electric System (BES). The NERC Reliability and Security Technical Committee per its charter is authorized by the NERC Board of Trustees (Board) to develop Reliability and Security Guidelines. These guidelines establish a voluntary code of practice on a particular topic for consideration and use by BES users, owners, and operators. These guidelines are coordinated by the technical committees and include the collective experience, expertise and judgment of the industry. The objective of this reliability guideline is to distribute key best practices and information on specific issues critical to maintaining the highest levels of BES reliability. Reliability guidelines are not to be used to provide binding norms or create parameters by which compliance to standards is monitored or enforced. While the incorporation and use of guideline practices is strictly voluntary, the review, revision, and development of a program using these practices is highly encouraged to promote and achieve the highest levels of reliability for the BES.

Purpose

The purpose of this reliability guideline is to address industry practices related to the usage of ADI.

Background

Area Control Error Diversity Interchange (ADI) is a process in which participating Balancing Authorities exchange information related to their unadjusted Area Control Error (ACE) values (ACE before, or without, adjustment by the ADI process) in order to develop ADI adjustment values to their ACE. When there is a diversity of algebraic sign among ADI participants' unadjusted ACE, ADI adjustments are applied to yield ADI-adjusted ACE values that are closer to zero. Fundamentally, ADI is simply exchanging a real-time portion of one Balancing Authority's ACE for an equal but opposite portion of another Balancing Authority's ACE, thereby, reducing the ACE values of both Balancing Authorities. ADI is considered by some to be a form of supplemental regulation, and there have been several implementations since its inception in the 1990s, of which a few have been retired due to Balancing Authority consolidations. Eastern Interconnection ADI participants consider it to be supplemental regulation, while Western Interconnection ADI participants consider it to be solely an ACE exchange. Balancing Authorities participating in ADI cite the following benefits as reasons for their participation:

- Low cost and ease of implementation.
- Fewer output adjustments that reduce heat rate degradation and "wear and tear" on generating facilities.
- Reduced regulation requirements while having fewer generators operate out of economic merit order.

Relevant Definitions from the NERC Glossary

Capitalized terms in this document are defined in the *NERC Glossary of Terms Used in NERC Reliability Standards*. Note that a definition for ADI does not exist within the NERC glossary at this time but a working definition is provided in the section below, entitled Basic ADI Operating Concepts.

Basic ADI Operating Concepts

The following working definition was developed and reflects the present implementations of ADI:

- **ACE Diversity Interchange** – A frequency neutral form of ACE exchange that uses real-time, sub-minute adjustments to the unadjusted ACE values of participating Balancing Authorities that always net to zero and are non-zero individually only when at least one participating Balancing Authority's unadjusted ACE value differs in algebraic sign from at least one other participating Balancing Authority's unadjusted ACE. Participating Balancing Authorities achieve reductions in their generation control and reporting ACE values by incorporating the ADI adjustments computed by an ACE Diversity Interchange algorithm. A participating BA's ADI adjustment term for each calculating cycle allows a flow that has already occurred on the participating BA's tie-lines to be maintained.

While ADI adjustment allocation methods may differ among the ADI implementations, two key features are that the computed ADI adjustments for all participating Balancing Authorities must always have a zero sum (see OP1 below) and the computed ADI adjustment for each participating Balancing Authority will equal zero in the absence of diversity in algebraic sign of the participating Balancing Authorities' unadjusted ACE. These are distinguishing features of the ADI process.

ADI Implementation Mechanics

ADI processes depend on the timely exchange of relevant data, and consistent implementation of ADI adjustments in the same timeframe of EMS scan rates (e.g., six seconds, or less). While the information exchange processes used for ADI have very high availability, Balancing Authorities participating in ADI have backup plans to address failures in data exchange communications.

The ADI processes that exist presently allow for individual Balancing Authorities to enable or disable their participation in real-time for local or interconnected reliability concerns and allow for a global enabling or disabling of ADI when appropriate for global reliability concerns.

Balancing Authorities participating in ADI communicate with their Transmission Operators and Reliability Coordinators, often with a consistent set of data being exchanged, to address congestion management problems that might be affected adversely by the continued use of ADI.

Present ADI implementations require that the participating Balancing Authorities are electrically contiguous (see OP5 below).

Balancing Authorities presently utilizing ADI do not use or acquire transmission service for the ADI process. The common premise is that ADI is a net zero flow that would have occurred absent ADI. However, Balancing Authorities must be directly connected to at least one participating Balancing Authority to participate in ADI. The ADI process will be disabled in the event that normal or contingent operations require the use of transmission being used for ADI-related power flows. Most often, the inadvertent power flows do not persist for extended periods and would net reasonably close to zero over longer intervals.

In theory, the ADI adjustment for each participating Balancing Authority should net to zero in the longer term if ACE values are more or less random, normally distributed, and having a mean of zero. Deviations from this basic premise could impact inadvertent energy accumulations.

Present ADI implementations all track the impact that the ADI process is having on hourly inadvertent and its cumulative impact in the longer term (e.g., monthly). Differing methods are in use among the present ADI implementations to address various aspects of managing the ADI adjustments.

Within Hour Assessments (Real Time)

The ADI process as defined above is a process that directly modifies Area Control Error (ACE) with an ADI adjustment term in order to achieve a final ACE value of lesser magnitude for each participating Balancing Authority. The resulting ACE value is used in the calculation of Control Performance Standard 1 (CPS1) and Balancing Authority ACE Limit (BAAL) under BAL-001.

NOTE: ADI adjustments not implemented as stand-alone adjustment to ACE can be accomplished by modifications to the the instantaneous Actual Net Interchange (NI_A) or Scheduled Net Interchange (NI_S) terms to achieve the appropriate offset in ACE. Specifically, for after-the-fact calculation of primary frequency response under BAL-003 it is necessary to exclude (or back out) the ADI adjustment from the NI_A value, as primary frequency response is measured using solely the change in actual tie line measurements. Similarly, it is also necessary to ignore (or back out) the ADI adjustment when calculating the Balancing Authority Area's (BAA's) Load, as the ADI adjustment is the shared Area Control Error that does not represent a transfer of load between to or from the BAA.

End of Hour Settlements

Since the summation of ADI adjustments within an ADI group sum to zero hourly, it is up to the ADI participants, as a group, to decide on how to settle for their ADI adjustment accounts, as long as the settlement method does not affect interconnection reliability and non-participants. Regardless of which method is used, all participants within an ADI group must use the same method.

ADI Implementation Mechanics and Controls Summary

- Balancing Authorities participating in ADI have backup plans to address failures in data exchange communications.
- Individual Balancing Authorities can enable or disable their participation in real-time for local or interconnected reliability concerns.
- Global enabling or disabling of ADI is activated when appropriate for global reliability concerns.
- The ADI process will be disabled in the event that normal or contingent operations require the use of transmission being used for ADI-related power flows.
- The present ADI implementations all have limits on the magnitude of ADI exchanges and are subject to oversight by the ADI program's stakeholders.

Operating Principles Associated with ADI Applications

The following Operating Principles (OP) must be observed by those participating in ADI applications.

OP1 – The algebraic sum of the ADI adjustments used in participating Balancing Authorities' ACE equations need to be zero so that frequency is not affected (hence frequency neutral), with due consideration of different scan rates and data latency.

OP2 – Since ADI is dependent on successful exchange of ACE-related data, Balancing Authorities that participate in ADI need to have an agreed upon backup plan that utilizes a consistent method of validating the integrity of its data exchange process, in the event of the loss of communications or data quality. (For example, the detection of an invalid data exchange due to the loss of communications or poor data quality will initiate the backup plan within 1 minute, with automatic disabling of participation upon detection.)

OP3 – The initial implementations and any subsequent modifications of ADI need to be reviewed and approved, prior to implementation, by the NERC Resources Subcommittee and the NERC Real-Time Operating Subcommittee in order to verify that the implementation of applicable Balancing and Transmission related Standards are not compromised by the implementation.

OP4 –Balancing Authorities participating in ADI need to develop and implement an appropriate methodology to continuously assure that their regulation control is not affecting the reliability of the transmission system.

OP5 – Balancing Authorities need to be directly connected to at least one participating Balancing Authority to participate in ADI. ADI needs to be designed to avoid adverse impacts on intermediary Balancing Authorities and Transmission Operators. Additionally, there needs to be an established method by which affected Balancing Authorities, Transmission Operators and Reliability Coordinators can be updated with the real-time ADI adjustments being exchanged so that they can monitor any potential reliability impacts.

OP6 – The implementation of ADI needs to allow participating Balancing Authorities to change their participation status in real-time, and the ADI algorithm needs to respond immediately to apply the ADI adjustments in recognition of the status changes.

OP7 – Real-time observability of participation and communication status, unadjusted ACE, ADI adjustments, and ADI-adjusted ACE values need to be available to Balancing Authorities, Transmission Operators, and Reliability Coordinators.

OP8 – When a Balancing Authority participates in supplemental regulation and it experiences a contingency that qualifies as a NERC Reportable Balancing Contingency Event and the other Balancing Authorities participating in supplemental regulation do not jointly activate contingency reserve sharing for the resource loss or restoration of demand, then supplemental regulation needs to be disabled by the contingent Balancing Authority when their contingency occurs, or after-the-fact corrections need to be made to remove the supplemental regulation adjustment from ACE to compute the percentage of recovery (BAL-002).

OP9 – For purposes of calculating Frequency Response Measure (BAL-003) or the calculation of BAA's load, the ADI adjustment term should be excluded as it will distort the true values.

OP10 – Balancing Authorities participating in ADI need to determine a maximum value for capping real-time ADI adjustments and ADI accumulations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Guideline

Area Control Error Diversity Interchange Process – Version 3

Applicability

Balancing Authorities (BAs)

For Information

Transmission Operators (TOPs)
Reliability Coordinators (RCs)

Preamble

It is in the public interest for the North American Electric Reliability Corporation (NERC) to develop guidelines that are useful for maintaining or enhancing the reliability of the Bulk Electric System (BES). The NERC Reliability and Security Technical Committee per its charter is authorized by the NERC Board of Trustees (Board) to develop Reliability and Security Guidelines. These guidelines establish a voluntary code of practice on a particular topic for consideration and use by BES users, owners, and operators. These guidelines are coordinated by the technical committees and include the collective experience, expertise and judgment of the industry. The objective of this reliability guideline is to distribute key best practices and information on specific issues critical to maintaining the highest levels of BES reliability. Reliability guidelines are not to be used to provide binding norms or create parameters by which compliance to standards is monitored or enforced. While the incorporation and use of guideline practices is strictly voluntary, the review, revision, and development of a program using these practices is highly encouraged to promote and achieve the highest levels of reliability for the BES.

Purpose

The purpose of this reliability guideline is to address industry practices related to the usage of ADI.

Background

Area Control Error Diversity Interchange (ADI) is a process in which participating Balancing Authorities exchange information related to their unadjusted Area Control Error (ACE) values (ACE before, or without, adjustment by the ADI process) in order to develop ADI adjustment values to their ACE. When there is a diversity of algebraic sign among ADI participants' unadjusted ACE, ADI adjustments are applied to yield ADI-adjusted ACE values that are closer to zero. Fundamentally, ADI is simply exchanging a real-time portion of one Balancing Authority's ACE for an equal but opposite portion of another Balancing Authority's ACE, thereby, reducing the ACE values of both Balancing Authorities. ADI is considered by some to be a form of supplemental regulation, and there have been several implementations since its inception in the 1990s, of which a few have been retired due to Balancing Authority consolidations. Eastern Interconnection ADI participants consider it to be supplemental regulation, while Western Interconnection ADI participants consider it to be solely an ACE exchange. Balancing Authorities participating in ADI cite the following benefits as reasons for their participation:

- Low cost and ease of implementation.
- Fewer output adjustments that reduce heat rate degradation and "wear and tear" on generating facilities.
- Reduced regulation requirements while having fewer generators operate out of economic merit order.

~~Purpose~~

~~The purpose of this reliability guideline is to address industry practices related to the usage of ADI.~~

Relevant Definitions from the NERC Glossary

Capitalized terms in this document are defined in the *NERC Glossary of Terms Used in NERC Reliability Standards*. Note that a definition for ADI does not exist within the NERC glossary at this time but a working definition is provided in the section below, entitled Basic ADI Operating Concepts.

Basic ADI Operating Concepts

The following working definition was developed and reflects the present implementations of ADI:

- **ACE Diversity Interchange** – A frequency neutral form of ACE exchange that uses real-time, sub-minute adjustments to the unadjusted ACE values of participating Balancing Authorities that always net to zero and are non-zero individually only when at least one participating Balancing Authority's unadjusted ACE value differs in algebraic sign from at least one other participating Balancing Authority's unadjusted ACE. Participating Balancing Authorities achieve reductions in their generation control and reporting ACE values by incorporating the ADI adjustments computed by an ACE Diversity Interchange algorithm. A participating BA's ADI adjustment term for each calculating cycle allows a flow that has already occurred on the participating BA's tie-lines to be maintained.

While ADI adjustment allocation methods may differ among the ADI implementations, two key features are that the computed ADI adjustments for all participating Balancing Authorities must always have a zero sum (see OP1 below) and the computed ADI adjustment for each participating Balancing Authority will equal zero in the absence of diversity in algebraic sign of the participating Balancing Authorities' unadjusted ACE. These are distinguishing features of the ADI process.

ADI Implementation Mechanics

ADI processes depend on the timely exchange of relevant data, and consistent implementation of ADI adjustments in the same timeframe of EMS scan rates (e.g., six seconds, or less). While the information exchange processes used for ADI have very high availability, Balancing Authorities participating in ADI have backup plans to address failures in data exchange communications.

The ADI processes that exist presently allow for individual Balancing Authorities to enable or disable their participation in real-time for local or interconnected reliability concerns and allow for a global enabling or disabling of ADI when appropriate for global reliability concerns.

Balancing Authorities participating in ADI communicate with their Transmission Operators and Reliability Coordinators, often with a consistent set of data being exchanged, to address congestion management problems that might be affected adversely by the continued use of ADI.

Present ADI implementations require that the participating Balancing Authorities are electrically contiguous (see OP5 below).

Balancing Authorities presently utilizing ADI do not use or acquire transmission service for the ADI process. The common premise is that ADI is a net zero flow that would have occurred absent ADI. However, Balancing Authorities must ~~have transmission connectivity and have arrangements for transmission~~ be directly connected to at least one participating Balancing Authority to participate in ADI. The ADI process will be disabled in the event that normal or contingent operations require the use of transmission being used for ADI-related power flows. Most often, the inadvertent power flows do not persist for extended periods and would net reasonably close to zero over longer intervals.

In theory, the ADI adjustment for each participating Balancing Authority should net to zero in the longer term if ACE values are more or less random, normally distributed, and having a mean of zero. Deviations from this basic premise could impact inadvertent energy accumulations.

Present ADI implementations all track the impact that the ADI process is having on hourly inadvertent and its cumulative impact in the longer term (e.g., monthly). Differing methods are in use among the present ADI implementations to address various aspects of managing the ADI adjustments.

Within Hour Assessments (Real Time)

The ADI process as defined above is a process that directly modifies Area Control Error (ACE) with an ADI adjustment term in order to achieve a final ACE value of lesser magnitude for each participating Balancing Authority. The resulting ACE value is used in the calculation of Control Performance Standard 1 (CPS1) and Balancing Authority ACE Limit (BAAL) under BAL-001.

NOTE: ~~However, if~~ ADI adjustments ~~are~~ not implemented as stand-alone adjustment to ACE can be accomplished by modifications to the ~~made to~~ the instantaneous Actual Net Interchange (NI_A) or Scheduled Net Interchange (NI_S) terms to achieve the appropriate offset in ~~calculating~~ ACE. ~~-~~

~~then for~~Specifically, for after-the-fact calculation of primary frequency response under BAL-003 it is necessary to exclude (or back out) the ADI adjustment from the NI_A value, as primary frequency response is measured using solely the change in actual tie line measurements. Similarly, it is also necessary to ignore (or back out) the ADI adjustment when calculating the Balancing Authority Area's (BAA's) Load, as the ADI adjustment is the shared Area Control Error that does not represent a transfer of load between to or from the BAA.

Formatted: Font: 10 pt, Italic

Formatted: Font: 10 pt, Italic

Formatted: Font: 10 pt, Italic

Formatted: Font: 10 pt, Italic

Formatted: Font: 10 pt, Italic

Formatted: Font: 10 pt, Italic

Formatted: Font: 10 pt, Italic

Formatted: Font: 10 pt, Italic

Formatted: Font: 10 pt, Italic

Formatted: Font: 10 pt, Italic

Formatted: Font: 10 pt, Italic

Formatted: Font: Italic

Formatted: Font: 10 pt, Italic

End of Hour Settlements

Since the summation of ADI adjustments within an ADI group sum to zero hourly, it is up to the ADI participants, as a group, to decide on how to settle for their ADI adjustment accounts, as long as the settlement method does not affect interconnection reliability and non-participants. Regardless of which method is used, all participants within an ADI group must use the same method.

ADI Implementation Mechanics and Controls Summary

- Balancing Authorities participating in ADI have backup plans to address failures in data exchange communications.
- Individual Balancing Authorities can enable or disable their participation in real-time for local or interconnected reliability concerns.
- Global enabling or disabling of ADI is activated when appropriate for global reliability concerns.
- The ADI process will be disabled in the event that normal or contingent operations require the use of transmission being used for ADI-related power flows.
- The present ADI implementations all have limits on the magnitude of ADI exchanges and are subject to oversight by the ADI program's stakeholders.

Operating Principles Associated with ADI Applications

The following Operating Principles (OP) must be observed by those participating in ADI applications.

OP1 – The algebraic sum of the ADI adjustments used in participating Balancing Authorities' ACE equations need to be zero so that frequency is not affected (hence frequency neutral), with due consideration of different scan rates and data latency.

OP2 – Since ADI is dependent on successful exchange of ACE-related data, Balancing Authorities that participate in ADI need to have an agreed upon backup plan that utilizes a consistent method of validating the integrity of its data exchange process, in the event of the loss of communications or data quality. (For example, the detection of an invalid data exchange due to the loss of communications or poor data quality will initiate the backup plan within 1 minute, with automatic disabling of participation upon detection.)

OP3 – The initial implementations and any subsequent modifications of ADI need to be reviewed and approved, prior to implementation, by the NERC Resources Subcommittee and the NERC Real-Time Operating Subcommittee in order to verify that the implementation of applicable Balancing and Transmission related Standards are not compromised by the implementation.

OP4 –Balancing Authorities participating in ADI need to develop and implement an appropriate methodology to continuously assure that their regulation control is not affecting the reliability of the transmission system.

OP5 – Balancing Authorities need to ~~have transmission connectivity and arrangements for transmission~~ be directly connected to at least one participating Balancing Authority to participate in ADI. ADI needs to be designed to avoid adverse impacts on intermediary Balancing Authorities and Transmission Operators. Additionally, there needs to be an established method by which affected Balancing Authorities, Transmission Operators and Reliability Coordinators can be updated with the real-time ADI adjustments being exchanged so that they can monitor any potential reliability impacts.

OP6 – The implementation of ADI needs to allow participating Balancing Authorities to change their participation status in real-time, and the ADI algorithm needs to respond immediately to apply the ADI adjustments in recognition of the status changes.

OP7 – Real-time observability of participation and communication status, unadjusted ACE, ADI adjustments, and ADI-adjusted ACE values need to be available to Balancing Authorities, Transmission Operators, and Reliability Coordinators. ~~The ADI participants need to share the ADI results with the appropriate Reliability Coordinators who can also assess the impacts.~~

Commented [A1]: If this statement is about real time data sharing then it is redundant and can be removed. The term "ADI results" is vague.

OP8 – When a Balancing Authority participates in supplemental regulation and it experiences a contingency that qualifies as a NERC Reportable Balancing Contingency Event and the other Balancing Authorities participating in supplemental regulation do not jointly activate contingency reserve sharing for the resource loss or restoration of demand, then supplemental regulation needs to be disabled by the contingent Balancing Authority when their contingency occurs, or after-the-fact corrections need to be made to remove the supplemental regulation adjustment from ACE to compute the percentage of recovery (BAL-002).

OP9 – For purposes of calculating Frequency Response Measure (BAL-003) or the calculation of BAA's load, the ADI adjustment term should be excluded as it will distort the true values.

OP10 – Balancing Authorities participating in ADI need to determine a maximum value for capping real-time ADI adjustments and ADI accumulations.

Page #	Line / Paragraph	Comment	Proposed Change	NERC Response
		None - Duke Energy BA does not use ADI.		Thank you for your comment.
General	45-46	Recommended to move the Purpose section of the document directly before or after the Preable section.		Proposed change accepted.
3	106	It may be helpful to define the terms CPS1 and BAAL in the document (or spell out the acronym).		Proposed change accepted.
4	137-142/OP2	The word "poor" should be included to describe data quality.	.....the loss of communications or poor data quality.	Proposed change accepted.
	89	We would ask the drafting team to provide clarity on what is meant by the phrase "have arrangements for transmission". From our perspective, it is unclear what the expectations are for this phrase. Also, we would ask for clarity in reference to the term "transmission connectivity". it is our understanding that the term suggests that BAs are physically adjacent.	If there aren't any expectations applicable toward the phrase "arrangements for transmisssion", we would suggest that the phrase be removed from the sentence.	The phrase "have transmission connectivity and have arrangements for transmission" has been changed to "be directly connected to at least one participating Balancing Authority ". OP5 has also been similarly modified.
	106-112	We have a concern that the language in this paragraph creates confusion by using the inappropirtate term "Actual Net Interchange (NIA)" in which is not a defined NERC term. From our perspective, the correct NERC defined term is "Net Actual Interchange" and this term's definition doesn't allow the ADI process to be included in the ACE formula and/or calculation. We would ask that the drafting team provide clarity on which term they are trying to use. For example, it not clear if your intent is to use the suggested NERC defined term or are you creating a new term which isn't defined in the NERC Glossary?	Modify the ACE definition to include ADI term or provide guidance that doesn't contridict the defined terms.	The term "Actual Net Interchange (NIA)" is in fact a defined NERC term and is emphasized in the document by the preceding word "instantaneous" to indicate that the ADI adjustment can be incorporated into this NIA term in the ACE equation each ACE calculating cycle. Note that there is a SAR being developed that will, in part, consider modifying the ACE definition to include the ADI term as suggested. The concerned paragraph has been modified for better clarity.
	113-117	We have a concern that the end of the hour adjustements may have a negavtive impact on the reporting ACE. From our perspective, language at the beginning of the guideline mentions that ADI is incorporated into generation control, however, this propose language contridicts the defintion for ADI. Furthermore, through our observation, we feel that this language doesn't align with OP7 language proposed in this document	Remove language from document	We believe that the end of the hour settlement is an integrated value and its adjustments should not impact the reporting ACE which is an instantaneous real time value. Since ATF settlement is not considered a reliability issue, the drafting team believe it should be addressed by ADI group members, not by a Reliability Guideline, as expressed in the language. A sentence in OP7 has been removed to eliminate ambiguity.

Agenda Item 5b
Reliability and Security
Technical Committee Meeting
June 8, 2021

Reliability Guideline: Operating Reserve Management

Action

Approve

Summary

*Reliability Guideline: Operating Reserve Management** is a three-year review of an existing, posted document. This document was posted for a 45-day comment period and conforming revisions made to it based on comments received. A clean and redline version were included in the agenda package along with a response to comments. The RS is requesting that this document be approved.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Guideline

Operating Reserve Management: Version 3

Preamble

It is in the public interest for NERC to develop guidelines that are useful for maintaining and enhancing the reliability of the Bulk Electric System (BES). The subgroups of the Reliability and Security Technical Committee (RSTC)—in accordance with the RSTC charter[1] are authorized by the NERC Board of Trustees to develop reliability and security guidelines. These guidelines establish a voluntary code of practice on a particular topic for consideration and use by BES users, owners, and operators. These guidelines are coordinated by the technical committees and include the collective experience, expertise, and judgment of the industry. The objective of this reliability guideline is to distribute key practices and information on specific issues critical to appropriately maintaining BES reliability. Reliability guidelines are not to be used to provide binding norms or create parameters by which compliance to NERC Reliability sStandards are monitored or enforced. While the incorporation, of guideline practices, is strictly voluntary, reviewing, revising, or developing a program using these practices is highly encouraged to promote and achieve appropriate BES reliability.

Purpose

This reliability guideline is intended to provide recommended practices for the management of an appropriate mix of Operating Reserve as well as readiness to respond to loss of load events. It also provides guidance with respect to the management of Operating Reserve required to meet the NERC Reliability Standards.

The reliability guideline applies primarily to Balancing Authorities (BAs) or, as appropriate, contingency reserve sharing groups (RSGs), regulation RSGs, or frequency response sharing groups. For ease of reference, this guideline uses the common term “responsible entity” for these entities, and allows the readers to make the appropriate substitution applying to them when participating or not in various groups.

Reserve planning has been practiced for a long time by NERC operating entities, dating back to Policy 1 of NERC’s operating policies. This reliability guideline leads responsible entities toward the best practices for management of the operating reserve types by dividing them into individual components to provide visibility and accountability. While the incorporation of guideline practices is strictly voluntary, reviewing, revising, or developing a process using these practices is highly encouraged to promote and achieve reliability for the BES.

[1] https://www.nerc.com/comm/RSTC/RelatedFiles/RSTC_Charter_approved20191105.pdf

Assumptions

- There can be a variety of methods that responsible entities use to ensure that sufficient Operating Reserves are available to deploy in order to support reliability. This guideline does not specify or prescribe how the need for sufficient operating reserves are met.
- NERC, as the FERC certified ERO, is responsible for the reliability of the BES and has a suite of tools to accomplish this responsibility, including but not limited to lessons learned, reliability and security guidelines, assessments and reports, the Event Analysis Program, the Compliance Monitoring and Enforcement Program, and mandatory NERC Reliability Standards.
- Each registered entity in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with the mandatory NERC Reliability Standards to maintain the reliability of the BES.
- This guideline is not intended to supersede any NERC Reliability Standards or Regional Specific Reliability Standards. Its intent is to provide a general overview to its readers of the concepts of Operating Reserve Management.
- Entities should review this reliability guideline in detail in conjunction with the periodic review of their internal processes and procedures and make any needed changes to their procedures based on their system design, configuration, and business practices.

Background

There is often confusion when operators and planners talk about reserves. One major reason for misunderstanding is a lack of common definitions; NERC’s definitions have changed over time. In addition, most NERC Regional Entities (REs) developed their own definitions. Capacity obligations have historically been the purview of state and provincial regulatory bodies, meaning that there are many different expectations and obligations across North America.

The second area of confusion concerning reserves deals with the limitations of each BA’s energy management system (EMS). Common problems include the following:

- Counting all “headroom” of on-line units as spinning reserve even though it may not be available in 10 minutes (i.e., lag from adding mills or fan speed changes)
- No intelligence in the EMS regarding load management resources
- No corrections for “temperature sensitive” resources, such as natural gas turbines
- Inadequate information on resource limitations and restrictions
- Reserves that may exist and are deployed outside the purview of the EMS system

Definitions

When reading this Reliability Guideline, the reader should note that all terms contained in the NERC Glossary of Terms and used in this Guideline are capitalized. In addition to those terms some additional terms have been defined and provided below to assist the reader. Terms defined in Italics below distinguish them from those defined and approved by NERC.

Bottoming Out Condition: A situation experienced by a BA where the Balancing Authority Area load is at or below the minimum unit capabilities of online units. This situation results in the BA having no regulation down to support operations and further load reductions. Also known as a min gen condition.

Contingency Reserve: This is the provision of capacity deployed by the BA to respond to a balancing contingency event and other contingency requirements, such as Energy Emergency Alerts (EEAs) as specified in the associated NERC Reliability Standards.

Contingency Event Recovery Period: A period that begins at the time that the resource output begins to decline within the first one-minute interval of a Reportable Balancing Contingency Event and extends for fifteen minutes thereafter.

Contingency Reserve Restoration Period: A period not exceeding 90 minutes following the end of the Contingency Event Recovery Period.

Frequency-Responsive Reserve (FRR): On-line generation with headroom that has been tested and verified to be capable of providing droop as described in the *Primary Frequency Control Reliability Guideline Reliability Guideline.*[2] Variable load that mirrors governor droop and dead-band may also be considered FRR.

Interruptible Load/Demand: Demand that the end-use customer makes available to its load-serving entity via contract or agreement for curtailment. Note: If the load can be interrupted within 10 minutes, it may be included in Contingency Reserve; otherwise, this load is generally included in Operating Reserves - Supplemental.

Most Severe Single Contingency (MSSC): The Balancing Contingency Event, due to a single contingency that was identified using system models maintained within the RSG or a BA's area that is not part of an RSG, that would result in the greatest loss (measured in megawatt (MW) of resource output used by the RSG or a BA that is not participating as a member of an RSG at the time of the event to meet firm demand and export obligation (excluding export obligation for which contingency reserve obligations are being met by the sink BA).

Operating Reserve: Operating reserve is the capability above firm system demand required to provide for regulation, load forecasting error, equipment forced and scheduled outages, and local area protection. It consists of spinning and non-spinning reserve.

[2] https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/PFC_Reliability_Guideline_rev20190501_v2_final.pdf

Operating Reserve–Spinning: This includes generation synchronized to the system and fully available to serve load within the Disturbance Recovery Period following the contingency event or load fully removable from the system within the Disturbance Recovery Period following the contingency event deployable in 10 minutes.

Operating Reserve–Supplemental: This includes generation (synchronized or capable of being synchronized to the system) that is fully available to serve load within the disturbance recovery period following the contingency event or load fully removable from the system within the disturbance recovery period following the contingency event that can be removed from the system within 10 minutes.

Other Reserve Resources**:** This includes resources that can be used outside the continuum of Operation Reserves *Figure: 1* (e.g. on four hours' notice, generations that cannot be started within 90 minutes, preplanned demand response resources).

Planning Reserve: This is the difference between a BA's expected annual peak capability and its expected annual peak demand expressed as a percentage of the annual peak demand.

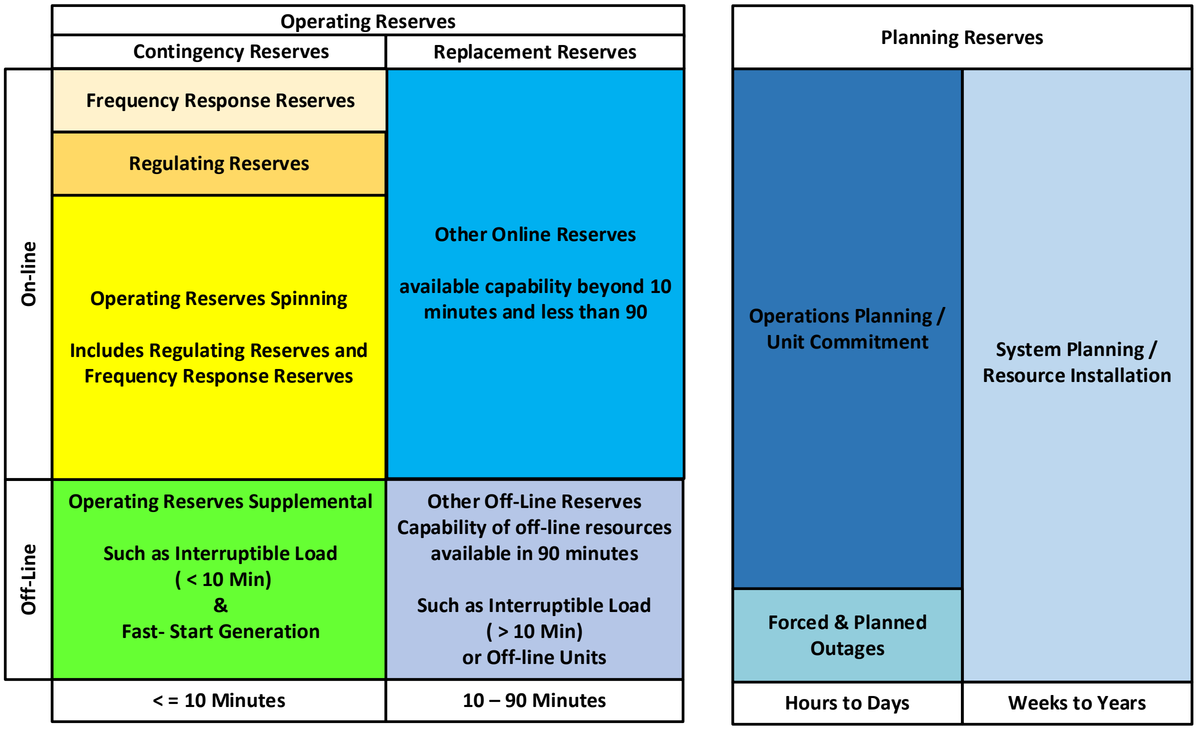
Projected Operating Reserve**:** This includes resources expected to be deployed for the point in time in question.

Regulating Reserve: This is an amount of Operating Reserve – Spinning that is responsive to automatic generation control (AGC) sufficient to provide normal regulating margin.

Replacement Reserve: Resources used to replace designated Contingency Reserve that have been deployed to respond to a contingency event. Each NERC RE sets times for Contingency Reserve restoration, typically in the 60–90-minute range. The NERC default Contingency Reserve restoration period is 90 minutes after the Contingency Event Recovery Period.

Supplemental Reserve Service**:** Supplemental reserve service provides additional capacity from electricity generators that can be used to respond to a contingency within a short period, usually 10 minutes. This is an ancillary service identified in FERC Order 888 as necessary to affect a transfer of electricity between purchasing and selling entities and is effectively FERC's equivalent to NERC's Operating Reserve.

Figure 1: Operating Reserves



Operating Reserves
Contingency Reserves
Replacement Reserves
On-line
Frequency Response Reserves
Regulating Reserves
Operating Reserves Spinning
Includes Regulating Reserves and Frequency Response Reserves
Other Online Reserves
available capability beyond 10 minutes and less than 90
Off-Line
Operating Reserves Supplemental
Such as Interruptible Load
(< 10 Min)
&
Fast- Start Generation
Other Off-Line Reserves
Capability of off-line resources available in 90 minutes
Such as Interruptible Load
(> 10 Min)
or Off-line Units
< = 10 Minutes
10 – 90 Minutes
Planning Reserves
Operations Planning / Unit Commitment
Forced & Planned Outages
System Planning / Resource Installation
Hours to Days
Weeks to Years

The various terms associated with this guideline document represent distinct conditions pertaining to reserve management and assessment. Figure 1 clearly shows the differing types of reserves between the operating and planning environment and potential availability based on time or generating unit operational status.

Guideline Details

An effective Operating Reserve program should address the following components:

- Management roles and expectation
- System operator roles
- Regulating reserve
- Contingency reserve
- Frequency responsive reserve
- Capability to respond to large loss-of-load events
- Reserve sharing groups
- Operating reserve interaction
- Load forecast error
- Fuel constraints

- Deliverability of reserves
- Unit commitment

Each individual component should address safety; processes and procedures; evaluation of any issues or problems along with solutions; testing; training; and communications. These provisions and activities together should be understood to be an Operating Reserve program.

Each responsible entity should evaluate the total reserve needed to meet its obligations under NERC Reliability Standards, namely frequency response reserves, regulating reserves up, regulating reserves down, contingency reserves, and operating reserves. Given that different reserves may be difficult to separate in actual operation, the system operator will need an understanding of the quantity of each type of reserve required. Each responsible entity should consider the types of resources and the associated portion of their capacity capable of reducing the BA's area control error (ACE) in either direction in response to each of the following:

- Frequency deviations
- Bottoming out conditions
- Ramping requirements
- A Balancing Contingency Event
- Events associated with EEA 2[3]
- Events associated with EEA 3[4]
- A large loss-of-load event

Management Roles and Expectations

Management plays an important role in maintaining an effective Operating Reserve program. The management role and expectations below provide a high-level overview of the core management responsibilities related to each Operating Reserve program. The management of each responsible entity should tailor these roles and expectations to fit within its own structure:

- Set expectations for safety, reliability, and operational performance
- Assure that an Operating Reserve program exists for each responsible entity and is current
- Provide periodic training on the Operating Reserve program and its purpose and requirements
- Ensure the proper expectation of Operating Reserve program performance
- Share insights across industry associations
- Conduct periodic evaluations of the effectiveness of the Operating Reserve program considering feedback from participants and incorporating lessons learned

[3] https://www.nerc.com/EOP-011-1.pdf

System Operator Roles

BA Operator

It is important for the system operator to know the specifics of their BA reserve strategy and maintain situation awareness through the following:

- Participate in appropriate system operator training that includes BA reserves management
- Ensure the Operating Reserve information is always current
- Maintain situation awareness and projection of reserves for a 2-hour to 6-hour horizon
- Review and validate reserve plan while considering load forecast, unit commitment, fuel supply, weather conditions, and reserve requirements
- Implement the BA Operating Reserve program in real-time that should
  - Ensure adequate reserves are available to address loss of MSSC or Frequency deviations in real-time
  - Coordinate communications with RC if inadequate reserves are forecasted or experienced
  - Adhere to EOP Operating Standards
  - Ensure the proper EEA is called when a reserve short fall is forecasted or experienced

RC Operator

It is important for the system operator to look at other indicators to determine the ultimate course of action, such as the following:

- Is the BA or BAs' ACE predominantly negative for an extended period?
- Is frequency low (i.e., more than 0.03 Hz below scheduled frequency)?
- Are reserves low in multiple BAs?
- Is load trending upward or higher than anticipated?

Based on the duration and severity of the situation, action steps may include the following:

- Verify reserve levels
- Follow EEA–review and understand individual BA EEA plans
- Direct BA(s) to take action to restore reserves
- Direct the identification of load to shed to withstand the next contingency for a post contingent action.
- Redistribute reserves by requesting BA to redispatch units to hold reserves in different areas of the BA footprint
- Shed load where appropriate if the BA or Transmission Operator cannot withstand the next contingency

Regulating Reserve

The responsible entity's balance between demand, supply (generation minus metered interchange) and frequency support is measured by its ACE. Because changes in supply and demand cannot be predicted precisely, there will be a mismatch between them, resulting in a nonzero ACE.

Each responsible entity should have a documented regulating reserve process that ensures that the responsible entity has sufficient capacity to meet the performance requirements of BAL-001. The responsible entity's process should include the following at a minimum:

- **A method for determining its regulating needs**: This method should consider the entity's generation mix, type of load, the variability in both generation and load, and the probability of extreme influences (e.g., weather).
- **Knowing what types of resources and the portion of their capacity that can be made available for regulation:** The responsible entity should have resources that will respond to the entity's need to balance supply and demand to meet the performance requirements of NERC Reliability Standards.
- **The incorporation of contractual arrangements into regulating needs, such as exports and imports:** Changes to contractual arrangements should be assessed and accounted for in the responsible entity's ability to respond and meet the performance requirements
- **Evaluation of its planned regulating reserve needs over the operating time horizon and gauge its ability to meet its regulating reserve needs on at least an hourly basis:** This should be based on changing system conditions, such as the current load, forecast errors, and generation mix.
- **Planning and implementation of the ability to restore its regulating reserve as needed:** This may include the ability to restore regulating reserve in either direction.
- **Ensuring that the regulating reserve is used by only one entity:** The regulating reserve process should include a method whereby its regulating reserve is not included in another responsible entity's Operating Reserve (i.e. regulating, contingency, or FRR) policy.

Contingency Reserve

When a responsible entity experiences an event (i.e., loss of supply or significant scheduling problems that can cause frequency disturbances), it should be able to adjust its resources in such a manner to assure its ACE recovers in accordance with the requirements of the applicable NERC Reliability Standards.

For a responsible entity to meet the requirements of the NERC Reliability Standards BAL-002, the BA needs to identify its MSSC to determine its base contingency reserve. Because there is no forgiveness for this minimum amount of contingency reserve not deployed when called upon, the individual entity could consider additional amounts based on risk analyses. To be effective, contingency reserves should be able to be deployed (including activation or communication needs) to meet the contingency event recovery period for balancing contingency events. Reserve amounts set aside as frequency responsive include unit governor reserves. These local unit governor responses are independent of control center control. A unit may or may not be able to provide frequency reserves or contingency reserves if operating at maximum output. If the unit is not operating at maximum output, the unit should be capable of providing frequency response. Due to the interactions of frequency reserves, these frequency reserves are included in the available minimum contingency reserve amounts in Interconnections composed of more than one responsible entity. At any given time, a unit may instead be loaded to maximum output and, if so, unavailable to participate in frequency response and contingency reserves.

Additionally, the responsible entity should consider an appropriate mix and coordination of FRR and contingency reserve to ensure that the responsible entity has the ability to respond to frequency events on the Interconnection as well as in its own BA area in accordance with all NERC and RE reliability standards.

Various resources may be considered for use as contingency reserve provided, they can be deployed within the appropriate time frame. As technology and innovations occur, this list may continue to grow and may include the following:

- Unloaded/loaded generation, such as quick start CTs, hydro facilities, portions of unit ramping capabilities
- Off-line generation
- Demand resources
- Energy storage devices
- Resources like wind, solar, etc., provided that any limitations are considered
- Hybrid Facilities – (e.g. Solar/Battery)

Responsible entities should consider how schedule interruption would affect their Contingency Reserves while considering the terms and conditions under which such energy schedules were arranged.

Responsible entities that choose to use energy schedules to respond to a balancing contingency event should take into account the terms and conditions under which such energy schedules were arranged and verify that they would not detract from a responsible entity's use of such schedules when meeting their contingency reserve requirements for balancing contingency events.

For RSGs, there is a prohibition against counting toward the responsible entity’s Contingency Reserve any capacity that is already included in another responsible entity’s regulating, contingency, or FRR policy. Special coordination between RSG members may be required for resources dynamically transferred between multiple responsible entities.

To assure a responsible entity can respond to a balancing contingency event in real-time, the responsible entity should plan for its available Contingency Reserves for the operating time horizon (i.e. operations planning, same day and real-time operations). The BA operator should focus their situation awareness and evaluation of reserves in a time horizon between next hour and multiple days out. The review should be flexible so that it can be updated to reflect changes available generation, load forecast, the amount of reserve available or the amount of reserve required.

Responsible entities should consider developing some form of electronic reserve monitor that would track resources available to provide the necessary response and the amount of capacity each could provide. Many EMSs currently provide this type of feature for measuring the up and down ranges of their resources. Care should be taken to recognize the up and down ranges on resources that have been made available by the purchase or sale of non-firm energy that may disappear during an event.

Responsible entities should consider leveraging their *Replacement Reserves* to meet the Contingency Reserve Restoration Period, preplanning and training of system operators may be required. Actions like the following should be considered:

- Verification of status/availability of additional resources
- Commitment of additional resources
- Implementation of demand resources, such as interruptible loads (usually prearranged contractually)
- Curtailment of recallable transactions
- The effect of emergency schedules that end before recovery completion

The responsible entity should exercise prudent operating judgment in distributing Contingency Reserves, considering the effective use of capacity in an emergency, the time required to be effective, transmission limitations, and local area requirements.

Frequency Responsive Reserve

Each responsible entity should maintain an amount of resources available to respond to frequency deviations. Planned FRR (day-ahead, day of, and hour prior) should be available in addition to planned regulating and contingency reserve. For a responsible entity experiencing a frequency deviation, FRR would be deployed to arrest frequency change and remain deployed until frequency is returned to its normal range. Although response is generally expected to come from on-line rotating machines, other resources (e.g., inverter based resources, controllable load contracted for that purpose, certain energy storage devices) can provide initial and sustained response that would help to arrest frequency change and sustain frequency at an acceptable post event-level until frequency is returned within its normal range. Each responsible entity should have a documented FRR process ensuring the responsible entity has sufficient capacity to meet the performance requirements of BAL-003. The process should include at least the following:

- The BAL-003 standard, *Frequency Response and Frequency Bias Setting*[4], specifies (in Table 1 in Attachment A) the interconnection frequency response obligation (IFRO) and the maximum delta frequency (MDF). Attachment A also provides the calculation methodology used to determine the frequency response obligation (FRO) assigned to each responsible entity in a multiple responsible entity Interconnection (the responsible entity's FRO is the same as the IFRO in a single responsible entity Interconnection). In a multiple responsible entity Interconnection, each responsible entity's FRO is its pro-rata share of the IFRO based on the sum of its annual generation MWh plus load MWh as a fraction of those for the entire Interconnection. The attachments and forms associated with the BAL-003 standard cover these calculations in more detail. To determine an initial target (at scheduled frequency) FRR level (in MW) for a given responsible entity, multiply 10 times the

[4] http://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-003-2.pdf

responsible entity's FRO (because FRO is in MW/0.1 Hz) by the MDF for the responsible entity's Interconnection. An example to illustrate this is as follows:

Given: ABC responsible entity is in the Eastern Interconnection and its pro-rata portion of IFRO is 1.5%.

Currently, the key Eastern Interconnection parameters from are: IFRO = 1015 MW/0.1 Hz and MDF = 0.420 Hz. The responsible entity's FRO is {1.5% *1015 MW/0.1 Hz} or 15.2 MW/0.1 Hz.

The responsible entity's initial FRR target is {10 * 15.2 * 0.420} or 63.84MW.

The initial target may need to be modified based on several factors. For example, if actual performance indicates additional response is needed, then the target should be increased. The responsible entity also may choose to perform a risk analysis in determining the level of FRR that assures compliance at an acceptable cost.

- Any resource (generation, load, storage device, etc.) that is capable of responding to frequency can be a candidate for inclusion as part of a responsible entity's FRR; however, such resources should help to arrest the initial frequency change (also known as primary response, and often referred to as droop or governor response) and/or provide sustained support at a post-event frequency level until frequency returns to its normal range. It is prudent practice to evaluate and test units periodically. Therefore, any resource that participates in frequency response reserve should be evaluated periodically to ensure the expected response (e.g. NERC Generator Owner/Operator Survey, or internal evaluation). Moreover, the responsible entity should have an appropriate mix of both primary and secondary reserves. The Lawrence Berkeley National Laboratory report highlights this: *Use of Frequency Response Metrics to Assess the Planning and Operating Requirements for Reliable Integration of Variable Renewable Generation, Key Findings*.[5]
- As long as the total FRR amounts for each responsible entity are satisfied, any amount of FRR may be provided through contractual agreements within the same Interconnection between responsible entities. This is the basis of the concept of frequency response sharing groups. Responsible entities can also contract for demand side options that respond to frequency deviations (usually at preset thresholds) to provide FRR. Responsible entities can likewise contract for energy storage devices to supply FRR as long as applicable terms ensure that either the devices themselves or a partnered resource provide sustained response until frequency is returned to its normal range.
- Daily resource commitment plans should include considerations to provide FRR throughout the day. In real-time operations, responsible entity operators should monitor their FRR levels in much the same way that contingency and regulating reserve are monitored. To the greatest possible extent

[5] "Increased variable renewable generation will have … impacts on the efficacy of primary frequency control actions: … Place[ing] increased requirements on the adequacy of secondary frequency control reserve. The demands placed on slower forms of frequency control, called secondary frequency control reserve, will increase because of more frequent, faster, and/or longer ramps in net system load caused by variable renewable generation. If these ramps exceed the capabilities of secondary reserves, primary frequency control reserve (that is set- aside to respond to the sudden loss of generation) will be used to make up for the shortfall. We recommend greater attention be paid to the impact of variable renewable generation on the interaction between primary and secondary frequency control reserve than has been the case in the past because we believe this is likely to emerge as the most significant frequency-response-based impact of variable renewable generation on reliability."
https://www.ferc.gov/sites/default/files/2020-05/frequencyresponsemetrics-report.pdf

possible, review of and adherence to planned levels and actual performance should be fed back into the commitment planning process to improve both the commitment plan and actual performance. This feedback should be integrated into commitment planning as well as be available to responsible entity operators to monitor levels.

- If a responsible entity experiences a frequency deviation in conjunction with a balancing contingency event, FRR will normally be restored when Contingency Reserves have been deployed in response to the balancing contingency event, but there may be circumstances when this is not the case. The key difference between this and the noncontingent case is whether Contingency Reserves have been deployed. During a balancing contingency event, it may not be possible to restore FRR from previously designated resources until Contingency Reserves have been deployed (a key reason that reserves are additive).

  For a non-contingent responsible entity experiencing a frequency deviation due to a balancing contingency event in another BA area, FRR will normally be restored when frequency returns to its normal range, but there are some exceptions where this may not be the case. If load is shed (either as a contractual resource or for other reasons) and is not restored automatically, the FRR will have served as Contingency Reserves for the contingent responsible entity (even if unintentionally) and FRR for the noncontingent responsible entity will not have been restored. If this is the case, operator action may be needed to restore the FRR by either restoring the load so that it is again available to be shed or obtaining it from other available resources.

Capability to Respond to Large Loss-of-Load Events

Because a responsible entity should be able to adjust its resources in such a manner to ensure its ACE recovers in accordance with applicable NERC Reliability Standards, a responsible entity should identify options to respond to large loss-of-load events, meaning the ability to reduce resources or rapidly bring on additional load. In many cases, decommitment of resources is an option, but with this option comes the risk that the decommitted resource cannot be recommitted in a timely manner, resulting in the exchange of a current solution for a future reliability problem. Planning can mitigate this problem.

Each responsible entity's planning for the possibility of a large loss-of-load event should include consideration of its energy import and export schedules with other responsible entities; how large loss-of-load events could be affected by interruption of these schedules while taking into account the terms and conditions under which such energy schedules were arranged; and the available down range on resources that have been made available by the sale of non-firm energy that may disappear during a contingency or other disturbance.

As noted previously, responsible entities should consider developing some form of electronic reserve monitor to track resources available to provide both up and down range of reserves.

Reserve Sharing Groups

RSGs are commercial arrangements among BAs to better enable them to collectively meet the requirements of BAL-001, BAL-002 and BAL-003. The spreading of reserve across a larger geographically dispersed group can improve reliability and provides for the opportunity to comply with the BAL performance standards while at the same time economically supplying reserve. However, the RSG should take into account the possibility of delivery being compromised by transmission constraints or generation failures when considering establishing the group's minimum reserve requirements.

An RSG is a group whose members consist of two or more BAs that collectively maintain, allocate, and supply Contingency Reserves to enable each BA within the group to recover from balancing contingency events. The NERC Reliability Standard BAL-002 allows BAs to meet the requirements of the standard through participation in an RSG, something BAs have done for many years to increase efficiency and enhance reliability. The primary benefit of RSGs is that they reduce the capacity a BA is required to withhold for reserves. This can be especially impactful for smaller BAs that have a large generator within their boundaries. Without RSGs, some smaller BAs could be required to withhold 20% or more of their capacity just for Contingency Reserves in addition to all the other reserves they carry.

Compliance for an RSG is measured via monitoring individual and group performance. The RSG can meet the compliance obligations of an event if all members individually pass based upon individual ACE values. If each member of the RSG demonstrates recovery by returning its Reporting ACE to the least of the recovery value of zero or its pre-reporting contingency event ACE value, the NERC compliance requirement is met. In addition, the RSG can also meet the compliance obligation if the collective ACE or sum of the ACE demonstrates recovery by returning the RSG's reporting ACE to the least of the recovery value of zero or its pre-reporting contingency event ACE value. An RSG can meet compliance via either method.
In order for an event to be an RSG event, the contingent BA normally has to call on reserves from the group. If it does not, then the BA is standing alone for that event. Some agreements can require that all events are RSG events by rule. Based on the agreements of the RSG, some BAs in an RSG will not have a single contingency that is a reportable event; the only possible way for them to cause a reportable event is with multiple contingencies all occurring within the 60-second period as defined in the Balancing Contingency Event glossary Term. For example, losing an entire generating station due to a fault that clears the bus.

The agreement among the participant BAs for the RSG should address the following:

- The minimum reserve requirement for the group
- The allocation of reserve among members
- The procedure for activating reserve in detailed terms that should include communication protocols and infrastructure, how long reserve is available, and who can call for reserve
- The method of establishing its MSSC or minimum reserve requirements for the group
- How the BAs will manage shortages in reserves and capacity
- The criteria used to determine when a member must declare an EEA
- The criteria that allow members to aid a deficient entity through the RSG by allowing BAs to contribute additional reserves to the group

- How generation and transmission contingencies may affect the deliverability of Contingency Reserves among the members
- Each member's portion of the total reserve requirement
- The methodology used to calculate the member's reserve responsibility
- Identification of valid reasons for failure to respond to a reserve-sharing request
- The reporting and record keeping for regulatory compliance

Scheduling energy from an adjacent BA to aid recovery need not constitute reserve sharing provided the transaction is ramped in over a period the supplying party could reasonably be expected to load generation in (e.g., 10 minutes). For certain RSG arrangements, if the transaction is ramped in more quickly (e.g., between 0 and 10 minutes) then, for the purposes of BAL-002, the BA areas are considered to be an RSG. RSGs typically flow on transmission reliability margin (TRM) and have an annual deliverability study done by all the respective transmission planners. Some BAs may have to carry a disproportionate share of reserve if some of their large units are not completely deliverable. These issues may require a special operating guide for local congestion management.

Frequency Response Sharing Group

As defined by NERC, a frequency response sharing group (FRSG) is a group whose members consist of two or more BAs that collectively maintain, allocate, and supply operating resources required to jointly meet the sum of the FRO of its members.

Frequency response has many unique characteristics that make an FRSG different from an RSG. The frequency response capability of individual generating units can change from moment to moment depending on operating point, mode of operation, type of unit, and type of control system. A steam unit that is operating at full valve but not at full capability will have no frequency response even though it appears to have additional capability above its current output. These issues may require responsible entities to develop one or more of the following:

- New unit commitment processes
- New operating guidelines
- Additional tools for operators
- more consistent governor settings

The agreement among the participant responsible entities for the FRSG should address the minimum reserve requirement for the group, the allocation of reserve among members, and reporting and record keeping for regulatory compliance. The FRSGs minimum reserve requirement should be conservative to allow for conditions, such as a unit-tripping or transmission contingencies, that could affect members' ability to supply FRR to each other. The agreement should clearly state each member's portion of the total reserve requirement as well as the methodology used to calculate the member's reserve responsibility.

Also, the agreement should consider how the information is shared in real-time based on tools created for the operators.

NERC Reliability Standard BAL-003 allows BAs to meet their FROs by electing to form FRSGs. Attachment A of that same standard specifies that an FRSG may calculate their frequency response measure (FRM) performance in one of two ways; calculate a group NIA or aggregate the group response to all events in the reporting year as one of the two following options:

- Single FRS Form 2 utilizing a group NI_A for each event and an accompanying FRS form 1 for the FRSG
- A summary spreadsheet that contains the sum of each participant's individual event performance and an accompanying FRS Form 1 for the FRSG

This section of the guideline is intended to provide recommended practices to consider for BAs when performing the following actions:

- Establishing FRSGs
- Calculating FRSG FRM performance

The Generator Governor Frequency Response Advisory[6] issued notice to industry on the importance of resource configurations for governors and control systems to allow for the provision of primary frequency response. Subsequently, a specific description of practices necessary for resources to provide primary frequency control, including the coordination of turbine controls with plant outer loop controls and an explanation of the different components of frequency response, can be found in the *Primary Frequency Control Reliability Guideline*[7].

Existing BAL-003 Forms 1 and 2 provide short-term bilateral transactions of frequency response and do not require the formal establishment and registration of a long-term FRSG, so these arrangements are not addressed by this guideline. This section of the guideline focuses solely on establishment and operating practice guidelines for a multiparty FRSG.

Establishment/Structure of an FRSG

Certain minimum criteria should apply to all candidate FRSGs prior to registration and establishment. FRSG registration is necessary to provide ERO staff with sufficient information to modify the FRSG's FRO for each operating year. The FRSG FRO is the aggregate of member BAs' FROs, including the information in the tables used in Form 1, and determine unique FRSG codes (substitutes for the BA codes normally used) for use in summary Form 1.

[6]https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/2015%20Alerts/NERC%20Alert%20A-2015-02-05-01%20Generator%20Governor%20Frequency%20Response.pdf

[7] https://www.nerc.com/comm/OC/RS_GOP_Survey_DL/PFC_Reliability_Guideline_rev20190501_v2_final.pdf

An FRSG should have a formal agreement among its members in place prior to registration. Depending on the structure and characteristics of the member BAs, the FRSG agreement among the participant responsible entities for the FRSG may need to address the following:

- Minimum frequency-responsive reserve requirement for the group
- Each member's portion of the total frequency-responsive reserve requirement
- Requirements, if applicable, of specific resources to provide frequency response
- Members' reporting, record keeping, and accountability for regulatory compliance
- Provisions for each member's alternative minimum frequency-responsive reserve requirements in identified areas in the event of emergency scenarios, such as an islanding event
- Methodology used to calculate the member's frequency-responsive reserve responsibility
- How information is shared among members in real-time
- Tools for operators to have situational awareness of frequency-responsive reserves of the FRSG
- When and how to bring more frequency-responsive reserves to bear (e.g. conservative operations, periods of low inertia)

FRSGs must be pre-arranged and member participation must coincide with the BAL-003 operating year (i.e., December 1 through November 30 of the following year). Any member of the BA's minimum period of participation must be one BAL-003 operational year. Partial BAL-003 operating year participation is not allowed. Per-event participation with other BAs is a bilateral transaction and is not considered a formation of an FRSG. Like bilateral transactions, FRSGs can only be established prior to the analysis period, and no BA may be a member of more than one FRSG at any given time.

All FRSG member BAs must be in the same Interconnection. An FRSG can be noncontiguous, but each FRSG may be subject to a transmission security review by potentially affected BAs and Transmission Operators. In some cases, a transmission security review by potentially affected BAs and Transmission Operators may be necessary for contiguous FRSGs if, for example, parallel flows caused by individual members' responses may impact other BAs or Transmission Operators.

Operations of a FRSG

FRSGs and their constituent BAs should attempt to fully respond to each event in the BAL-003 operating year.

FRSG who calculate an FRSG NI_A, should properly time-align tie line data to account for data latency and difference in member BAs' EMS scan rates. To the extent possible, this adjustment should be reflected in real-time data provided to operators. The adjustment times for each alignment should be reviewed at least annually to determine if a different amount of adjustment is needed.

The FRSGs minimum frequency-responsive reserve requirement should be conservative to allow for conditions, such as a unit-tripping or transmission contingencies, that could affect members' ability to supply frequency-responsive reserve to each other.

Although an explicit frequency-responsive reserve requirement is not necessary in every case, the FRSG should account for frequency-responsive reserves among its members in real-time. Members of an FRSG should consider including such provisions in their organizational documents.

Analysis/Reporting

FRSG member BAs must select an entity to report summary information for the FRSG to NERC. As noted above, FRSG reporting is done according to Attachment A in BAL-003.

For tie line data not already time-aligned, the FRSG and its member BAs should properly time-align prior to completing the aggregate FRS Form 2s to account for data latency and difference in member BAs' EMS scan rates.

Changes to Form 1 necessary to allow use of appropriate adjustments of FRM will be referred to NERC staff for development and implementation and those changes will be routed through the appropriate NERC committees for any vetting/validation needed.

Regulation Reserve Sharing Group

A regulation RSG is a group whose members consist of two or more BAs that collectively maintain, allocate, and supply the regulating reserve required for all member BAs to use in meeting applicable regulating standards.

A regulation RSG may be used to satisfy the Control Performance Standard (CPS) requirement in BAL-001. Sharing of regulating reserve will require real-time data sharing and dynamic transfers[8] between members. The agreement among the participant BAs of the regulation RSG should contain the maximum amount of regulation to be exchanged and the medium used to communicate the regulation to be shared. The agreement should assign responsibility for arranging transmission service and posting schedules. Regulation magnitudes may at times be limited due to resource availability or transmission constraints, so the regulation RSG agreement should include mechanisms to provide for such restrictions. If a regulation RSG has many members, the members may need central data sharing to enable communication in Real-time, as well as more complex definitions of transmission paths among members and mechanisms to address transmission path limitations. Record keeping for the regulation RSG will primarily be energy schedule records (E-Tags) and Open Access Same-Time Information System postings that allow energy flow between members. The regulation RSG agreement should also have mechanisms to settle imbalances and limit the amounts of imbalances between members.

[8] For a more detailed explanation of the implementation of dynamic transfers in general and for regulation sharing (discussed as supplemental regulation in the document) specifically, see the Dynamic Transfer Reference Guidelines reference document. This document can be found at https://www.nerc.com/comm/OC/ReferenceDocumentsDL/Dynamic_Transfer_Reference_Document_v4.pdf

Operating Reserve Interaction

The responsible entity's Operating Reserves definition should include three general categories: FRR, regulating reserve, and contingency reserve. NERC Reliability Standards primarily govern the deployment of these three categories.

Load Forecast Error

The BA Operating Reserve projections should consider load forecast error when establishing reserve levels. The following is a list of considerations that may be evaluated. These may change from day to day, from season to season, and should be included in the commitment of resources.

- Weather forecast
- Seasonal temperature variations
- Model error
- Speed of weather event

Fuel Constraints

Once resources are identified, a second review should consider fuel constraints to determine if any limitations generation exist. The following is a list of considerations that may be evaluated. These may change from day to day, from season to season, and should be included as part of a BA's projection of operating reserves and contingency reserves.

- Delivery Limitations such as Operational Flow Orders – (OFOs)
- Availability of fuel (e.g. weather impacts, market, ability to purchase)
- Transportation considerations
- Fuel supply (e.g. size of coal pile, amount of fuel oil, water reserves)
- Variability (e.g. solar and wind)
- Energy Storage Resources
    - Energy Storage Duration
    - State of Charge

Deliverability of Reserves

Deliverability of reserves is an important consideration. If reserves are undeliverable across the BA, then the BA is at increased risk of not complying with BAL-002. As transmission outages occur, the ability to deliver energy across the BA changes. A BA should consider any restrictions or limitations that may reduce generation capability as part of their operating and contingency reserve projections. The following may impact the deliverability of reserves:

- Transmission availability
- Transmission constraints

- Shape/size of BA
- RSG Considerations –
  - Ability to deliver with available transmission
  - Connection through an intermediate member
  - Operating procedures

Unit Commitment

When developing plans and addressing the needs of a BA or an RSG to reliably meet the demands of customers, unit commitment is a key component of successfully planning and ensuring that the needed generation is available in real-time operations. When dispatching the system, the BA operator should coordinate and consider any impacts to operating reserves and contingency reserves. The following is a list of considerations that may be included in the unit commitment process:

- Unit start-up time
- Available personnel
- Maintenance activities
- Environmental limitations:
  - Drought constraints
  - Intake constraints
  - Weather Conditions (Temperatures, cloud coverage, wind speeds, precipitation and humidity)
- Hydrothermal limitations
- Battery Management
- Fuel Supply
- Renewable Forecast Error

For all imbalances occurring on its power system, the responsible entity will use its reserve that is addressed by the following four-step process.

Step 1: Arrest Frequency Change

The first step in recovery is to arrest the frequency change caused by the imbalance. In most circumstances, this arresting action is performed automatically by the frequency response of generators and load on the Interconnection within the first few seconds of the imbalance. If there is insufficient frequency response or FRR to arrest a frequency decline, the Interconnection frequency will reach underfrequency relay trip points before any of the other steps can be initiated. Frequency response is therefore the most important of the required responses and FRR is the most important of the reserves.

Step 2: Contingency Reserve Deployment- Returning Frequency to its Normal Range

The second step in the recovery process is to return the frequency to its normal range. Again, this is usually accomplished by applying FRR or regulating reserve in most circumstances for small imbalances, and the CPS1 portion of BAL-001 governs the timeliness of the aggregate of such recoveries. The timeliness of the recovery from larger imbalances is governed by BAL-002 as well as CPS1. For large, sudden imbalances due to loss of generation, this is usually accomplished by applying contingency reserve. Current rules in North America require the completion of this step within a fixed time, 15 minutes in most cases. The remainder of the operating reserve not used for the frequency response is available to complete this return to the normal frequency range.

Step 3: Restore Frequency Responsive Reserve

The third step in the recovery process is the restoration of the FRR. Restoration of FRR is what indicates the Interconnection is secure and, in a position, to survive the next imbalance or disturbance. The timeliness of achieving this condition affects the risk that the Interconnection faces.

Step 4: Operating Reserves Conversion–Restoring Regulating Reserve or Contingency Reserve

The fourth step is to restore any Regulating or Contingency Reserves that has been deployed to ensure that the Interconnection can recover from the next imbalance or disturbance within an appropriate time.

Interaction

This four-step process demonstrates that the Operating Reserve components (i.e. FRR, regulating reserve and contingency reserve) are used in conjunction with one another, do not function in isolation, are always interacting, and often overlap due to timing requirements.

The Operating Reserve components can be distinguished from each other by the response time it takes to convert the reserve capacity into deliverable energy. The differences in response time allow the reserves to be utilized from the reserve with the fastest response (i.e. FRR) to the reserve with the slowest response time (i.e., Contingency Reserve). The deployment of regulating reserve in some scenarios can lead to the restoration of FRR. The deployment of Contingency Reserve in some scenarios will assist in the restoration of FRR and regulating reserve.

FRR is a “sub-minute” reserve product, and governor response provides it in most cases. Typically, Regulating Reserves and Contingency Reserves cannot be deployed in the time frame to assist in keeping frequency above underfrequency relay settings. Regulating Reserve usually does not respond quickly enough to be observable in the FRM. Contingency Reserves most often takes more than a minute and can take up to 15 minutes to deploy following the start of the contingency.

Regulating Reserves are often thought of as a “minute plus” reserve product. If it is deployed by any responsible entity in an Interconnection in a direction that supports pushing frequency towards 60 Hz, it will help restore FRR within the Interconnection.

For resource losses, contingency reserve activated by the contingent responsible entity often takes a few minutes to begin to be deployed. As its deployment progresses over time and frequency approaches 60 Hz, there will be some restoration of FRR and regulating reserve for the contingent responsible entity. A noncontingent responsible entity's FRR will tend to be restored with the deployment of the contingent responsible entity's contingency reserve as well.

For a responsible entity in a multiple responsible entity Interconnection, it may coincidentally need to deploy FRR for a load greater than generation imbalance within its Interconnection at the same time that it needs to deploy its regulating reserve in the upward direction. It may also experience its MSSC, requiring the deployment of contingency reserve while the need for FRR and regulating reserve are at a maximum. The responsible entity should plan its reserve allocations to be compliant with the NERC Reliability Standards in such a coincidental scenario.

Interconnections with only one responsible entity are unique in that only they can correct their system frequency. FRR will always be deployed automatically and coincidentally when contingency reserve needs to be deployed for a large contingency. FRR and contingency reserve are inherently co-mingled, and together they must at least equal MSSC. As with a multiple responsible entity Interconnection, regulating reserve needs to be separate from FRR and contingency reserve.

There is an additional characteristic of reserve enabling the reserve categories to be ordered. Operating Reserve categories are partially substitutable for one another. FRR is the only type of reserve that could be used as the exclusive reserve that would enable an Interconnection to operate reliably. Attempts to operate an Interconnection without FRR would result eventually in the activation of frequency relays. As long as the amount of FRR available is greater than the energy imbalance on the Interconnection, Interconnection reliability will be supported to arrest frequency deviations.

The difficulty with operating an Interconnection with only FRR is that FRR is limited in the total amount available. FRR will arrest the frequency change but will not restore frequency to its normal range, leaving the Interconnection vulnerable to the next contingency. The FRR provided by load damping is limited and the additional FRR provided by governor response is relatively expensive to provide in large quantities.

Regulating reserve is a reserve that can be substituted on a limited basis for FRR. When regulating reserve is substituted for FRR, the regulating reserve restores the FRR by returning governor response to the plants and replacing it with dispatched energy. As frequency is returned to normal range, the FRR is restored and available for reuse. The amount of regulating reserve that can be substituted for frequency response is determined by the difference between the FRR required to manage the largest imbalance that could occur on the Interconnection and the FRR that could be required in a period shorter than the response time for regulating reserve. This ensures there is sufficient FRR available to manage any imbalance occurring before there is time to replace the FRR being used with regulating reserve. Also, it extends the effective amount of FRR available, allowing the Interconnection to operate with less governor response because the amount of load damping is not easily modified.

In all cases, the maximum imbalance that is unmanageable by supplementing FRR with regulating reserve (when only FRR and regulating reserve are available) determines the minimum FRR required. In addition, the sum of the FRR and regulating reserve should exceed the largest energy imbalance occurring on the

Interconnection. Thus, when substituting regulating reserve for FRR the total amount of the FRR and regulating reserve should be equal to or exceed the amount of FRR when it is used alone.

Contingency Reserves can further supplement regulating reserve and FRR and can be manually dispatched to restore any FRR currently being used to respond to declining frequency. When dispatched, it restores both FRR and regulating reserve, making them available for reuse. Therefore, contingency reserve can be substituted for a portion of the regulating reserve that could be substituted for FRR. When this substitution is implemented, the sum of the FRR, regulating reserve, and contingency reserve should exceed the sum of regulating reserve and FRR if contingency reserve is not used.

This illustrates a power system that uses many levels of substitution to improve economic efficiency and reliability. Regulating Reserve is substituted for FRR as determined by reliability needs; contingency reserve is substituted for regulating reserve as determined by reliability needs. Reliability limits for these substitutions can be quantified with a set of inequalities:

$$FRR + RRO \geq FRRO \qquad \text{Inequality (1)}$$
$$FRR + RR + CR \geq FRR + RRO \qquad \text{Inequality (2)}$$

FRRO = FRO, equal to MW of FRR when only FRR is used.
FRR = MW of FRR when another service is substituted for FRR.
RRO = MW of regulating reserve (RR) when nothing is substituted for RR.
RR = MW of RR when another service is substituted for RR.
CR = MW of Contingency Reserves when nothing is substituted for Contingency Reserves.

Both inequalities represent the total required reserve on both sides of the inequality.

These inequalities are used to determine the FRO in BAL-003 as adjusted by the base frequency error profile that results from reserve substitution. In addition, the contingency reserve requirement in R2 of BAL-002 determines the minimum CR when it is not in use for recovery, but it does not require that the reserve used to meet the requirement exclude FRR or regulating reserve. Since regulating reserve is unique to each responsible entity and can be determined only by evaluating the characteristics of their load and generation resources, a minimum regulating reserve obligation is not specified in BAL-001. The variations of substitution of reserve as shown above suggests that the best test for reserve adequacy is whether the total capability of resources designated to provide regulating reserve, contingency reserve, and FRR is at least equal to the amount required to meet all reserve requirements concurrently.

Additionally, during the deployment of reserves in real-time, there are only limited ways to determine whether a responsible entity is holding adequate reserves. This determination can only be based on a prospective look during operations planning when there are no deviations from the expected deployment of reserves. Because this is the case, it is also important for the responsible entity to have a feedback mechanism included in its evaluations of reserve to include the uncertainties experienced during actual reserve usage. A reserve-monitoring tool could accomplish this.

The calculation of reserve levels (including FRR, regulating reserve, and contingency reserve) begins with the calculation of the amount of each type of reserve available from each resource providing any of these three types of Operating Reserves. Once the individual resource reserve contributions have been calculated, the responsible entity's total reserves by category can be determined by the sum of the reserve contributions for all contributing resources.

The calculation for these three types of reserves (i.e., FRR, regulating reserve, and contingency reserve) may not be supported in some EMSs because the FRR calculation and the interaction between reserves requires additional data not currently maintained in many EMSs. Additional data required to support the FRR calculation includes, but is not limited to, unit droop, dead-band settings, and Interconnection underfrequency load shedding (UFLS) frequency limits. Additional data may be required for other types of resources.

Finally, any calculation of the total amount of reserve and the amount in each category can change with a change in output/use of any of the resources that provide reserve for the responsible entity. For example, dispatch of contingency reserve from a resource could also affect the FRR or regulating reserve that is available from that same resource by moving the operating point of the resource nearer to one of the resource's operating limits. This could result in a reduction of one of the other reserve types in addition to the reduction in the amount of contingency reserve resulting from the dispatch. This dynamic reserve interaction should be included in operations planning and the tools used to provide the system operator with the best information.

Related Documents and Links:

NERC Reliability and Security Technical Committee Charter

NERC Operating Manual

Use of Frequency Response Metrics to Assess the Planning and Operating Requirements for Reliable Integration of Variable Renewable Generation, Key Findings

Cited Documents

NERC Alert A-2015-02-05-01 Generator Governor Frequency Response

Primary Frequency Control Reliability Guideline

NERC Standard BAL-003

FERC Final Order on Third-Party Provision of Primary Frequency Response Service - FERC Docket RM15-2-000 Order No. 819

Revision History

Date	Version Number	Reason/Comments
10/18/2013	1.0	Initial Version – “Operating Reserve Management”
12/13/2017	2.0	Revised to include more detailed description of FRSG
9/13/2020	3.0	3-year review and revisions
4/15/2021	3.0	Industry Comments addressed

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Guideline

Operating Reserve Management: Version 3

Preamble

It is in the public interest for NERC to develop guidelines that are useful for maintaining and enhancing the reliability of the Bulk Electric System (BES). The subgroups of the Reliability and Security Technical Committee (RSTC)—in accordance with the RSTC charter[1] are authorized by the NERC Board of Trustees to develop reliability and security guidelines. These guidelines establish a voluntary code of practice on a particular topic for consideration and use by BES users, owners, and operators. These guidelines are coordinated by the technical committees and include the collective experience, expertise, and judgment of the industry. The objective of this reliability guideline is to distribute key practices and information on specific issues critical to appropriately maintaining BES reliability. Reliability guidelines are not to be used to provide binding norms or create parameters by which compliance to NERC Reliability sS~~s~~tandards are monitored or enforced. While the incorporation, of guideline practices, is strictly voluntary, reviewing, revising, or developing a program using these practices is highly encouraged to promote and achieve appropriate BES reliability.

Purpose

This reliability guideline is intended to provide recommended practices for the management of an appropriate mix of Operating Reserve as well as readiness to respond to loss of load events. It also provides guidance with respect to the management of Operating Reserve required to meet the NERC Reliability Standards.

The reliability guideline applies primarily to Balancing Authorities (BAs) or, as appropriate, contingency reserve sharing groups (RSGs), regulation RSGs, or frequency response sharing groups. For ease of reference, this guideline uses the common term “responsible entity” for these entities, and allows the readers to make the appropriate substitution applying to them when participating or not in various groups.

Reserve planning has been practiced for a long time by NERC operating entities, dating back to Policy 1 of NERC’s operating policies. This reliability guideline leads responsible entities toward the best practices for management of the operating reserve types by dividing them into individual components to provide visibility and accountability. While the incorporation of guideline practices is strictly voluntary, reviewing, revising, or developing a process using these practices is highly encouraged to promote and achieve reliability for the BES.

[1] https://www.nerc.com/comm/RSTC/RelatedFiles/RSTC_Charter_approved20191105.pdf

Assumptions

- There can be a variety of methods that responsible entities use to ensure that sufficient Operating Reserves are available to deploy in order to support reliability. This guideline does not specify or prescribe how the need for sufficient operating reserves are met.
- NERC, as the FERC certified ERO,~~[2]~~ is responsible for the reliability of the BES and has a suite of tools to accomplish this responsibility, including but not limited to lessons learned, reliability and security guidelines, assessments and reports, the Event Analysis Program, the Compliance Monitoring and Enforcement Program, and mandatory NERC Reliability Standards.
- Each registered entity in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with the mandatory NERC Reliability S~~s~~tandards to maintain the reliability of the BES.
- This guideline is not intended to supersede any NERC Reliability Standards or Regional Specific Reliability Standards. Its intent is to provide a general overview to its readers of the concepts of Operating Reserve Management.
- Entities should review this reliability guideline in detail in conjunction with the periodic review of their internal processes and procedures and make any needed changes to their procedures based on their system design, configuration, and business practices.

Formatted: Font:

Background

There is often confusion when operators and planners talk about reserves. One major reason for misunderstanding is a lack of common definitions; NERC's definitions have changed over time. In addition, most NERC Regional Entities (REs) developed their own definitions. Capacity obligations have historically been the purview of state and provincial regulatory bodies, meaning that there are many different expectations and obligations across North America.

The second area of confusion concerning reserves deals with the limitations of each BA's energy management system (EMS). Common problems include the following:

- Counting all "headroom" of on-line units as spinning reserve even though it may not be available in 10 minutes (i.e., lag from adding mills or fan speed changes)
- No intelligence in the EMS regarding load management resources
- No corrections for "temperature sensitive" resources, such as natural gas turbines
- Inadequate information on resource limitations and restrictions
- Reserves that may exist and are deployed outside the purview of the EMS system

~~[2] http://www.ferc.gov/whats-new/comm-meet/072006/E-5.pdf~~

Definitions

When reading this Reliability Guideline, the reader should note that all terms contained in the NERC Glossary of Terms and used in this Guideline are capitalized. In addition to those terms some additional terms have been defined and provided below to assist the reader. Terms defined in Italics below distinguish them from those defined and approved by NERC.~~Capitalized terms used within this guideline are defined as part of the NERC Glossary. Terms which are not capitalized are used as references within this guideline.~~

Bottoming Out Condition: A situation experienced by a BA where the Balancing Authority Area load is at or below the minimum unit capabilities of online units. This situation results in the BA having no regulation down to support operations and further load reductions. Also known as a min gen condition.

Contingency Reserve: This is the provision of capacity deployed by the BA to respond to a balancing contingency event and other contingency requirements, such as E~~e~~nergy E~~e~~mergency A~~a~~lerts (EEAs) as specified in the associated NERC Reliability Standards.

Contingency Event Recovery Period: A period that begins at the time that the resource output begins to decline within the first one-minute interval of a Reportable Balancing Contingency Event and extends for fifteen minutes thereafter.

Contingency Reserve Restoration Period: A period not exceeding 90 minutes following the end of the Contingency Event Recovery Period.

Frequency-Responsive Reserve (FRR): On-line generation with headroom that has been tested and verified to be capable of providing droop as described in the *Primary Frequency Control Reliability Guideline Reliability Guideline.*[3] Variable load that mirrors governor droop and dead-band may also be considered FRR.

Interruptible Load/Demand: Demand that the end-use customer makes available to its load-serving entity via contract or agreement for curtailment. Note: If the load can be interrupted within 10 minutes, it may be included in Contingency Reserve; otherwise, this load is generally included in Operating Reserves - Supplemental.

Most Severe Single Contingency (MSSC): The Balancing Contingency Event, due to a single contingency that was identified using system models maintained within the RSG or a BA's area that is not part of an RSG, that would result in the greatest loss (measured in megawatt (MW) of resource output used by the RSG or a BA that is not participating as a member of an RSG at the time of the event to meet firm demand and export obligation (excluding export obligation for which contingency reserve obligations are being met by the sink BA).

[3] https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/PFC_Reliability_Guideline_rev20190501_v2_final.pdf

Formatted: Font: Italic

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Font: Not Bold

Operating Reserve: Operating reserve is the capability above firm system demand required to provide for regulation, load forecasting error, equipment forced and scheduled outages, and local area protection. It consists of spinning and non-spinning reserve.

Operating Reserve–Spinning: This includes generation synchronized to the system and fully available to serve load within the Disturbance Recovery Period following the contingency event or load fully removable from the system within the Disturbance Recovery Period ~~disturbance recovery period~~ following the contingency event deployable in 10 minutes.

Formatted: Highlight

Operating Reserve–Supplemental: This includes generation (synchronized or capable of being synchronized to the system) that is fully available to serve load within the disturbance recovery period following the contingency event or load fully removable from the system within the disturbance recovery period following the contingency event that can be removed from the system within 10 minutes.

***Other Reserve Resources*:** This includes resources that can be used outside the continuum of Operation Reserves *Figure: 1* (e.g.~~i.e~~., on four hours' notice, generators that cannot be started within 90 minutes, preplanned demand response resources).

Formatted: Font: Italic

Planning Reserve: This is the difference between a BA's expected annual peak capability and its expected annual peak demand expressed as a percentage of the annual peak demand.

***Projected Operating Reserve*:** This includes resources expected to be deployed for the point in time in question.

Formatted: Font: Italic

Regulating Reserve: This is an amount of Operating Reserve – Spinning that is responsive to automatic generation control (AGC) sufficient to provide normal regulating margin.

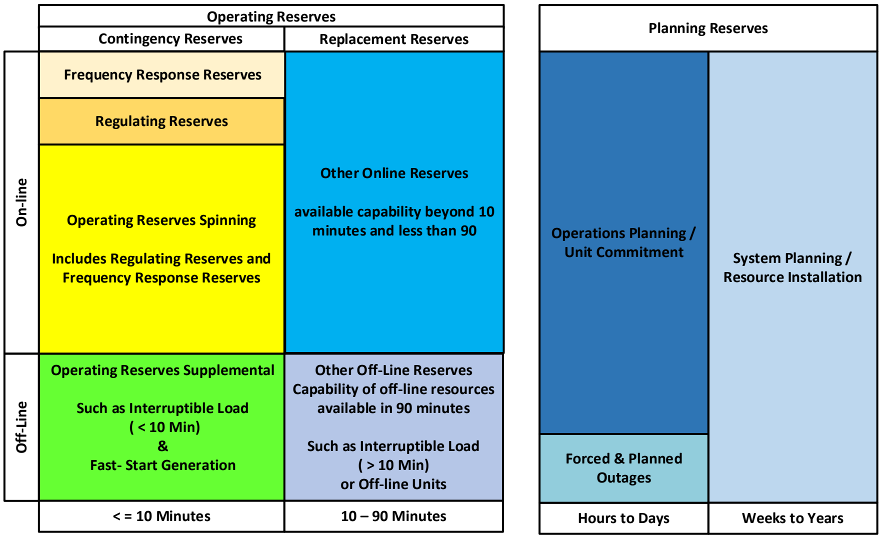
Replacement Reserve: Resources used to replace designated Contingency Reserve that have been deployed to respond to a contingency event. Each NERC RE sets times for Contingency Reserve restoration, typically in the 60–90-minute range. The NERC default Contingency Reserve restoration period is 90 minutes after the ~~Disturbance~~ Contingency Event Recovery Period.

Formatted: Font: Italic

***Supplemental Reserve Service*:** Supplemental reserve service provides additional capacity from electricity generators that can be used to respond to a contingency within a short period, usually 10 minutes. This is an ancillary service identified in FERC Order 888 as necessary to affect a transfer of electricity between purchasing and selling entities and is effectively FERC's equivalent to NERC's Operating Reserve.

Formatted: Font: Italic

Figure 1: Operating Reserves


Operating Reserves
Contingency Reserves
Replacement Reserves
Planning Reserves
On-line
Off-Line
Frequency Response Reserves
Regulating Reserves
Operating Reserves Spinning
Includes Regulating Reserves and Frequency Response Reserves
Other Online Reserves
available capability beyond 10 minutes and less than 90
Operations Planning / Unit Commitment
System Planning / Resource Installation
Operating Reserves Supplemental
Such as Interruptible Load (< 10 Min) & Fast- Start Generation
Other Off-Line Reserves Capability of off-line resources available in 90 minutes
Such as Interruptible Load (> 10 Min) or Off-line Units
Forced & Planned Outages
< = 10 Minutes
10 – 90 Minutes
Hours to Days
Weeks to Years

The various terms associated with this guideline document represent distinct conditions pertaining to reserve management and assessment. Figure 1 clearly shows the differing types of reserves between the operating and planning environment and potential availability based on time or generating unit operational status.

Formatted: Font: (Default) +Body (Calibri), 12 pt, Not Bold, Font color: Auto

Guideline Details

An effective Operating Reserve program should address the following components:

- Management roles and expectation
- System operator roles
- Regulating reserve
- Contingency reserve
- Frequency responsive reserve
- Capability to respond to large loss-of-load events
- Reserve sharing groups
- Operating reserve interaction
- Load forecast error
- Fuel constraints

- Deliverability of reserves
- Unit commitment

Each individual component should address safety; processes and procedures; evaluation of any issues or problems along with solutions; testing; training; and communications. These provisions and activities together should be understood to be an Operating Reserve program.

Each responsible entity should evaluate the total reserve needed to meet its obligations under NERC Reliability Standards, namely frequency response reserves, regulating reserves up, regulating reserves down, contingency reserves, and operating reserves. Given that different reserves may be difficult to separate in actual operation, the system operator will need an understanding of the quantity of each type of reserve required. Each responsible entity should consider the types of resources and the associated portion of their capacity capable of reducing the BA's area control error (ACE) in either direction in response to each of the following:

- Frequency deviations
- Bottoming out conditions
- Ramping requirements
- A Balancing Contingency Event
- Events associated with EEA 2[4]
- Events associated with EEA 3[4]
- A large loss-of-load event

Commented [ORA1]: Need to define bottoming out as part of the bullets – several comments – Min Generation Events system conditions where BA has no regulation down to address. Definitions section.

Formatted: Superscript

Management Roles and Expectations

Management plays an important role in maintaining an effective Operating Reserve program. The management role and expectations below provide a high-level overview of the core management responsibilities related to each Operating Reserve program. The management of each responsible entity should tailor these roles and expectations to fit within its own structure:

- Set expectations for safety, reliability, and operational performance
- Assure that an Operating Reserve program exists for each responsible entity and is current
- Provide ~~annual~~ periodic training on the Operating Reserve program and its purpose and requirements
- Ensure the proper expectation of Operating Reserve program performance
- Share insights across industry associations

[4] https://www.nerc.com/EOP-011-1.pdf

- Conduct ~~an~~ periodic evaluations of the effectiveness of the Operating Reserve program considering feedback from participants and incorporating ~~e~~ lessons learned

System Operator Roles

BA Operator

It is important for the system operator to know the specifics of their BA reserve strategy and maintain situation awareness through the following:

- Participate in appropriate system operator training that includes BA reserves management
- Ensure the Operating Reserve information is always current
- Maintain situation awareness and projection of reserves for a 2-hour to 6-hour horizon
- Review and validate reserve plan while considering load forecast, unit commitment, fuel supply, weather conditions, and reserve requirements
- Implement the BA Operating Reserve program in real-time that should
  - Ensure adequate reserves are available to address loss of MSSC or Frequency deviations in real-time
  - Coordinate communications with RC if inadequate reserves are forecasted or experienced
  - Adhere to EOP Operating Standards
  - ~~Issue~~ Ensure the proper EEA is called when a reserve short fall is forecasted or experienced

RC Operator

It is important for the system operator to look at other indicators to determine the ultimate course of action, such as the following:

- Is the BA or BAs' ACE predominantly negative for an extended period?
- Is frequency low (i.e., more than 0.03 Hz below scheduled frequency)?
- Are reserves low in multiple BAs?
- Is load trending upward or higher than anticipated?

Based on the duration and severity of the situation, action steps may include the following:

- Verify reserve levels
- Follow EEA–review and understand individual BA EEA plans
- Direct BA(s) to take action to restore reserves
- Direct the identification of load to shed to withstand the next contingency for a post contingent action.
- Redistribute reserves by requesting BA to redispatch units to hold reserves in different areas of the BA footprint

- Shed load where appropriate if the BA or Transmission Operator cannot withstand the next contingency

Regulating Reserve

The responsible entity's balance between demand, supply (generation minus metered interchange) and frequency support is measured by its ACE. Because changes in supply and demand cannot be predicted precisely, there will be a mismatch between them, resulting in a nonzero ACE.

Each responsible entity should have a documented regulating reserve process that ensures that the responsible entity has sufficient capacity to meet the performance requirements of BAL-001~~-2~~. The responsible entity's process should include the following at a minimum:

- **A method for determining its regulating needs**: This method should consider the entity's generation mix, type of load, the variability in both generation and load, and the probability of extreme influences (e.g., weather).
- **Knowing what types of resources and the portion of their capacity that can be made available for regulation:** The responsible entity should have resources that will respond to the entity's need to balance supply and demand to meet the performance requirements of NERC Reliability Standards.
- **The incorporation of contractual arrangements into regulating needs, such as exports and imports:** Changes to contractual arrangements should be assessed and accounted for in the responsible entity's ability to respond and meet the performance requirements
- **Evaluation of its planned regulating reserve needs over the operating time horizon and gauge its ability to meet its regulating reserve needs on at least an hourly basis:** This should be based on changing system conditions, such as the current load, forecast errors, and generation mix.
- **Planning and implementation of the ability to restore its regulating reserve as needed:** This may include the ability to restore regulating reserve in either direction.
- **Ensuring that the regulating reserve is used by only one entity:** The regulating reserve process should include a method whereby its regulating reserve is not included in another responsible entity's Operating Reserve (i.e. regulating, contingency, or FRR) policy.

Contingency Reserve

When a responsible entity experiences an event (i.e., loss of supply or significant scheduling problems that can cause frequency disturbances), it should be able to adjust its resources in such a manner to assure its ACE recovers in accordance with the requirements of the applicable NERC Reliability Standards.

For a responsible entity to meet the requirements of the NERC Reliability Standards BAL-002~~-3~~, the BA needs to identify its MSSC to determine its base contingency reserve. Because there is no forgiveness for this minimum amount of contingency reserve not deployed when called upon, the individual entity could consider additional amounts based on risk analyses. To be effective, contingency reserves should be able to be deployed (including activation or communication needs) to meet the contingency event recovery period for balancing contingency events. Reserve amounts set aside as frequency responsive include unit governor reserves. These local unit governor responses are independent of control center control. A unit may or may not be able to provide frequency reserves or contingency reserves if operating at maximum output. If the unit is not operating at maximum output, the unit should be capable of providing frequency response. Due to the interactions of frequency reserves, these frequency reserves are included in the available minimum contingency reserve amounts in Interconnections composed of more than one responsible entity. At any given time, a unit may instead be loaded to maximum output and, if so, unavailable to participate in frequency response and contingency reserves.~~Reserve amounts set aside as frequency responsive include unit governor reserves. These local responses are independent of control center control. If the unit is not operating at maximum output, the unit should be capable of providing frequency response. Due to the interactions of frequency reserves, these are included in the available minimum contingency reserve amounts in Interconnections composed of more than one responsible entity. At any given time, a unit may also be loaded to maximum output and unavailable to meet the reliability requirements associated with frequency response and contingency reserves.~~

Additionally, the responsible entity should consider an appropriate mix and coordination of FRR and contingency reserve to ensure that the responsible entity has the ability to respond to frequency events on the Interconnection as well as in its own BA area in accordance with all NERC and RE reliability ~~s~~standards.

Various resources may be considered for use as contingency reserve provided, they can be deployed within the appropriate time frame. As technology and innovations occur, this list may continue to grow and may include the following:

- Unloaded/loaded generation, such as quick start CTs, hydro facilities, portions of unit ramping capabilities
- Off-line generation
- Demand resources
- Energy storage devices
- Resources like wind, solar, etc., provided that any limitations are considered
- Hybrid Facilities – (e.g. Solar/Battery)

Formatted: Font: (Intl) Calibri

Responsible entities should consider how schedule interruption would affect their Contingency Reserves while considering the terms and conditions under which such energy schedules were arranged.

Responsible entities that choose to use energy schedules to respond to a balancing contingency event should take into account the terms and conditions under which such energy schedules were arranged and verify that they would not detract from a responsible entity's use of such schedules when meeting their contingency reserve requirements for balancing contingency events.

For RSGs, there is a prohibition against counting toward the responsible entity’s Contingency Reserve any capacity that is already included in another responsible entity’s regulating, contingency, or FRR policy. Special coordination between RSG members may be required for resources dynamically transferred between multiple responsible entities.

To assure a responsible entity can respond to a balancing contingency event in real-time, the responsible entity should plan for its available Contingency Reserves for the operating time horizon (i.e. operations planning, same day and real-time operations). The BA operator should focus their situation awareness and evaluation of reserves in a time horizon between next hour and multiple days out. The review should be flexible so that it can be updated to reflect changes available generation, load forecast, the amount of reserve available or the amount of reserve required.

Responsible entities should consider developing some form of electronic reserve monitor that would track resources available to provide the necessary response and the amount of capacity each could provide. Many EMSs currently provide this type of feature for measuring the up and down ranges of their resources. Care should be taken to recognize the up and down ranges on resources that have been made available by the purchase or sale of non-firm energy that may disappear during an event.

Responsible entities should consider leveraging their *Replacement Reserves* to meet the Contingency Reserve Restoration Period, preplanning and training of system operators may be required. Actions like the following should be considered: ~~For a responsible entity should leverage their Replacement Reserves to meet the Contingency Reserve Restoration Period, preplanning and training of system operators may be required. Actions like the following may be considered:~~

Formatted: Font: Italic

- Verification of status/availability of additional resources
- Commitment of additional resources
- Implementation of demand resources, such as interruptible loads (usually prearranged contractually)
- Curtailment of recallable transactions
- ~~Consider the~~The effect of emergency schedules that end before recovery completion

Formatted: Numbering Bullet 1, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

The responsible entity should exercise prudent operating judgment in distributing Contingency Reserves, considering the effective use of capacity in an emergency, the time required to be effective, transmission limitations, and local area requirements.

Frequency Responsive Reserve

Each responsible entity should maintain an amount of resources available to respond to frequency deviations. Planned FRR (day-ahead, day of, and hour prior) should be available in addition to planned regulating and contingency reserve. For a responsible entity experiencing a frequency deviation, FRR would be deployed to arrest frequency change and remain deployed until frequency is returned to its normal range. Although response is generally expected to come from on-line rotating machines, other resources (e.g., inverter based resources, controllable load contracted for that purpose, certain energy storage devices) can provide initial and sustained response that would help to arrest frequency change and sustain frequency at an acceptable post event-level until frequency is returned within its normal range. Each responsible entity should have a documented FRR process ensuring the responsible entity has sufficient capacity to meet the performance requirements of BAL-003~~-2~~. The process should include at least the following:

- The BAL-003~~-2~~ standard, *Frequency Response and Frequency Bias Setting*[5], specifies (in Table 1 in Attachment A) the interconnection frequency response obligation (IFRO) and the maximum delta frequency (MDF). Attachment A also provides the calculation methodology used to determine the frequency response obligation (FRO) assigned to each responsible entity in a multiple responsible entity Interconnection (the responsible entity's FRO is the same as the IFRO in a single responsible entity Interconnection). In a multiple responsible entity Interconnection, each responsible entity's FRO is its pro-rata share of the IFRO based on the sum of its annual generation MWh plus load MWh as a fraction of those for the entire Interconnection. The attachments and forms associated with the BAL-003~~-2~~ standard cover these calculations in more detail. To determine an initial target (at scheduled frequency) FRR level (in MW) for a given responsible entity, multiply 10 times the responsible entity's FRO (because FRO is in MW/0.1 Hz) by the MDF for the responsible entity's Interconnection. An example to illustrate this is as follows:

  Given: ABC responsible entity is in the Eastern Interconnection and its pro-rata portion of IFRO is 1.5%.

  Currently, the key Eastern Interconnection parameters from are: IFRO = 1015 MW/0.1 Hz and MDF = 0.420 Hz. The responsible entity's FRO is {1.5% *1015 MW/0.1 Hz} or 15.2 MW/0.1 Hz.

  The responsible entity's initial FRR target is {10 * 15.2 * 0.420} or 63.84MW.

  The initial target may need to be modified based on several factors. For example, if actual performance indicates additional response is needed, then the target should be increased. The responsible entity also may choose to perform a risk analysis in determining the level of FRR that assures compliance at an acceptable cost.

- Any resource (generation, load, storage device, etc.) that is capable of responding to frequency can be a candidate for inclusion as part of a responsible entity's FRR; however, such resources should help to arrest the initial frequency change (also known as primary response, and often referred to as droop or governor response) and/or provide sustained support at a post-event frequency level until frequency returns to its normal range. It is prudent practice to evaluate and test units periodically. Therefore, any resource that participates in frequency response reserve should be evaluated periodically to ensure the expected response (e.g. NERC Generator Owner/Operator Survey, or internal evaluation). Moreover, the responsible entity should have an appropriate mix of both primary and secondary reserves. The Lawrence Berkeley National Laboratory report highlights this: *Use of Frequency Response Metrics to Assess the Planning and Operating Requirements for Reliable Integration of Variable Renewable Generation, Key Findings*.[6]

[5] http://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-003-2.pdf

[6] "5. Increased variable renewable generation will have … impacts on the efficacy of primary frequency control actions: … Place[ing] increased requirements on the adequacy of secondary frequency control reserve. The demands placed on slower forms of frequency control, called secondary frequency control reserve, will increase because of more frequent, faster, and/or longer ramps in net system load caused by variable renewable generation. If these ramps exceed the capabilities of secondary reserves, primary frequency control reserve (that is set- aside to respond to the sudden loss of generation) will be used to make up for the shortfall. We recommend greater attention be paid to the impact of variable renewable generation on the interaction between primary and secondary frequency control reserve than has been the case in the past because we believe this is likely to emerge as the most significant frequency-response-based impact of variable renewable generation on reliability."
https://www.ferc.gov/sites/default/files/2020-05/frequencyresponsemetrics-report.pdf

- As long as the total FRR amounts for each responsible entity are satisfied, any amount of FRR may be provided through contractual agreements within the same Interconnection between responsible entities. This is the basis of the concept of frequency response sharing groups. Responsible entities can also contract for demand side options that respond to frequency deviations (usually at preset thresholds) to provide FRR. Responsible entities can likewise contract for energy storage devices to supply FRR as long as applicable terms ensure that either the devices themselves or a partnered resource provide sustained response until frequency is returned to its normal range.
- Daily resource commitment plans should include considerations to provide FRR throughout the day. In real-time operations, responsible entity operators should monitor their FRR levels in much the same way that contingency and regulating reserve are monitored. To the greatest possible extent possible, review of and adherence to planned levels and actual performance should be fed back into the commitment planning process to improve both the commitment plan and actual performance. This feedback should be integrated into commitment planning as well as be available to responsible entity operators to monitor levels.
- If a responsible entity experiences a frequency deviation in conjunction with a balancing contingency event, FRR will normally be restored when Contingency Reserves have been deployed in response to the balancing contingency event, but there may be circumstances when this is not the case. The key difference between this and the noncontingent case is whether Contingency Reserves have been deployed. During a balancing contingency event, it may not be possible to restore FRR from previously designated resources until Contingency Reserves have been deployed (a key reason that reserves are additive).

  For a non-contingent responsible entity experiencing a frequency deviation due to a balancing contingency event in another BA area, FRR will normally be restored when frequency returns to its normal range, but there are some exceptions where this may not be the case. If load is shed (either as a contractual resource or for other reasons) and is not restored automatically, the FRR will have served as Contingency Reserves for the contingent responsible entity (even if unintentionally) and FRR for the noncontingent responsible entity will not have been restored. If this is the case, operator action may be needed to restore the FRR by either restoring the load so that it is again available to be shed or obtaining it from other available resources.

Capability to Respond to Large Loss-of-Load Events

Because a responsible entity should be able to adjust its resources in such a manner to ensure its ACE recovers in accordance with applicable NERC Reliability Standards, a responsible entity should identify options to respond to large loss-of-load events, meaning the ability to reduce resources or rapidly bring on additional load. In many cases, decommitment of resources is an option, but with this option comes the risk that the decommitted resource cannot be recommitted in a timely manner, resulting in the exchange of a current solution for a future reliability problem. Planning can mitigate this problem.

Each responsible entity's planning for the possibility of a large loss-of-load event should include consideration of its energy import and export schedules with other responsible entities; how large loss-of-load events could be affected by interruption of these schedules while taking into account the terms and conditions under which such energy schedules were arranged; and the available down range on resources that have been made available by the sale of non-firm energy that may disappear during a contingency or other disturbance.

As noted previously, responsible entities should consider developing some form of electronic reserve monitor to track resources available to provide both up and down range of reserves.

Reserve Sharing Groups

RSGs are commercial arrangements among BAs to better enable them to collectively meet the requirements of BAL-001~~-2~~, BAL-002~~-3~~ and BAL-003~~--2~~. The spreading of reserve across a larger geographically dispersed group can improve reliability and provides for the opportunity to comply with the BAL performance standards while at the same time economically supplying reserve. However, the RSG should take into account the possibility of delivery being compromised by transmission constraints or generation failures when considering establishing the group’s minimum reserve requirements.

An RSG is a group whose members consist of two or more BAs that collectively maintain, allocate, and supply Contingency Reserves to enable each BA within the group to recover from balancing contingency events. The NERC Reliability Standard BAL-002~~-2~~ allows BAs to meet the requirements of the standard through participation in an RSG, something BAs have done for many years to increase efficiency and enhance reliability. The primary benefit of RSGs is that they reduce the capacity a BA is required to withhold for reserves. This can be especially impactful for smaller BAs that have a large generator within their boundaries. Without RSGs, some smaller BA~~’~~s could be required to withhold 20% or more of their capacity just for Contingency Reserves in addition to all the other reserves they carry.

Compliance for an RSG is measured via monitoring individual and group performance. The RSG can meet the compliance obligations of an event if all members individually pass based upon individual ACE values. If each member of the RSG demonstrates recovery by returning its Reporting ACE to the least of the recovery value of zero or its pre-reporting contingency event ACE value, the NERC compliance requirement is met. In addition, the RSG can also meet the compliance obligation if the collective ACE or sum of the ACE demonstrates recovery by returning the RSG’s reporting ACE to the least of the recovery value of zero or its pre-reporting contingency event ACE value. An RSG can meet compliance via either method.
In order for an event to be an RSG event, the contingent BA normally has to call on reserves from the group. If it does not, then the BA is standing alone for that event. Some agreements can require that all events are RSG events by rule. Based on the agreements of the RSG, some BAs in an RSG will not have a single contingency that is a reportable event; the only possible way for them to cause a reportable event is with multiple contingencies all occurring within the 60-second period as defined in the Balancing Contingency Event glossary term~~BAL-002-2~~. For example, losing an entire generating station due to a fault that clears the bus.

The agreement among the participant BAs for the RSG should address the following:

- The minimum reserve requirement for the group

- The allocation of reserve among members
- The procedure for activating reserve in detailed terms that should include communication protocols and infrastructure, how long reserve is available, and who can call for reserve
- The method of establishing its MSSC or minimum reserve requirements for the group
- How the BAs will manage shortages in reserves and capacity
- The criteria used to determine when a member must declare an EEA
- The criteria that allow members to aid a deficient entity through the RSG by allowing BAs to contribute additional reserves to the group
- How generation and transmission contingencies may affect the deliverability of Contingency Reserves among the members
- Each member's portion of the total reserve requirement
- The methodology used to calculate the member's reserve responsibility
- Identification of valid reasons for failure to respond to a reserve-sharing request
- The reporting and record keeping for regulatory compliance

Scheduling energy from an adjacent BA to aid recovery need not constitute reserve sharing provided the transaction is ramped in over a period the supplying party could reasonably be expected to load generation in (e.g., 10 minutes). For certain RSG arrangements, if the transaction is ramped in more quickly (e.g., between 0 and 10 minutes) then, for the purposes of BAL-002~~-3~~, the BA areas are considered to be an RSG. RSGs typically flow on transmission reliability margin (TRM) and have an annual deliverability study done by all the respective transmission planners. Some BAs may have to carry a disproportionate share of reserve if some of their large units are not completely deliverable. These issues may require a special operating guide for local congestion management.

Frequency Response Sharing Group

As defined by NERC, a frequency response sharing group (FRSG) is a group whose members consist of two or more BAs that collectively maintain, allocate, and supply operating resources required to jointly meet the sum of the FRO of its members.

Frequency response has many unique characteristics that make an FRSG different from an RSG. The frequency response capability of individual generating units can change from moment to moment depending on operating point, mode of operation, type of unit, and type of control system. A steam unit that is operating at full valve but not at full capability will have no frequency response even though it appears to have additional capability above its current output. These issues may require responsible entities to develop one or more of the following:

- -N~~n~~ew unit commitment processes

Formatted: List Bullet, No bullets or numbering

Formatted

- ~~,~~ N~~n~~ew operating guidelines~~,~~
- ~~-~~Additional tools for operators
- ~~, and~~ more consistent governor settings~~.~~

The agreement among the participant responsible entities for the FRSG should address the minimum reserve requirement for the group, the allocation of reserve among members, and reporting and record keeping for regulatory compliance. The FRSGs minimum reserve requirement should be conservative to allow for conditions, such as a unit-tripping or transmission contingencies, that could affect members' ability to supply FRR to each other. The agreement should clearly state each member's portion of the total reserve requirement as well as the methodology used to calculate the member's reserve responsibility.

Also, the agreement should consider how the information is shared in real-time based on tools created for the operators.

NERC Reliability Standard BAL-003~~-2~~ allows BAs to meet their FROs by electing to form FRSGs. Attachment A of that same standard specifies that an FRSG may calculate their frequency response measure (FRM) performance in one of two ways; calculate a group NIA or aggregate the group response to all events in the reporting year as one of the two following options:

- Single FRS Form 2 utilizing a group NI_A for each event and an accompanying FRS form 1 for the FRSG
- A summary spreadsheet that contains the sum of each participant's individual event performance and an accompanying FRS Form 1 for the FRSG

This section of the guideline is intended to provide recommended practices to consider for BAs when performing the following actions:

- Establishing FRSGs
- Calculating FRSG FRM performance

The Generator Governor Frequency Response Advisory[7] issued notice to industry on the importance of resource configurations for governors and control systems to allow for the provision of primary frequency response. Subsequently, a specific description of practices necessary for resources to provide primary frequency control, including the coordination of turbine controls with plant outer loop controls and an explanation of the different components of frequency response, can be found in the *Primary Frequency Control Reliability Guideline*[8].

Existing BAL-003~~-2~~ Forms 1 and 2 provide short-term bilateral transactions of frequency response and do not require the formal establishment and registration of a long-term FRSG, so these arrangements are not

Formatted

Formatted: Character scale: 100%

Formatted

Formatted

Formatted

Formatted: List Bullet

[7] https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/2015%20Alerts/NERC%20Alert%20A-2015-02-05-01%20Generator%20Governor%20Frequency%20Response.pdf

[8] https://www.nerc.com/comm/OC/RS_GOP_Survey_DL/PFC_Reliability_Guideline_rev20190501_v2_final.pdf

addressed by this guideline. This section of the guideline focuses solely on establishment and operating practice guidelines for a multiparty FRSG.

Establishment/Structure of an FRSG

Certain minimum criteria should apply to all candidate FRSGs prior to registration and establishment. FRSG registration is necessary to provide ERO staff with sufficient information to modify the FRSG's FRO for each operating year. The FRSG FRO is the aggregate of member BAs' FROs, including the information in the tables used in Form 1, and determine unique FRSG codes (substitutes for the BA codes normally used) for use in summary Form 1.

An FRSG should have a formal agreement among its members in place prior to registration. Depending on the structure and characteristics of the member BAs, the FRSG agreement among the participant responsible entities for the FRSG may need to address the following:

- Minimum frequency-responsive reserve requirement for the group
- Each member's portion of the total frequency-responsive reserve requirement
- Requirements, if applicable, of specific resources to provide frequency response
- Members' reporting, record keeping, and accountability for regulatory compliance
- Provisions for each member's alternative minimum frequency-responsive reserve requirements in identified areas in the event of emergency scenarios, such as an islanding event
- Methodology used to calculate the member's frequency-responsive reserve responsibility
- How information is shared among members in real-time
- Tools for operators to have situational awareness of frequency-responsive reserves of the FRSG
- When and how to bring more frequency-responsive reserves to bear (e.g. conservative operations, periods of low inertia)

FRSGs must be pre-arranged and member participation must coincide with the BAL-003~~-2~~ operating year (i.e., December 1 through November 30 of the following year). Any member of the BA's minimum period of participation must be one BAL-003~~-2~~ operational year. Partial BAL-003~~-2~~ operating year participation is not allowed. Per-event participation with other BAs is a bilateral transaction and is not considered a formation of an FRSG. Like bilateral transactions, FRSGs can only be established prior to the analysis period, and no BA may be a member of more than one FRSG at any given time.

All FRSG member BAs must be in the same Interconnection. An FRSG can be noncontiguous, but each FRSG may be subject to a transmission security review by potentially affected BAs and Transmission Operators. In some cases, a transmission security review by potentially affected BAs and Transmission Operators may be necessary for contiguous FRSGs if, for example, parallel flows caused by individual members' responses may impact other BAs or Transmission Operators.

Operations of a FRSG

FRSGs and their constituent BAs should attempt to fully respond to each event in the BAL-003~~-2~~ operating year.

FRSG who calculate an FRSG NI_A, should properly time-align tie line data to account for data latency and difference in member BAs’ EMS scan rates. To the extent possible, this adjustment should be reflected in real-time data provided to operators. The adjustment times for each alignment should be reviewed at least annually to determine if a different amount of adjustment is needed.

The FRSGs minimum frequency-responsive reserve requirement should be conservative to allow for conditions, such as a unit-tripping or transmission contingencies, that could affect members’ ability to supply frequency-responsive reserve to each other.

Although an explicit frequency-responsive reserve requirement is not necessary in every case, the FRSG should account for frequency-responsive reserves among its members in real-time. Members of an FRSG should consider including such provisions in their organizational documents.

Analysis/Reporting

FRSG member BAs must select an entity to report summary information for the FRSG to NERC. As noted above, FRSG reporting is done according to Attachment A in BAL-003~~-2~~.

For tie line data not already time-aligned, the FRSG and its member BAs should properly time-align prior to completing the aggregate FRS Form 2s to account for data latency and difference in member BAs’ EMS scan rates.

Changes to Form 1 necessary to allow use of appropriate adjustments of FRM will be referred to NERC staff for development and implementation and those changes will be routed through the appropriate NERC committees for any vetting/validation needed.

Regulation Reserve Sharing Group

A regulation RSG is a group whose members consist of two or more BAs that collectively maintain, allocate, and supply the regulating reserve required for all member BAs to use in meeting applicable regulating standards.

A regulation RSG may be used to satisfy the Control Performance Standard (CPS) requirement in BAL-001~~-2~~. Sharing of regulating reserve will require real-time data sharing and dynamic transfers[9] between members. The agreement among the participant BAs of the regulation RSG should contain the maximum amount of regulation to be exchanged and the medium used to communicate the regulation to be shared. The agreement should assign responsibility for arranging transmission service and posting schedules.

[9] For a more detailed explanation of the implementation of dynamic transfers in general and for regulation sharing (discussed as supplemental regulation in the document) specifically, see the Dynamic Transfer Reference Guidelines reference document~~ in the *NERC Operating Manual*~~. ~~This~~ This document can be found at https://www.nerc.com/comm/OC/ReferenceDocumentsDL/Dynamic_Transfer_Reference_Document_v4.pdf ~~http://www.nerc.com/comm/OC/Pages/Operating-Manual.aspx~~

Formatted: Left

Field Code Changed

Regulation magnitudes may at times be limited due to resource availability or transmission constraints, so the regulation RSG agreement should include mechanisms to provide for such restrictions. If a regulation RSG has many members, the members may need central data sharing to enable communication in Real-time, as well as more complex definitions of transmission paths among members and mechanisms to address transmission path limitations. Record keeping for the regulation RSG will primarily be energy schedule records (E-Tags) and Open Access Same-Time Information System postings that allow energy flow between members. The regulation RSG agreement should also have mechanisms to settle imbalances and limit the amounts of imbalances between members.

Operating Reserve Interaction

The responsible entity's Operating Reserves definition should include three general categories: FRR, regulating reserve, and contingency reserve. NERC Reliability Standards primarily govern the deployment of these three categories.

Load Forecast Error

The BA Operating Reserve projections should consider load forecast error when establishing reserve levels. The following is a list of considerations that may be evaluated. These may change from day to day, from season to season, and should be included in the commitment of resources.

- Weather forecast
- Seasonal temperature variations
- Model error
- Speed of weather event

Fuel Constraints

Once resources are identified, a second review should consider fuel constraints to determine if any limitations generation ~~exits~~exist. The following is a list of considerations that may be evaluated. These may change from day to day, from season to season, and should be included as part of a BA's projection of operating reserves and contingency reserves.

- Delivery Limitations such as Operational Flow Orders – (OFOs)
- Availability of fuel (e.g. weather impacts, market, ability to purchase)
- Transportation considerations
- Fuel supply (e.g. size of coal pile, amount of fuel oil, water reserves)
- Variability (e.g. solar and wind)
- Energy Storage Resources
  - Energy Storage Duration
  - State of Charge

Formatted: List Bullet 2

Deliverability of Reserves

Deliverability of reserves is an important consideration. If reserves are undeliverable across the BA, then the BA is at increased risk of not complying with BAL-002~~-3~~. As transmission outages occur, the ability to deliver energy across the BA changes. A BA should consider any restrictions or limitations that may reduce generation capability as part of their operating and contingency reserve projections. The following may impact the deliverability of reserves:

- Transmission availability
- Transmission constraints
- Shape/size of BA
- RSG Considerations –
  - Ability to deliver with available transmission
  - Connection through an intermediate member
  - Operating procedures

Unit Commitment

When developing plans and addressing the needs of a BA or an RSG to ~~reliability~~ reliably meet the demands of customers, unit commitment is a key component of successfully planning and ensuring that the needed generation is available in real-time operations. When dispatching the system, the BA operator should coordinate and consider any impacts to operating reserves and contingency reserves. The following is a list of considerations that may be included in the unit commitment process:

- Unit start-up time
- Available personnel
- Maintenance activities
- Environmental limitations:
  - Drought constraints
  - Intake constraints
  - Weather Conditions (Temperatures, cloud coverage, wind speeds, precipitation and humidity)
- Hydrothermal limitations
- Battery Management
- Fuel Supply
- Renewable Forecast Error

For all imbalances occurring on its power system, the responsible entity will use its reserve that is addressed by the following four-step process.

Step 1: Arrest Frequency Change

The first step in recovery is to arrest the frequency change caused by the imbalance. In most circumstances, this arresting action is performed automatically by the frequency response of generators and load on the Interconnection within the first few seconds of the imbalance. If there is insufficient frequency response or FRR to arrest a frequency decline, the Interconnection frequency will reach underfrequency relay trip points before any of the other steps can be initiated. Frequency response is therefore the most important of the required responses and FRR is the most important of the reserves.

Step 2: Contingency Reserve Deployment- Returning Frequency to its Normal Range

The second step in the recovery process is to return the frequency to its normal range. Again, this is usually accomplished by applying FRR or regulating reserve in most circumstances for small imbalances, and the CPS1 portion of BAL-001~~-2~~ governs the timeliness of the aggregate of such recoveries. The timeliness of the recovery from larger imbalances is governed by BAL-002~~-2~~ as well as CPS1. For large, sudden imbalances due to loss of generation, this is usually accomplished by applying contingency reserve. Current rules in North America require the completion of this step within a fixed time, 15 minutes in most cases. The remainder of the operating reserve not used for the frequency response is available to complete this return to the normal frequency range.

Step 3: Restore Frequency Responsive Reserve

The third step in the recovery process is the restoration of the FRR. Restoration of FRR is what indicates the Interconnection is secure and, in a position, to survive the next imbalance or disturbance. The timeliness of achieving this condition affects the risk that the Interconnection faces.

Step 4: Operating Reserves Conversion–Restoring Regulating Reserve or Contingency Reserve

The fourth step is to restore any Regulating or Contingency Reserves that has been deployed to ensure that the Interconnection can recover from the next imbalance or disturbance within an appropriate time.

Interaction

This four-step process demonstrates that the Operating Reserve components (i.e. FRR, regulating reserve and contingency reserve) are used in conjunction with one another, do not function in isolation, are always interacting, and often overlap due to timing requirements.

The Operating Reserve components can be distinguished from each other by the response time it takes to convert the reserve capacity into deliverable energy. The differences in response time allow the reserves to be utilized from the reserve with the fastest response (i.e. FRR) to the reserve with the slowest response time (i.e., Contingency Reserve). The deployment of regulating reserve in some scenarios can lead to the restoration of FRR. The deployment of Contingency Reserve in some scenarios will assist in the restoration of FRR and regulating reserve.

FRR is a “sub-minute” reserve product, and governor response provides it in most cases. Typically, Regulating Reserves and Contingency Reserves cannot be deployed in the time frame to assist in keeping frequency above underfrequency relay settings. Regulating Reserve usually does not respond quickly enough to be observable in the FRM. Contingency Reserves most often takes more than a minute and can take up to 15 minutes to deploy following the start of the contingency.

Regulating Reserves are often thought of as a “minute plus” reserve product. If it is deployed by any responsible entity in an Interconnection in a direction that supports pushing frequency towards 60 Hz, it will help restore FRR within the Interconnection.

For resource losses, contingency reserve activated by the contingent responsible entity often takes a few minutes to begin to be deployed. As its deployment progresses over time and frequency approaches 60 Hz, there will be some restoration of FRR and regulating reserve for the contingent responsible entity. A noncontingent responsible entity’s FRR will tend to be restored with the deployment of the contingent responsible entity’s contingency reserve as well.

For a responsible entity in a multiple responsible entity Interconnection, it may coincidentally need to deploy FRR for a load greater than generation imbalance within its Interconnection at the same time that it needs to deploy its regulating reserve in the upward direction. It may also experience its MSSC, requiring the deployment of contingency reserve while the need for FRR and regulating reserve are at a maximum. The responsible entity should plan its reserve allocations to be compliant with the NERC Reliability Standards in such a coincidental scenario.

Interconnections with only one responsible entity are unique in that only they can correct their system frequency. FRR will always be deployed automatically and coincidentally when contingency reserve needs to be deployed for a large contingency. FRR and contingency reserve are inherently co-mingled, and together they must at least equal MSSC. As with a multiple responsible entity Interconnection, regulating reserve needs to be separate from FRR and contingency reserve.

There is an additional characteristic of reserve enabling the reserve categories to be ordered. Operating Reserve categories are partially substitutable for one another. FRR is the only type of reserve that could be used as the exclusive reserve that would enable an Interconnection to operate reliably. Attempts to operate an Interconnection without FRR would result eventually in the activation of frequency relays. As long as the amount of FRR available is greater than the energy imbalance on the Interconnection, ~~the~~ Interconnection ~~will remain reliable~~reliability will be supported to arrest frequency deviations.

The difficulty with operating an Interconnection with only FRR is that FRR is limited in the total amount available. FRR will arrest the frequency change but will not restore frequency to its normal range, leaving the Interconnection vulnerable to the next contingency. The FRR provided by load damping is limited and the additional FRR provided by governor response is relatively expensive to provide in large quantities.

Regulating reserve is a reserve that can be substituted on a limited basis for FRR. When regulating reserve is substituted for FRR, the regulating reserve restores the FRR by returning governor response to the plants and replacing it with dispatched energy. As frequency is returned to normal range, the FRR is restored and available for reuse. The amount of regulating reserve that can be substituted for frequency response is determined by the difference between the FRR required to manage the largest imbalance that could occur on the Interconnection and the FRR that could be required in a period shorter than the response time for regulating reserve. This ensures there is sufficient FRR available to manage any imbalance occurring before there is time to replace the FRR being used with regulating reserve. Also, it extends the effective amount of FRR available, allowing the Interconnection to operate with less governor response because the amount of load damping is not easily modified.

In all cases, the maximum imbalance that is unmanageable by supplementing FRR with regulating reserve (when only FRR and regulating reserve are available) determines the minimum FRR required. In addition, the sum of the FRR and regulating reserve should exceed the largest energy imbalance occurring on the Interconnection. Thus, when substituting regulating reserve for FRR the total amount of the FRR and regulating reserve should be equal to or exceed the amount of FRR when it is used alone.

Contingency Reserves can further supplement regulating reserve and FRR and can be manually dispatched to restore any FRR currently being used to respond to declining frequency. When dispatched, it restores both FRR and regulating reserve, making them available for reuse. Therefore, contingency reserve can be substituted for a portion of the regulating reserve that could be substituted for FRR. When this substitution is implemented, the sum of the FRR, regulating reserve, and contingency reserve should exceed the sum of regulating reserve and FRR if contingency reserve is not used.

This illustrates a power system that uses many levels of substitution to improve economic efficiency and reliability. Regulating Reserve is substituted for FRR as determined by reliability needs; contingency reserve is substituted for regulating reserve as determined by reliability needs. Reliability limits for these substitutions can be quantified with a set of inequalities:

$$\boldsymbol{FRR + RRO \geq FRRO} \qquad \textbf{\textit{Inequality (1)}}$$

$$\boldsymbol{FRR + RR + CR \geq FRR + RRO} \qquad \textbf{\textit{Inequality (2)}}$$

FRRO = FRO, equal to MW of FRR when only FRR is used.

FRR = MW of FRR when another service is substituted for FRR.

RRO = MW of regulating reserve (RR) when nothing is substituted for RR.

RR = MW of RR when another service is substituted for RR.

CR = MW of Contingency Reserves ~~R~~ when nothing is substituted for Contingency Reserves~~R~~.

Both inequalities represent the total required reserve on both sides of the inequality.

These inequalities are used to determine the FRO in BAL-003~~-2~~ as adjusted by the base frequency error profile that results from reserve substitution. In addition, the contingency reserve requirement in R2 of BAL-002~~-2~~ determines the minimum CR when it is not in use for recovery, but it does not require that the reserve used to meet the requirement exclude FRR or regulating reserve. Since regulating reserve is unique to each responsible entity and can be determined only by evaluating the characteristics of their load and generation resources, a minimum regulating reserve obligation is not specified in BAL-001~~-2~~. The variations of substitution of reserve as shown above suggests that the best test for reserve adequacy is whether the total capability of resources designated to provide regulating reserve, contingency reserve, and FRR is at least equal to the amount required to meet all reserve requirements concurrently.

Additionally, during the deployment of reserves in real-time, there are only limited ways to determine whether a responsible entity is holding adequate reserves. This determination can only be based on a prospective look during operations planning when there are no deviations from the expected deployment of reserves. Because this is the case, it is also important for the responsible entity to have a feedback mechanism included in its evaluations of reserve to include the uncertainties experienced during actual reserve usage. A reserve-monitoring tool could accomplish this.

The calculation of reserve levels (including FRR, regulating reserve, and contingency reserve) begins with the calculation of the amount of each type of reserve available from each resource providing any of these three types of Operating Reserves. Once the individual resource reserve contributions have been calculated, the responsible entity's total reserves by category can be determined by the sum of the reserve contributions for all contributing resources.

The calculation for these three types of reserves (i.e., FRR, regulating reserve, and contingency reserve) may not be supported in some EMSs because the FRR calculation and the interaction between reserves requires additional data not currently maintained in many EMSs. Additional data required to support the FRR calculation includes, but is not limited to, unit droop, dead-band settings, and Interconnection underfrequency load shedding (UFLS) frequency limits. Additional data may be required for other types of resources.

Finally, any calculation of the total amount of reserve and the amount in each category can change with a change in output/use of any of the resources that provide reserve for the responsible entity. For example, dispatch of contingency reserve from a resource could also affect the FRR or regulating reserve that is available from that same resource by moving the operating point of the resource nearer to one of the resource's operating limits. This could result in a reduction of one of the other reserve types in addition to the reduction in the amount of contingency reserve resulting from the dispatch. This dynamic reserve interaction should be included in operations planning and the tools used to provide the system operator with the best information.

Related Documents and Links:

NERC Reliability and Security Technical Committee Charter

NERC Operating Manual

Use of Frequency Response Metrics to Assess the Planning and Operating Requirements for Reliable Integration of Variable Renewable Generation, Key Findings

Field Code Changed

Cited Documents

NERC Alert A-2015-02-05-01 Generator Governor Frequency Response

Primary Frequency Control Reliability Guideline

NERC Standard BAL-003~~-2~~

FERC Final Order on Third-Party Provision of Primary Frequency Response Service - FERC Docket RM15-2-000 Order No. 819

Revision History

Date	Version Number	Reason/Comments
10/18/2013	1.0	Initial Version – “Operating Reserve Management”
12/13/2017	2.0	Revised to include more detailed description of FRSG
9/13/2020	3.0	3-year review and revisions
4/15/2021	3.0	Industry Comments addressed

Organization(s)	Page #	Line / Paragraph	Comment	Proposed Change	NERC Response
Arizona Public Service, Balancing Authority & NERC Regulatory Compliance	18	626	Consider including proposed change	State of Charge, Energy storage duration; Amount of Battery charge and length of delivery.	Change Accepted
Arizona Public Service, Balancing Authority & NERC Regulatory Compliance	19	640	Consider including proposed change	Weather Conditions (high/low temperatures, cloud coverage, wind speed, preciptiation and humidity).	Change Accepted
Arizona Public Service, Balancing Authority & NERC Regulatory Compliance	19	640	Consider including proposed change	Battery Management, state of charge	Change Accepted
Arizona Public Service, Balancing Authority & NERC Regulatory Compliance	19	640	Consider including proposed change	Fuel Supply	Change Accepted
California ISO	7	System Operator Roles: RC Operator	For "Redistribute reserves" - what is meant by redistribute reserves? Is it moving reserves from one BA to another? If so, how would 10 minute response be coordinated? How is that transaction arranged where ancillary markets are in effect?		Wording Modified for clarity
California ISO	7	System Operator Roles: RC Operator	For "Shed Load where appropriate if the BA or TOP cannot withstand the next Contingency" - How does the RC determine that the BA can withstand the next contingency? What are the parameters? What are the required actions of the RC after the recovery period has ended if the BA has not taken sufficient action to recover reserves?		This is RC dependent and is not in scope of this document.
Bonneville Power Administration	8	258 - 259	In the previous version of this guideline, FRR was to be excluded from minimum CR amounts. In this guideline, they can be included in minimum CR amounts.	Can the guideline explain the change in this thinking? Also, please consider clarifying that deployment of contingency reserves is a set point change to a specific MW amount of lost energy, not just a regulation response to ACE, which is effected by many variables including frequency response and its interaction with the frequency bias of the BA.	Comment is unclear. Version 2 of the guideline stated the following "the Contingency Reserve Requirement in R2 of BAL-002-2 determines the minimum CR when it is not in use for recovery but it **does not require that the reserve used to meet the requirement exclude frequency responsive reserve or Regulating Reserve.** " There a number of factors that affect the ACE response, during a contingency event that influced the overall response. Contingency reserves is not limited to a setpoint change equivalant to a specific MW of lost energy. This includes but is not limited to the amount of frequency response of physical generators, the AGC response of generation within a BA, load variations, inverter based frequency response, operator actions, etc.. all play a part in the response to ACE deviations. This specific response seems to be directed toward the specific implemenation of contingency reserve managment with the BA.
Bonneville Power Administration	17 - 18	593 - 600	The Load Forecast Error section is missing considerations that need to be made for demand response, unconventional load types (such as arc furnaces and server farms), and incorporating how the system operator utilizes the Load Forecast.	Incorporate more of the operating impacts that BA's see or should consider, including demand response, unconventional load types (such as arc furnaces and server farms), and incorporating how the system operator utilizes the Load Forecast.	These loads should inherently be included in the load forecast and thus should already be included if running. This appears to be a BA specific issue that needs to be addressed with day ahead schedule requirements.
Bonneville Power Administration	18	602 - 611	VER Forecast/Scheduling Error is the largest driver for BPA's balancing/regulating reserve needs, and yet it is missing from this document. Briefly mentioning "Variability" in the Fuel Constraints section is not enough.	This document should include a separate VER Forecast/Scheduling Error section. If omitted, it will be a major deficit of this guideline.	Forecasting should be address in a separate guidelines. The SPIDER and the IRPTF have guidelines that cover the associated topics on VER. Please refer to these documents for additional details.
Bonneville Power Administration	18	N/A	Coincidental error evaluation is missing from the document.	This document should include a Coincidental Error section, detailing how the coincidental errors of load and generation should be considered when evaluating reserve levels to capture the coincidental and non-coincidental use of reserves.	Concept is addressed at the macro level to allow BA's to determine needs and impacts based on BA generation resources available.
Bonneville Power Administration		General Comments	While there appears to be more depth on Frequency Responsive Reserves and Contingency Reserves, which is valuable, the document needs more depth in the other areas.	Suggest adding depth to the areas that are only lightly touched.	Comments are to vauge and not actionable
Shannon V. Mickens (SPP)		115	We ask that the drafting team provide clarity on what the expectations are for the term **Other Reserve Resources** definiton and inclusion in the Figure 1.1 diagram.	Provide examples of the type of resources that meet this definition and time frames applicable in the Figure 1.1.	Edited to address comment
Shannon V. Mickens (SPP)		118	We ask that the drafting team provide clarity on what the expectations are for the use of the term **Planning Reserve** definition.	Proivde an equation/calculation to show the relavance and expecation of the definition.	Definition covers calculation method as suggested.
Shannon V. Mickens (SPP)		137-138	The diagram doesn't align with the defintions mentioned in the section above. We are asking the drafting team to provide clarity by showing how the terms and their definitions align with the Figure 1.1 diagram.	Create a mapping effort to align the defnitions and diagram.	Definitions reflect diagram and layout

Shannon V. Mickens (SPP)		189	We suggest the phrase should read " It is important for the system operator to know"	include "to" in the sentence	Change Accepted
Shannon V. Mickens (SPP)		201	We suggest the sentence should read " ensure the proper EES is called when a reserve short fall is forecasted or experienced"	Replace "issue" with "ensure" in the sentence	Change Accepted
Shannon V. Mickens (SPP)		217	We ask that the drafting team provide clarity to the definition for the term **Redistribute reserves** as well as provide supporting language stating how the RC would implement this definition into their roles and responsibilities.	Provide a definiton for this term and/or provide an example on how this method would be implemented from an RC perspective.	Clarification Added to Document
Shannon V. Mickens (SPP)		403	We suggest the phrase read "meet the requirements of BAL-001-2, BAL-002-3 and BAL-003-2"	Replace "BAL-003--2" with "BAL-003-2"	Change Accepted - removed version reference
Shannon V. Mickens (SPP)		411	We suggest the phrase read "The NERC Reliability Standard BAL-002-3 allows BAs"	Replace "BAL-002-2" with "BAL-002-3"	Change Accepted - removed version reference
Shannon V. Mickens (SPP)		415	We suggest the phrase should read "some smaller BAs could be required to withhold 20%"	Replace " BA's" with "BAs"	Change Accepted
Shannon V. Mickens (SPP)		429	We suggest the phrase read "within the Contingency Event Recovery Period as defined in BAL-002-3."	Relace "60-second period" with "Contingency Event Recovery Period", add "in", to the phrase Replace "BAL-002-2" with "BAL-002-3"	Edited to address comment
Shannon V. Mickens (SPP)		471-476	We suggest that this section be put in bullet format		Edited to address comment
Shannon V. Mickens (SPP)		541	we suggest the phrase should read "Operations of an FRSG"	Replace "a" with "an"	No change required
Shannon V. Mickens (SPP)		604	We suggest the phrase should read "limitation to generation exist"	Replace "exits" with "exist"	Change Accepted
Shannon V. Mickens (SPP)		628	We suggest the phrase should read "BA or an RSG to reliably meet"	Relpace "reliability" with "reliably"	Change Accepted
Shannon V. Mickens (SPP)		633-639	We suggest adding Renewable Forecast Error to the section for consideration for unit commitment.		Edited to address comment
Shannon V. Mickens (SPP)		656	We suggest the phrase read "larger imbalances is governed by BAL-002-3"	Replace "BAL-002-2" with "BAL-002-3"	Change Accepted - removed version reference
Shannon V. Mickens (SPP)		734	We suggest the phrase read "the maximum imbalance that is unmanageable"	add "is" to the phrase	Change Accepted
Shannon V. Mickens (SPP)		760	We suggest the phrase read "the contingency reserve requirement in R2 of BAL-002-3 determines the minimum CR"	Replace "BAL-002-2" with "BAL-002-3"	Change Accepted - removed version reference
ReliabilityFirst	Generic		The use of synonymous terms like Mandatory Standards, NERC Standards, Reliability Standards are often used interchangeably throughout this document.	It is recommend to consistently use one defined term throughout this document.	Edited to address comment
ReliabilityFirst	Generic		ReliabilityFirst has a regional specific Reliability Standard, BAL-502-RF-03, that pertains to guidance around performance of a planning resource adequacy analysis. It may be helpful to use this as a reference for considerations when performing this type of planning assessment.		Edited to address comment
ReliabilityFirst	5	Figure 1.1	This table is very helpful with providing additional context regarding the terms identified in the Definitions section of the document. It would be helpful to add some verbiage associated with the figure to explain the purpose and the differences between terms.	As a high-level example......The various terms associated with this guideline document represent distinct conditions pertaining to reserve management and assessment. Figure 1.1 clearly shows the differing types of reserves between the operating and planning environment and potential availability based on time or generating unit operational status.	Change Accepted
ReliabilityFirst	6	170-171	Define the acronym EEA	Change 'EEA' to 'Energy Emergency Alert (EEA)' or define EEA in the definitions section of this guideline document.	Defined in the definitions section under Contingency Reserves.
ReliabilityFirst	6	184	Reader could interpret this description as only a single evaluation is recommended. Evaluations should be performed on a periodic basis and solicit feedback from participants.	Consider periodic evaluations of the effectiveness of the Operating Reserve program, allow feedback from participants in the program, and incorporate lessons learned.'	Change Accepted
ReliabilityFirst	7	189	Wording change, missing the word 'to'	It is important for the system operator to know...'	Change Accepted
ReliabilityFirst	9	261	Recommended to replace 'reliability requirements' with Reliability Standards or similar term.		Edited to address comment
ReliabilityFirst	9	274	It may be useful to also specifically mention hybrid facilities as well		Edited to address comment
ReliabilityFirst	11	345	Replace 'normal' with 'nominal'		Thank you for comment
ReliabilityFirst	12	403	Minor typo correction	Change 'BAL-003--2' to 'BAL-003-2'	Change Accepted - removed version reference
ReliabilityFirst	13	421	Insert 'NERC'	.....the NERC compliance requirement is met.'	Change Accepted
ReliabilityFirst	19	653	Replace 'normal' with 'nominal'		Thank you for comment
ReliabilityFirst	19	654	Define "small" - It may be helpful to provide additional context related to the term small.		This is dependent on interconnect size and should be managed based on interconnection need. Guideline is written to allow flexibility of specific regions.

ReliabilityFirst	19	656	Define "larger" - It may be helpful to provide additional context related to the term larger.		This is dependent on interconnect size and should be managed based on interconnection need. Guideline is written to allow flexibility of specific regions.
ReliabilityFirst	21	725	Replace 'normal' with 'nominal'		Thank you for comment
ReliabilityFirst	21	734	Wording change, add the word 'is'	In all cases, the maximum imbalance that is unmanageable…'	Change Accepted
PJM	6	167	PJM requests clarification and examples for "Bottoming out conditions"	A proposed change may be requested following clarification of "Bottoming out conditions"	Definition added to document
PJM	7	217	PJM requests clarification and examples for "Redistribute Reserves"	A proposed change may be requested following clarification of "Redistribute reserves"	Clarification Added to Document
PJM	8, 9	256-262	Reserve amounts set aside as frequency responsive include unit governor reserves. These local responses are independent of control center control. If the unit is not operating at maximum output, the unit should be capable of providing frequency response. Due to the interactions of frequency reserves, these are included in the available minimum contingency reserve amounts in Interconnections composed of more than one responsible entity. At any given time, a unit may also be loaded to maximum output and unavailable to meet the reliability requirements associated with frequency response and contingency reserves.	Reserve amounts set aside as frequency responsive include unit governor reserves. These local unit governor responses are independent of control center control. A unit may or may not be able to provide frequency reserves or contingency reserves dependent on if it is operating at maximum output. If the unit is not operating at maximum output, the unit should be capable of providing frequency response. Due to the interactions of frequency reserves, these frequency reserves are included in the available minimum contingency reserve amounts in Interconnections composed of more than one responsible entity. At any given time, a unit may instead be loaded to maximum output and, if so, unavailable to meet the reliability requirements associated with frequency response and contingency reserves.	Edited to address comments
PJM	11	349	PJM requests the meaning of secondary reserves as written within this Reliability Guideline.	A proposed change may be requested following clarification of secondary reserves as written in this Guideline	Secondary reserves are terms used in a referenced report
PJM	20	708, 709	As with a multiple responsible entity Interconnection, regulating reserve needs to be separate from FRR and contingency reserve.	As with a multiple responsible entity Interconnection, although a single unit may provide different reserve types, all regulating reserve across all units needs to be separate from FRR and contingency reserve.	Thank you for comment
PJM	20	714, 715, 716	As long as the amount of FRR available is greater than the energy imbalance on the Interconnection, the Interconnection will remain reliable.	"FRR alone does not ensure an Interconnection will remain reliable. However, FRR alone does greatly improve an Interconnection's reliability." Other operations that may occur following FRR deployment also ensure reliability. A proposed change may include the need for automatic generation control and other operator manual control actions to restore energy balance and CR.	Edited to address comment

Edison Electric Institue (Submitted by Mark Gray)	1	1	General Comments: EEI appreciates the opportunity to comment on Version 3 of this Reliability Guideline and suggests the following revisions to further enhance this document. NERC Reliability Guidelines should have a consistent look, feel, and contain certain elements and formatting, including: 1.Cover page with Date Approved and Revision No. 2.Table of Contents 3.Preface 4.Consistent Preamble 5.Executive Summary that includes: a.High level overview of the Guideline 6.Introduction a.Purpose Statement b.Background (if needed) c.How the document is to be used d.Other useful information that might assist the reader. 7.Body of the Guideline 8.Appendix a.Reference and ancillary documents where needed (e.g., Document specific definitions (not NERC GOT terms), supportive examples, supporting criteria, useful tools, etc.) b.Metrics The use of NERC Glossary of Terms (GOT) within NERC Reliability Guidelines should be capitalized to signal to the reader they are defined NERC GOT. Within this Reliability Guideline, these terms are inconsistently capitalized (e.g., Contingency Reserve, Operating Reserve, etc.). EEI recommends that all NERC GOT are	Use consistent format as suggested. Follow NERC convention regarding Glossary of Terms. Do not republish approved terms.	Document was reviewed by NERC Publications prior to industry comment. Will followup with NERC Publilcaitons to address format in future revisions.
Edison Electric Institue (Submitted by Mark Gray)	3, 4	69 to 135	Page 3 & 4, Lines 69 to 135: NERC GOT should not be duplicated in NERC documents, including NERC Reliability Guidelines. Revisions to Guidelines and the NERC GOT can occur on different cycles and definitions contained outside of the NERC GOT could become outdated and potentially create confusion. Additionally, if it is necessary to include definitions for terms not contained in the NERC GOT to aid the reader in their understanding of the Reliability Guideline, EEI supports the inclusion of document specific terms to be identified and defined and recommends placing those terms in italics throughout the Reliability Guideline but do not capitalize those terms since they are not NERC GOT.	Recommendation: Remove all NERC GOT definitions from this Reliability Guideline. Only include non-NERC GOT definitions in the definition section of this document.	Thank you for comment
Edison Electric Institue (Submitted by Mark Gray)	2	2	Footnote 2 is a dead link	Fix link	Removed reference
Edison Electric Institue (Submitted by Mark Gray)	3	70 to 71	Lines 70 to 71 contain a lead in statement to the Definition section. EEI suggests modifying this lead in statement to something like the following: When reading this Reliability Guideline, the reader should note that all terms contained in the NERC Glossary of Terms (footnote a link to the GOT) and used in this Guideline are capitalized. In addition to those terms some additional terms have been defined and provided below to assist the reader. These terms will be shown in Italic to distinguish them from those defined and approved by NERC.	Suggested edits	Edited to address comments
Edison Electric Institue (Submitted by Mark Gray)	4	116	Figure 1.1 would provide greater usefulness if it were on the same page as the definition that references the figure.	Suggest moving figure	Figure 1 references multiple definitions defined in the definitions section of the document. Not possible to place all definitions and Figure on same page.

Edison Electric Institue (Submitted by Mark Gray)	6	167	On lines 163 to 165 it states: "Each responsible entity should consider the types of resources and the associated portion of their capacity capable of reducing the BA's area control error (ACE) in either direction in response to each of the following:" after which a list of 7 bulleted conditions is provided. On line 167 the term "Bottoming out conditions" is listed. This term is undefined and potentially unclear. We recommend that it be defined.	Suggested edits	Definition added to document
Edison Electric Institue (Submitted by Mark Gray)	6	170	EEI suggests adding "Load management procedures in effect" after EEA 2 or possibly footnoting the Reliability Standard EOP-011 since this standard defines the various Energy Emergency Alert levels.	Suggested edits	Footnote to EOP-11 added
Edison Electric Institue (Submitted by Mark Gray)	6	171	EEI suggests adding "Firm load interruption imminent or in progress" after EEA 3 or possibly footnoting the Reliability Standard EOP-011 since this standard defines the various Energy Emergency Alert levels.	Suggested edits	Footnote to EOP-11 added
Edison Electric Institue (Submitted by Mark Gray)	7	193	When considering abnormal system conditions, a 2-to-6 hour window may be too short. Consider removing or expanding the window portion of this bullet.	Suggested edits	Expanded window of situation awareness is covered in next bullet.
Edison Electric Institue (Submitted by Mark Gray)	8	251	EEI suggests changing the referenced Reliability Standard BAL-002-3 to BAL-002. This change will ensure that if BAL-002 changes before this Reliability Guideline is updated the associated guideline will be unaffected.	Suggested edits	Change Accepted - removed version reference
Edison Electric Institue (Submitted by Mark Gray)	10	296 to 298	EEI suggests the following modification to the current language: ~~For a r~~Responsible entit**ies** should **consider** leverag**ing** their Replacement Reserves to meet the Contingency Reserve Restoration Period, preplanning and training of system operators may be required. Actions like the following ~~may~~ **should** be considered:	Suggested edits	Edited to address comments
Edison Electric Institue (Submitted by Mark Gray)	10	320	Consideration should be made to changing BAL-003-2 to BAL-003. Currently, this standard is being revised through Project 2017-01, Phase 2. For this reason, efforts should be made to address FRR in the context of BAL-003 in a manner that might allow the guideline to remain effective even after BAL-003-3 is approved. Additionally, it seems unnecessary to add a footnote hyperlink to approved NERC Reliability Standards within a NERC Reliability Guideline.	Suggested edits	Change Accepted - removed version reference
Edison Electric Institue (Submitted by Mark Gray)	12	403	Suggest changing the references to BAL-001-2, BAL-002-3, and BAL-003-2 to simply BAL-001, BAL-002 and BAL-003.	Suggested edits	Change Accepted - removed version reference
Edison Electric Institue (Submitted by Mark Gray)	13	411	Suggest changing the reference to BAL-002-3 to simply BAL-002	Suggested edits	Change Accepted - removed version reference
Edison Electric Institue (Submitted by Mark Gray)	13	429	Suggest changing the reference to BAL-002-3 to simply BAL-002	Suggested edits	Change Accepted - removed version reference
Edison Electric Institue (Submitted by Mark Gray)	14	481	Suggest changing the reference to BAL-003-2 to simply BAL-003.	Suggested edits	Change Accepted - removed version reference
Edison Electric Institue (Submitted by Mark Gray)	16	528	Suggest changing the reference to BAL-003-2 to simply BAL-003.	Suggested edits	Change Accepted - removed version reference
Edison Electric Institue (Submitted by Mark Gray)	16	530	Suggest changing the reference to BAL-003-2 to simply BAL-003.	Suggested edits	Change Accepted - removed version reference
Edison Electric Institue (Submitted by Mark Gray)	16	560	Suggest changing the reference to BAL-003-2 to simply BAL-003.	Suggested edits	Change Accepted - removed version reference
Edison Electric Institue (Submitted by Mark Gray)	17	575	Footnote 8 – The NERC Operating Manual linked through this footnote does not contain the Dynamic Transfer Reference Document. EEI suggests changing this link to the following: (https://www.nerc.com/comm/OC/ReferenceDocumentsDL/Dynamic_Transfer_Reference_Document_v4.pdf) which is a direct link to the currently approved Dynamic Transfer Reference Document (Version 4) dated 12/10/2019.	Suggested edits	Corrected Link
Edison Electric Institue (Submitted by Mark Gray)	18	615	Suggest changing the reference to BAL-002-3 to simply BAL-002	Suggested edits	Change Accepted - removed version reference
Edison Electric Institue (Submitted by Mark Gray)	20	691 to 692	Line space should be added between Lines 691 to 692.	Suggested edits	Change Accepted
Edison Electric Institue (Submitted by Mark Gray)	22	758	Suggest changing the reference to BAL-003-2 to simply BAL-003.	Suggested edits	Change Accepted - removed version reference
Edison Electric Institue (Submitted by Mark Gray)	22	759 to 769	BAL-002-2 is incorrectly referenced in the Guideline, currently BAL-002-3 is the approved version. EEI suggests consistent use of Reliability Standard numbers without use of the revision number. (i.e., BAL-002)	Suggested edits	Change Accepted - removed version reference

Edison Electric Institue (Submitted by Mark Gray)	22	760	CR as an acronym for Contingency Reserve which is a defined term. CR is not currently an approved acronym for this term. For this reason, the term should be spelled out and capitalized.	Suggested edits	Change Accepted
Edison Electric Institue (Submitted by Mark Gray)	23	801 to 802	The Lawrence Berkeley National Laboratory document should be identified by Name, not just by the Hyperlink given this is not a NERC document. Also, the link to this document no longer works and should be updated. This link works: https://eta-publications.lbl.gov/sites/default/files/lbnl-4142e.pdf	Suggested edits	Change Accepted - Need to verify link after accepting changes
FERC	7	189	missing the word "to" -or- replace "for" with "that"	typo	Change Accepted
FERC	7	191	This bullet is too generic; appropriate training is open ended.	"Participate in appropriate system operator training that includes BA reserves strategy."	Change Accepted
FERC	10	296, 297	Sentence not clear. Maybe replace the word "should" with "to be able to"	typo	Change Accepted
FERC	10	314-316	Should inverter based resources be included in the following statement: Although response is generally expected to come from on-line rotating machines, other resources (e.g., controllable load contracted for that purpose, certain energy storage devices) can provide initial and sustained response that would help to arrest frequency change and sustain frequency at an acceptable post event-level until frequency is returned within its normal range.	Possibly include inverter based resources in the lst of "other resources"	Change Accepted
Los Angeles Department of Water aand Power	6	181	This bullet is in direct contradiction to PER-005-2 requirements. PER-005-2 provides each entity with the latitude to conduct their own Training Gap Analysis and a DIF (Difficulty, Importance, Frequency) survey to determine how often to train on Reliability-related Tasks, of which are Operating Reserves.	Suggestion to update this bullet from "annual training" to "as deemed ncessary" for the Operating Reserve Program.	Edited to address comments
Los Angeles Department of Water aand Power	pages: 3, 4, and 8	106, 107, 111, 112, 130	Disturbance Recovery Period is not a defined term in either the NERC reliability standards or in the NERC glossary of terms.	Remove term from guidelines and glossary of terms.	NERC Definitions for Operating Reserve Spinning and Operating Reserve Supplemental use this term other references have been reviewed and edits made to support comment.

Agenda Item 5c
Reliability and Security
Technical Committee Meeting
June 8, 2021

Balancing and Frequency Control Reference Document

Action

Approve

Purpose

This Technical Reference Document, “Balancing and Frequency Control” is up for review by the NERC Resources Subcommittee (RS). This reference document is intended as a tutorial for those new to system operations or as a reference for executive level overview.

Background

The RS drafted this reference document at the request of the NERC Operating Committee as part of a series on operating and planning reliability concepts. The document covers balancing and frequency control concepts, issues, and recommendations with the goal to provide an understanding of the fundamentals.

Changes to the Updated Document

The major changes by a sub-team of the RS include:

- Numerous errata edits and re-wording
- Added discussion of inertial control
- Replaced CPS2 references with BAAL
- Added a section for BAL-003 frequency response requirements
- Added components of ATEC in the ACE equation
- Clarified frequency of Reporting ACE calculation with reference to Integrating Reporting ACE Guideline
- Refreshed charts and data
- Removed sections involving frequency response trends and speculation, and replaced with calculations that tie to the standards
- Removed references to market impact on frequency
- Replaced references to Interconnected Operations Services (IOS) with Essential Reliability Services (ERS)
- Removed references to the European Handbook – Union for the Coordination of Transmission of Electricity Operation
- Combined chapters 6 & 7
- Removed Appendix B Review Questions
- Conformed Ch4 Tertiary Control (Reserves) to Operating Reserve Management Guideline

In addition, this document has been through NERC Publications and includes the integrated comments from industry review as identified on the included spreadsheet.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Balancing and Frequency Control

Reference Document

Prepared by the NERC Resources Subcommittee

May 11, 2021

RELIABILITY | RESILIENCE | SECURITY

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

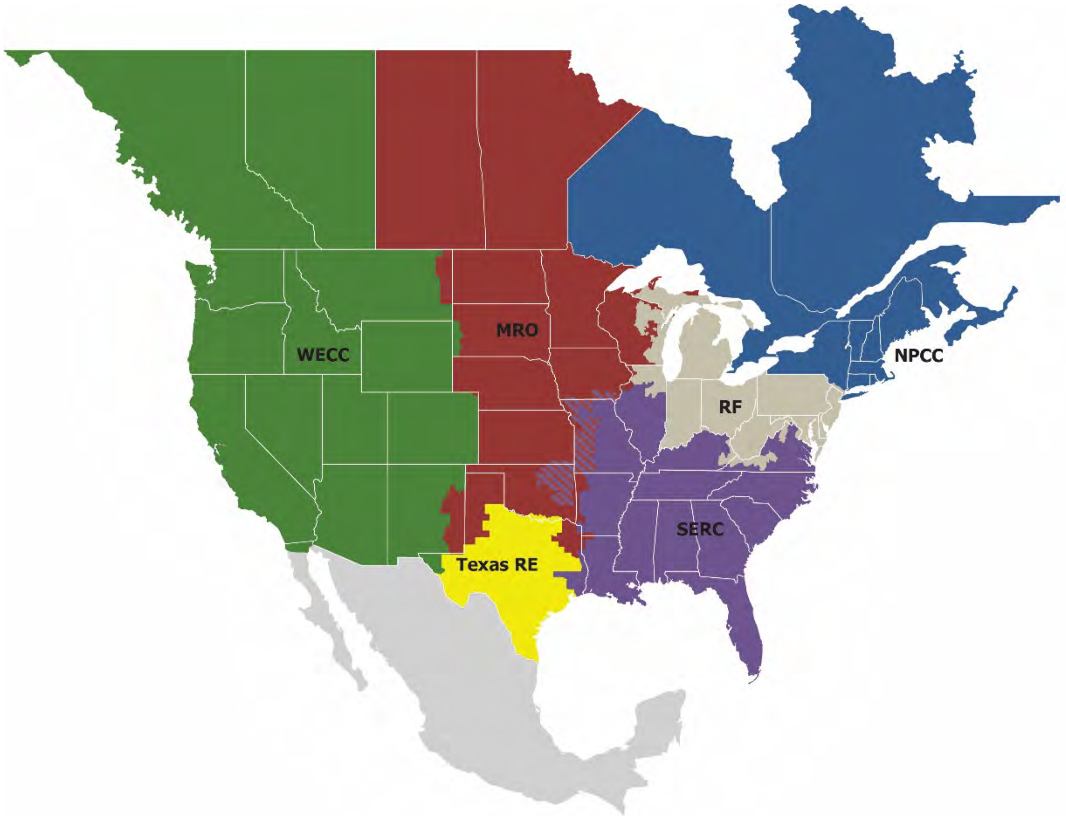
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



The Six Regional Entities	
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Background

The NERC Resources Subcommittee (RS) drafted this reference document at the request of the NERC Operating Committee as part of a series on operating and planning reliability concepts. The document covers balancing and frequency control concepts, issues, and recommendations. Send questions and suggestions for changes and additions to balancing@nerc.com.

Note to Trainers

Trainers are encouraged to develop and share materials based on this reference. The RS will post supporting information on the RS website.[1]

Disclaimer

This document is intended to explain the concepts and issues of balancing and frequency control. The goal is to provide an understanding of the fundamentals. Nothing in this document is intended to be used for compliance purposes or to establish obligations.

[1] https://www.nerc.com/comm/OC/Pages/Resources-Subcommittee.aspx

Chapter 1: Balancing Fundamentals

Balancing and Frequency Control Basics

The power system of North America is divided into four major Interconnections (see **Figure 1.1**). These Interconnections can be thought of as independent electrical islands. The four Interconnections consist of the following:

- **Western Interconnection (WI):** Generally everything west of the Rockies
- **Texas Interconnection (TI):** Operated by the Electric Reliability Council of Texas (ERCOT)
- **Eastern Interconnection (EI):** Generally everything east of the Rockies except Texas and Quebec
- **Quebec Interconnection (QI):** Operated by Hydro Quebec TransEnergie

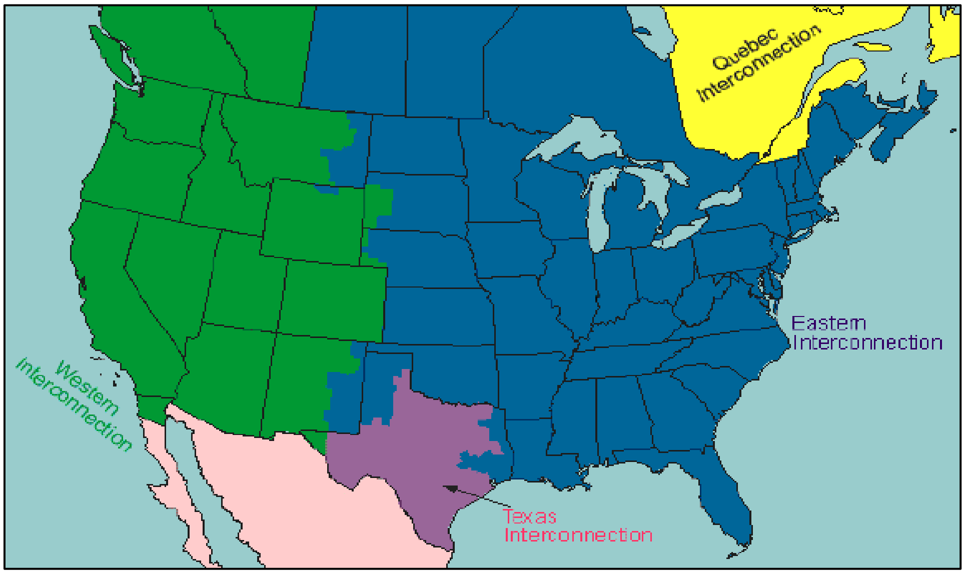


Figure 1.1: North American Interconnections

Each Interconnection can be viewed as a single large machine with every generator pulling together to supply electricity to all customers. This occurs as the electric generating units rotate (in steady-state) synchronously. The "speed" (rotational speed) of the Interconnection is frequency measured in cycles per second, or Hertz (Hz). When the total Interconnection supply exceeds customer demand, frequency increases beyond the scheduled value (typically 60 Hz[2]) until energy balance is achieved. Conversely, when there is a temporary supply deficiency, frequency declines until a balance between supply and demand is restored.

During normal operations it is typical for there to be small mismatches between total demand and total supply, so the frequency of each Interconnection varies above and below nominal on a continuous basis. Regardless of whether the variations are above or below scheduled frequency, the supply-demand balance is restored due to frequency sensitive demands and supply resources that change output in response to frequency changes. For example, some electric devices (e.g., electric motors) use more energy if driven at a higher frequency and less at a lower frequency. Most generating units are also equipped with governors that cause the generator to inject more energy into the Interconnection when frequency is lower than nominal and slightly less energy when the frequency is higher than nominal.

[2] Nominal frequency (termed "scheduled frequency") is sometimes intentionally offset by a small amount via a mechanism called time error corrections to correct for sustained periods of high or low frequency.

Balancing Authorities (BAs) balance generation and load within their Balancing Authority Areas (BAAs) of the Interconnections. See **Figure 1.2** for an example of BAAs across North America. The BAs dispatch generating resources in order to meet their BAA demand and manage the supply/demand balance. Some BAs also control demand to maintain the supply/demand balance.

Figure 1.2: North American Balancing Authorities and Regions

The number of BAs in an Interconnection varies; Texas and Quebec are single BA Interconnections while the Eastern and the Western are multi-BA Interconnections. Each BA in an Interconnection is connected via high voltage transmission lines (called tie-lines) to neighboring BAs. The Reliability Coordinators (RCs) oversee the BA operations and coordination. BAs are responsible for the supply/demand balance within their BAA while RCs are responsible for the wide area health of the Interconnection.

Frequency will be constant in an Interconnection when there is a balance between supply and demand, including various electrical losses. This balance is depicted in **Figure 1.3**.

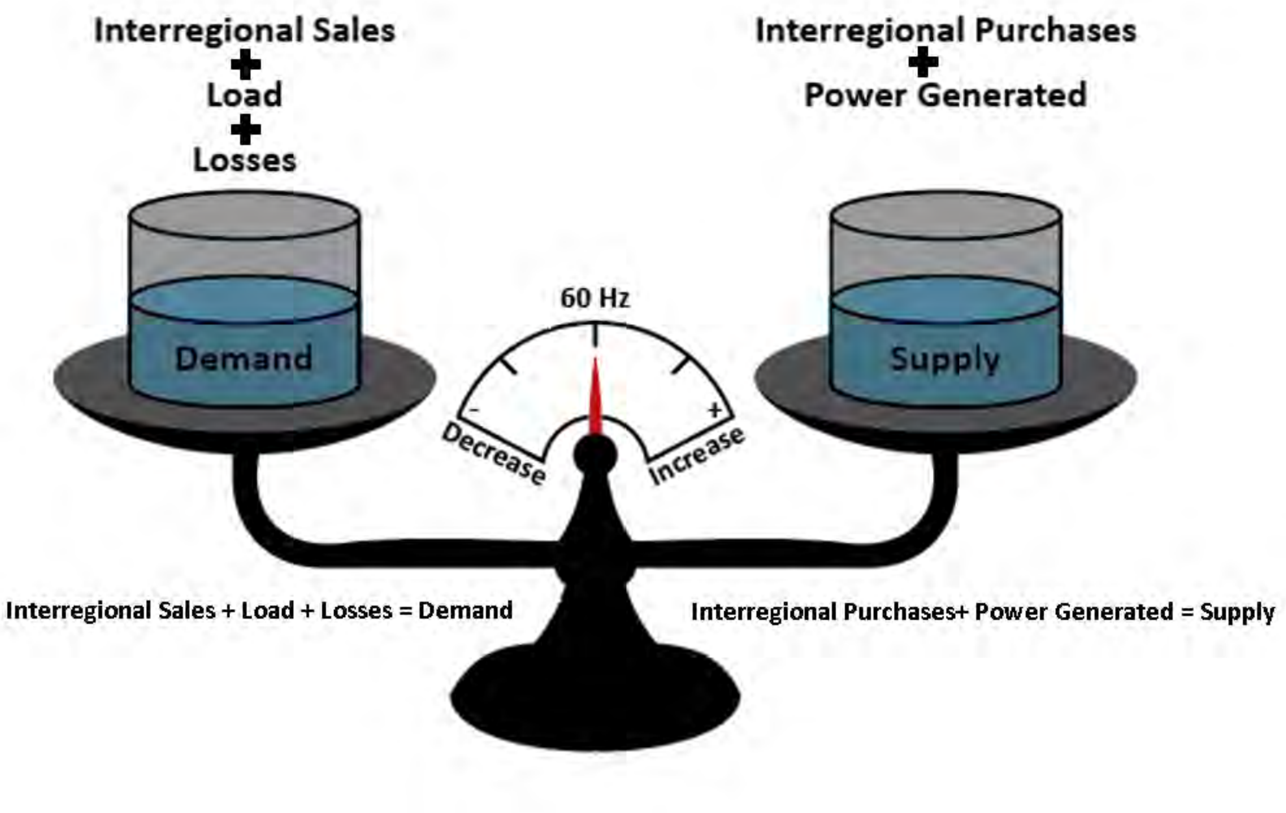


Figure 1.3: Generation | Demand Balance

Each supply resource embedded in an interconnected system has its own characteristics (e.g., ramp rates, fuel supply, output controllability and sustainability). From a simplified viewpoint, a supply resource can be analogized to a water pump with storage and control as shown in **Figure 1.4**. In this example, the pump's output fills an open storage tank similar to a swimming pool. The water depth in the tank needs to be controlled to within very tight limits: too much water accumulating will cause the pool to overflow, and too little water will cause other problems. The control valve changes average output to meet system demand in a manner analogous to automatic generation control (AGC). The surge tank on the final output is analogous to the rotational inertia of the generator.

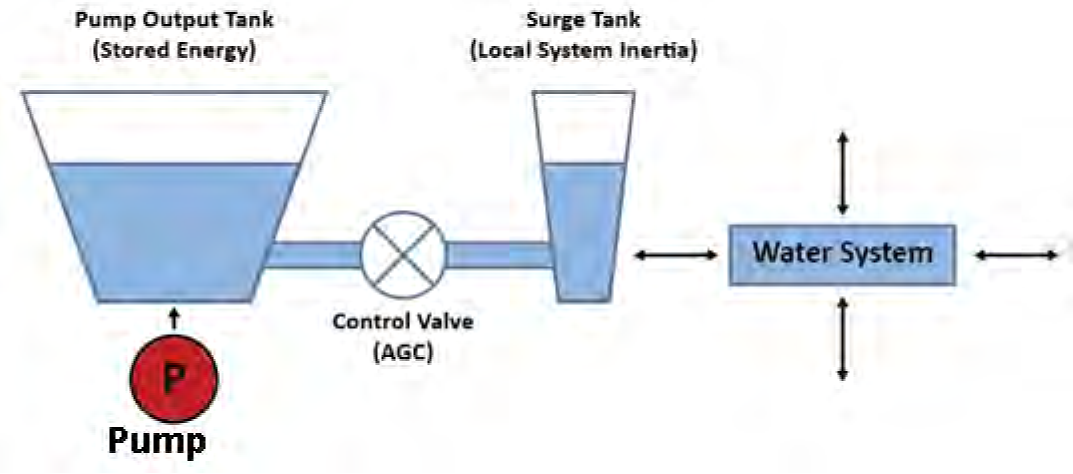


Figure 1.4: Generator | Pump Analogy

To understand how Interconnection frequency is controlled, it may help to visualize a traditional water utility that is composed of a delivery system, customers, and several pumping stations as depicted in **Figure 1.5**. If a municipality operates its own system, it needs sufficient pumps (supply) to maintain the water level in the pumping stations' storage tanks (frequency) to serve its customers. When demand exceeds supply, the water levels in the pumping station tanks will drop prompting the pumps to respond. Water level (frequency) is the primary parameter that must be controlled in an independent system.

In the early history of the power system, utilities quickly learned the benefits in reliability and realized reduced expense associated with maintaining operating reserves by connecting to neighboring systems. In our water utility example, an independent utility must have pumping stations in standby that are equivalent to its largest on-line pump if it wants to maintain the water level in case there is a problem with the largest pumping station. However, if utilities are connected together via tie-lines, reliability and economics are improved because of the larger resource capacity of the combined system and the ability to share capacity when needed.

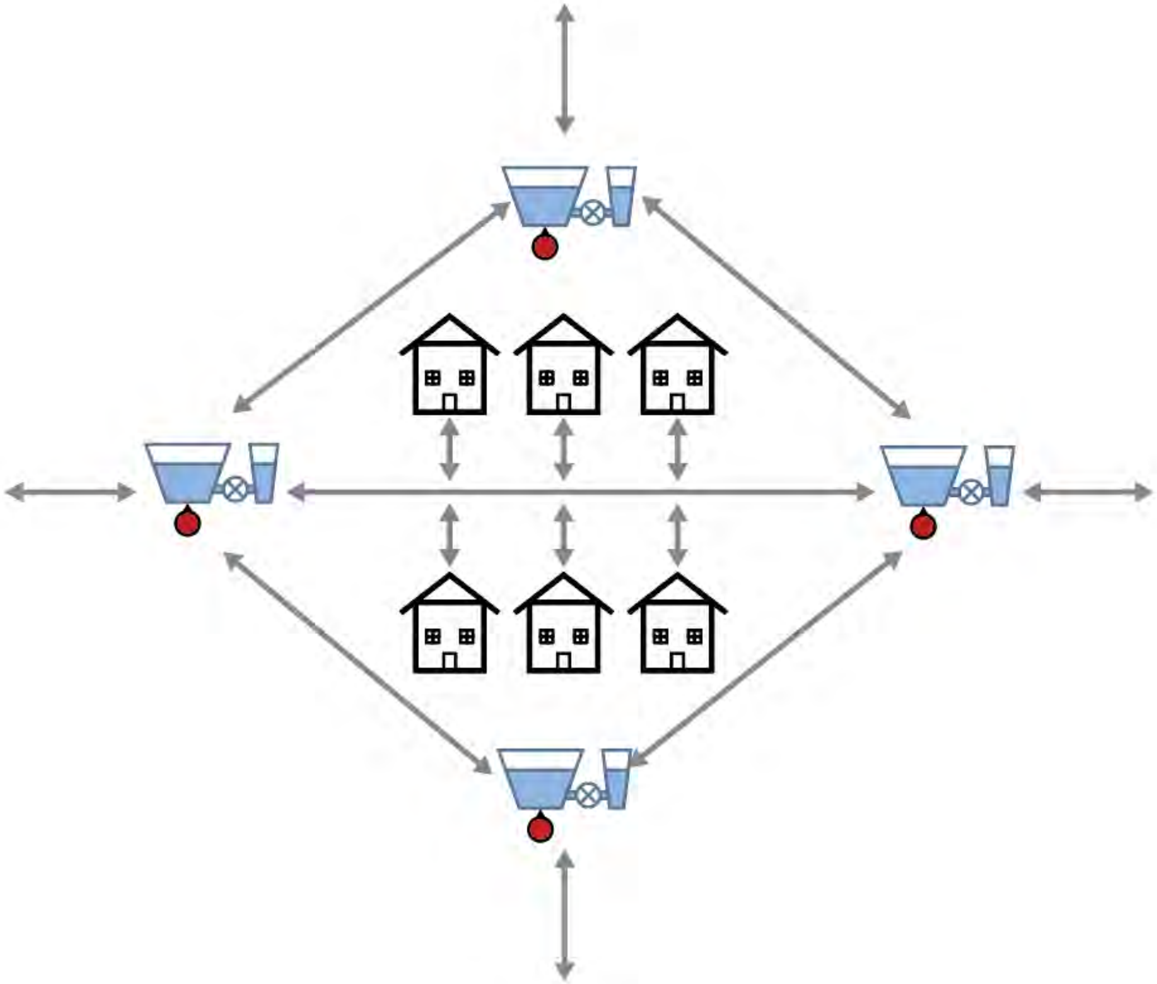


Figure 1:5: BA Analogy

Once the systems are interconnected, the steady state frequency (i.e. water level) is the same throughout. If one BA in the electric grid loses a generating resource, then there may be a drop in frequency. This drop in frequency is less than in an independent system because the overall resource capacity of the interconnected system is much greater. The BA that needs energy could purchase it from others provided that the interconnected system can reliably accommodate the additional flow. Purchasing and/or selling energy between BAs is known as Interchange.

There are two inputs to the BAs control process:[3]

- **Interchange Error:** the net outflow or inflow compared to the scheduled sales or purchases (The units of interchange error are in megawatts.)
- **Frequency Error:** the difference between actual and nominal frequency (The units of frequency error are hertz.)

Frequency bias is used to translate the frequency error into megawatts. Frequency bias is the BAs obligation to provide or absorb energy to assist in maintaining frequency. In other words, if frequency goes low, each BA is asked to contribute a small amount of extra generation in proportion to its system's relative size.

Each BAA usesa common source on the tie-lines with its neighbors for control and accounting. There will be an agreed upon meter at each BA boundary that both neighboring BAs use to perform balancing operations and accounting. Thus, all supply, load, and transmission lines in an Interconnection fall within the metered bounds of a BA.

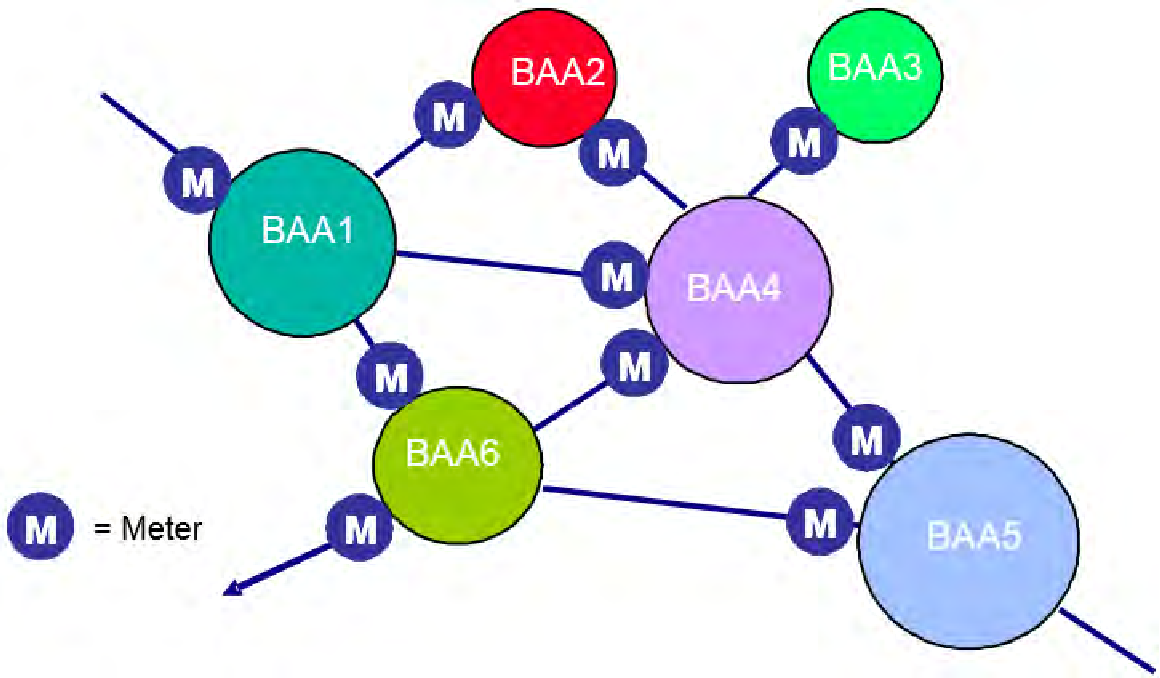


Figure 1:6: Interconnected BA Areas

If the BA is not buying or selling energy,[4] and its supply is exactly equal to the demand and losses within its metered boundary (BAA), the net of its tie line meters will be zero (assuming that the frequency of the system is at nominal). If the BA chooses to buy energy (e.g., 100 Megawatt hours (MWh)), it tells its control system to allow 100 MWh to flow in (by, for example, allowing 100 MW to flow in for one hour). Conversely, the seller will tell its control system to allow 100 MWh to flow out by allowing the corresponding 100 MW to flow out for one hour. If all BAs behave this way, the Interconnection remains in balance and frequency remains stable. Variations in the supply/demand balance

[3] There are two control inputs in multi-BA Interconnections. Texas and Quebec are single BA Interconnections and need only control to frequency.

[4] In most cases, BA's do not buy and sell energy. Transactions now are arranged by wholesale marketing agents that represent load or generation within the BA.

cause frequency to vary from its nominal value. Problems on the grid, such as congestion that prevents the ability to meet schedules, equipment faults that dictate rapid unilateral adjustments of generation, loss of load, incorrect schedules, or poor control cause changes in frequency. Maintaining Interconnection frequency near its nominal value can therefore be thought of as a fundamental indicator of the health of the power system.

Demand and supply are constantly changing within all BAAs. This means that a BA will usually have some unintentional outflow or inflow at any given instant. This mismatch in meeting a BA's internal obligations, along with the small additional "bias" obligation to maintain frequency, is represented via a real-time value called Area Control Error (ACE), with units of MW.

System operators at each BA fulfill their NERC obligations by monitoring ACE and keeping the value within limits that are generally proportional to BA size. This balancing is typically accomplished through a combination of adjustments of supply resources, purchases and sales of electricity with other BAs, and possibly adjustments of demand.

Conceptually, ACE is to a BA what frequency is to the Interconnection. Over-generation makes ACE go positive and puts upward pressure on Interconnection frequency. A large negative ACE can cause Interconnection frequency to drop. A highly variable or "noisy" ACE tends to contribute to similarly "noisy" frequency. However, the effect of ACE on frequency depends on how ACE is correlated (or anti-correlated) with frequency error. Over-frequency error tends to be made larger when ACE indicates over-generation, and is made smaller when ACE indicates under-generation. Under-frequency error has the opposite relationship. This principle is captured in the way Control Performance Standard 1 (CPS1) measures performance. Accumulation of frequency error over time results in the Interconnection's time error. For better overall Interconnection performance, the Western Interconnection (WI) uses automatic time error correction (ATEC) that allows BAs to make incremental corrections that are caused by under/over performing ACE.

Control Continuum

Figure 1.7 demonstrates that Balancing and frequency control occur over a continuum of time using different resources that have some overlap in timeframes of occurrence.

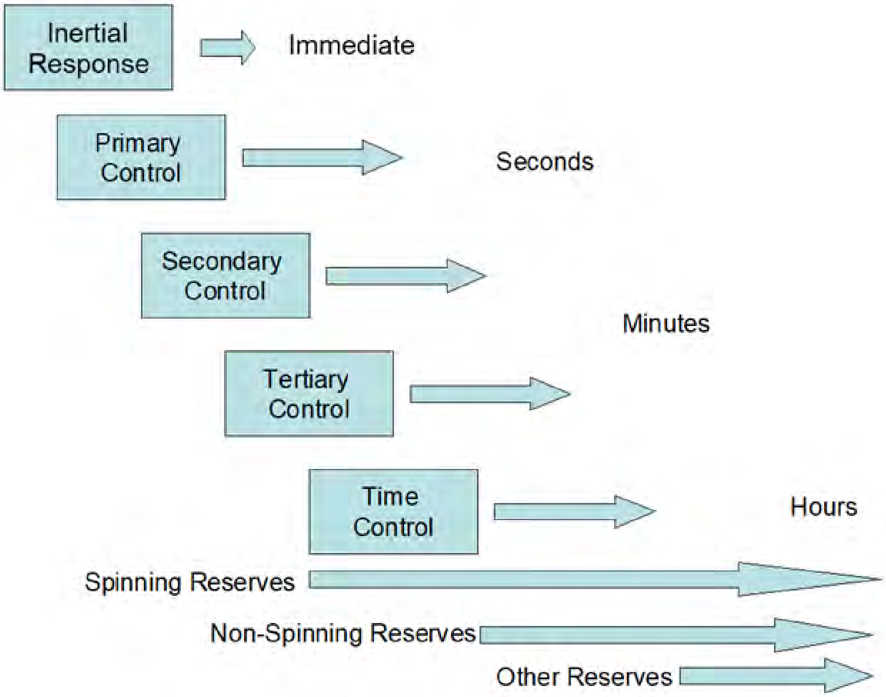


Figure 1.7: Control Continuum

A primary focus of the controls in the control continuum is to maintain nominal frequency under all conditions. One common operating condition is the loss of a (sometimes large) generator. This causes the frequency to drop which then requires the various pieces of the control continuum to recover the frequency to nominal. A stylized example is shown in figure 1.8. The frequency event is somewhat arbitrarily divided into 4 phases: the Arresting Period (when frequency decline is arrested), the Rebound Period (where frequency begins to recover towards nominal), the Stabilizing period (where frequency is stabilized), and the Recovery period (where frequency is recovered to nominal).

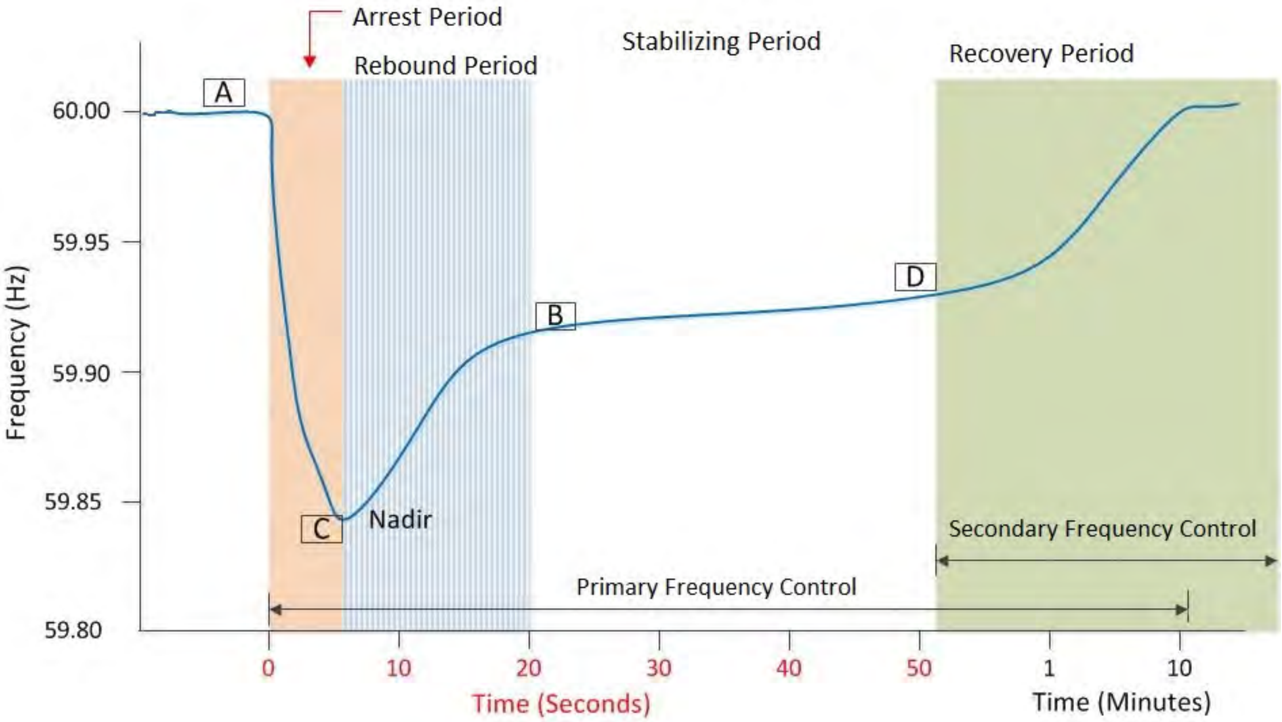


Figure 1.8: Typical Frequency Trend for the Loss of a Generating Resource

Four points of particular interest are shown in Figure 1.8: Point A is defined as the pre-disturbance frequency; Point C or Nadir is the maximum deviation due to loss of resource; Point B is defined as the stabilizing frequency and; Point D is the time the contingent BA begins the recovery from the loss of resource.

Inertial Control

Inertial control is more of an effect than an actual control since it is governed by physical principles for most resources and emulated by others. The rotating mass in a typical generator combined with the speed at which it is rotating creates a large amount of stored energy. If a decelerating force is applied (e.g., a large drop in system frequency), energy is transferred from the rotating mass and into the system. One analogy is that of a bicycle wheel and brake. If the wheel is first set spinning and then the brake is applied, the energy from the wheel flows into the braking surfaces. The contact surfaces of the brake will heat up due to the transformation of energy from the wheel into heat.

This is the same principle for the inertia effect in the power system. A sudden increase in the braking force is applied by a decrease in the amount of energy being injected into the system (e.g., losing a large generator or addition of a large load). When the mismatch between injected and consumed energy occurs, energy flows from the rotating masses of the connected resources into the power system. The propagation of this effect across an Interconnection happens within a handful of seconds.

Resources that are not directly coupled via an alternating current connection to the power system (e.g., inverter-based resources) are not typically governed by the same physical principles and therefore might not possess inertia per se from the perspective of the power system. Instead, inertia can be emulated to varying degrees of success by using sensing and control.

Primary Control

Primary control is more commonly known as primary frequency response (PFR). PFR also includes inertial response described under Inertial Control above as well as other types of frequency response actions, as described in the Primary Frequency Control Guideline.[5] PFR is autonomous; it does not require external inputs and begins to occur within the first few seconds following a change in system frequency (disturbance) to stabilize the Interconnection. Frequency response is provided by the following:

- **Governor Action:** Resource governors are like cruise controls for cars. They sense changes in local system frequency and adjust the energy output of the resource to counteract that change. Some resources do not have “governors” per se but instead can emulate governor action to varying degrees of success by using sensing and control actions.
- **Demand Response:** The speed of directly-connected motors in an Interconnection will change in direct proportion to frequency changes. As frequency drops, motors will turn slower and consume less energy.

  Rapid reduction of system load may also be affected by automatic operation of under-frequency relays which interrupt predefined loads within fractions of seconds or within seconds of frequency reaching a predetermined value. Such reduction of load may be contractually represented as interruptible load or may be provided in the form of resources procured as reliability or Ancillary services. As a safety net, percentages of firm load may be dropped by under-frequency load shedding programs to ensure stabilization of the systems under severe disturbance scenarios.

[5] PFC (v 2.0 approved by the Operating Committee 6/4/2019)

The most common type of a frequency disturbance in an Interconnection is associated with the loss of a generator, causing a decline in frequency; this happens on a daily basis and must be considered. In general, the amount of frequency-responsive, synchronized and unloaded generation (a.k.a. headroom) in an Interconnection will directly influence the amount of available frequency response because this is the amount of supply that is connected, ready, and able to immediately increase output when needed. Inverter-based resources, especially those coupled with storage or headroom, may also be able to contribute to frequency response.

It is important to note that primary control will not return frequency to nominal, but only arrest and stabilize it. Other control components are used to restore frequency to nominal.

Operating Tip: Frequency response is particularly important during disturbances and islanding situations. System operators should be aware of their frequency responsive resources. Blackstart units must be able to autonomously participate in frequency control; this is especially important during system restoration.

Secondary Control

Secondary control typically includes the balancing services deployed in the “minutes” time frame. However, some resources (e.g., hydroelectric generation or fast electrical storage) can respond faster in many cases. Secondary control is accomplished using the BA’s supervisory control and data acquisition (SCADA) and energy management systems (EMSs)[6], and the manual actions taken by the dispatcher to provide additional adjustments. Secondary control also includes some initial reserve deployment for disturbances.

In short, secondary control maintains the minute-to-minute balance throughout the day and is used to keep ACE within CPS bounds and thereby maintain Interconnection frequency close to its scheduled value (usually 60 Hz) following a disturbance. Secondary control is provided by both Operating Reserve – Spinning and Supplemental. During frequency disturbances, secondary control returns the frequency to nominal once primary control has arrested and stabilized it.

The most common means of exercising secondary control is through an EMS’s AGC (Automatic Generation Control). AGC operates in conjunction with SCADA systems; SCADA gathers information about an electric power system, particularly system frequency, generator outputs, and actual interchange between the BA and its neighbors. Using system frequency and net actual interchange and knowledge of net scheduled interchange and upcoming changes, it is possible to determine the BA’s energy balance (i.e., its ACE) within its Interconnection. Most SCADA systems poll data points sequentially for electric system data, with a typical periodicity of two to six seconds. Because of this, data is naturally slightly out of perfect time sync, but is of sufficient quality to permit balancing and good frequency control.

AGC computes a BAA’s ACE from interchange and frequency data. ACE indicates whether a system is in balance or is in need of an adjustment to generation resources. AGC software generally sends signals that cause resources performing secondary control to move to oppose the ACE. Some AGC systems use pulses for raise/lower signals while other AGC systems use MW set points.

The degree of success of AGC in complying with balancing and frequency control is manifested in a BA’s control performance statistics that are described in greater detail later in this document.

Tertiary Control

Tertiary Control encompasses actions taken to get resources in place to handle current and future contingencies. Reserve deployment and reserve restoration following a disturbance are common types of Tertiary Control.

[6] Terms most often associated with this are “load-frequency control” or “automatic generation control”

Time Control

Frequency and balancing control are not perfect. There will always be occasional errors in tie-line meters whether due to instrument transducer inaccuracy, problems with SCADA hardware or software, or communications errors. Due to these errors and normal load and generation variation, ACE in an Interconnection cannot be maintained at zero. In fact, the average value of ACE over many time frames is non-zero. ACE must be managed such that its magnitude is relatively small. There is no operational reason to force ACE to be an independently randomly distributed variable. This means that frequency is never maintained at exactly 60 Hz for any appreciable length of time and average frequency over time usually is not exactly 60 Hz.

Each Interconnection has a time control process that can be used to maintain the long-term average frequency at 60 Hz. While there are some differences in process, each Interconnection designates a RC as a "time monitor" to provide Time Control.

The time monitor compares a clock driven off Interconnection frequency against the "official time"[7] provided by the National Institute of Standards and Technology. If average frequency drifts, it creates a Time Error between these two clocks. The QI and TI operate so that Time Error is automatically minimized or eliminated while the WI operates to automatically mitigate accumulated Time Error through its ATEC. If the Time Error gets too large in the EI and WI, the Time Monitor may notify BAs in the Interconnection to manually correct the situation.

For example, if frequency has been running 2 mHz high (i.e., 60.002 Hz), a clock using Interconnection frequency as a reference will gain 1.2 seconds in a 10-hour interval:

$$\frac{(60.002\text{ Hz} - 60.000\text{ Hz})}{60\ Hz} * 10\ hr\ *\ 3600\frac{sec}{hr}\ =\ 1.2\ sec$$

If the Time Error accumulates to a predetermined initiation value (e.g., +10 sec in the Eastern Interconnection (EI)) the Time Monitor will send notices for all BAs in the Interconnection to offset their scheduled frequency by -0.02 Hz (Scheduled Frequency = 59.98 Hz). This offset, known as Time Error Correction, will be maintained until Time Error has decreased below the termination threshold (e.g., +6 sec).

A positive offset (i.e., Scheduled Frequency = 60.02 Hz) would be used if average frequency was low and Time Error reached its initiation value (e.g., -10 seconds). Manual time error corrections are no longer required by NERC Reliability Standards but each Interconnection may elect to perform manual time error correction. See the *NERC Time Monitoring Reference Document (Version 5)* on manual time error correction for additional information.[8]

Control Continuum

Table 1.1 summarizes the discussion on the control continuum and identifies the service that provides the control and the NERC standard that addresses the adequacy of the service. Current issues, good practices, and recommendations on balancing and frequency control are discussed later.

Table 1.1: Control Continuum Summary

Control	Ancillary Service/ERS	Timeframe	NERC Measurement
Inertial Control	Inertial Control	0–12 Seconds	N/A
Primary Control	Frequency Response	10–60 Seconds	FRM

[7] The Official NIST US Time: https://www.time.gov/

[8] https://naesb.org/pdf4/weq_bps062520w1.pdf

Secondary Control	Regulation	1–10 Minutes	CPS1 – DCS - BAAL
Tertiary Control	Imbalance/Reserves	10 Minutes–Hours	BAAL - DCS
Time Control	Time Error Correction	Hours	N/A

Area Control Error (ACE) Review

The CPSs are based on measures that limit the magnitude and direction of the BAs Reporting ACE. The equation for Reporting ACE is as follows:

- Reporting ACE = $(NI_A - NI_S) - 10B\,(F_A - F_S) - I_{ME}$
- Reporting ACE (WI) = $(NI_A - NI_S) - 10B\,(F_A - F_S) - I_{ME} + I_{ATEC}$

where:

- NI_A is Actual Net Interchange,
- NI_S is Scheduled Net Interchange,
- B is BA Bias Setting
- F_A is Actual Frequency,
- F_S is Scheduled Frequency,
- I_{ME} is Interchange (tie line) Metering Error
- I_{ATEC} is ATEC (WI only)

NI_A is the algebraic sum of tie line flows between the BA and the Interconnection. NI_S is the net of all scheduled transactions with other BAs. In most areas, flow into a BA is defined as negative; flow out is positive.

The difference between net actual interchange and net scheduled interchange (N_{IA} - N_{IS}) represents the so-called “inadvertent” error associated with meeting schedules without consideration for frequency error or bias. If it is used by itself for control, it would be referred to as “flat tie line” control.

The term 10B (F_A - F_S) is the BAs obligation to support frequency. B is the BAs frequency bias stated in MW/0.1 Hz (B’s sign is negative). The “10” converts the bias setting to MW/Hz. F_S is normally 60 Hz but may be offset ± 0.02 Hz for time error corrections. Control using “10B (F_A - F_S)” by itself is called “flat frequency” control.

I_{ME} is a correction factor for meter error. The meters that measure instantaneous[9] flow are not always as accurate as the hourly meters on tie lines. BAs are expected to check the error between the integrated instantaneous and the hourly meter readings. If there is a metering error, a value should be added to compensate for the estimated error; this value is I_{ME}. This term should normally be very small or zero.

I_{ATEC} is an ACE offsetting term for automatic timer error correction in the WI. BAs correct for any delta Time Error that they are responsible for each hour.

Reporting ACE is calculated in Real-time, at least as frequently as every six seconds, by the responsible entity’s Energy Management System (EMS) predominantly based on source data automatically collected by that system. Also, the data must be updated at least every six seconds for continuous scan telemetry and updated as needed for report-by-exception telemetry. See the Integrating Reporting ACE Guideline for more detail on the components of ACE and the calculation frequency.

Here is a simple example: Assume a BA with a bias of -50 MW/0.1 Hz is purchasing 300 MW. The actual flow into the BA is 310 MW. Frequency is 60.01 Hz. Assume no time correction, metering error or ATEC.

[9] Instantaneous, as used herein, refers to measurements that are as close to real-time as is possible within the limits of data acquisition and conversion equipment.

- ACE = (-310 – -300) – 10*(-50) * (60.01 – 60.00) = (-10) – (-5) = -5 MW.

The BA should be generating 5 MW more to meet its obligation to the Interconnection. Even though it may appear counterintuitive to increase generation when frequency is high, the reason is that this BA is more energy-deficient at this moment (-10 MW) than its bias obligation to reduce frequency (-5 MW). The decision on when or if to correct the -5 MW ACE would be driven by CPS compliance.

A distinction can be drawn between reporting ACE, which measures the effect of a BA on the Interconnection, and Control ACE. At any given time, a BA might use a control ACE that is different from reporting ACE because AGC resources respond to control ACE, and this difference might be used, for example, to cause AGC resources to assist in "paying down" accumulated inadvertent energy or some other purpose.[10]

Bias (B) vs. Frequency Response (Beta)

There is often confusion in the industry when discussing frequency bias and frequency response. Even though there are similarities between the two terms, frequency bias (B) is not the same as frequency response (β).

Frequency response, defined in the NERC Glossary,[11] is the mathematical expression of the net change in a BA's net actual interchange for a change in Interconnection frequency. It is a fundamental reliability characteristic provided by a combination of governor action and demand response. Frequency response represents the actual MW contribution by inertial control and primary control to stabilize frequency following a disturbance.

Bias is an approximation of β used in the ACE equation. Bias (B) is designed to prevent AGC withdrawal of frequency support following a disturbance. If B and β were exactly equal, a BA would see no change in ACE following a frequency decline even though it provided a MW contribution to stabilize frequency.

Bias and frequency response are both expressed as negative numbers. In other words, as frequency drops, MW output (β) or desired output (B) increases. Both are measured in MW/0.1 Hz

Important Note: When people talk about frequency response and bias, they often discuss them as positive values (e.g., as "our bias is 50MW/0.1Hz"). Frequency response and bias are actually negative values.

Early research (Cohn) found that it is better to be over-biased (i.e., absolute value of B greater than the absolute value of β) than to be under-biased.

[10] Bilateral or Unilateral payback of inadvertent is not allowed in the WI. ATEC is used by BAs in the WI to control primary inadvertent accumulation while automatically correcting time error.

[11] Select from list found at: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

Chapter 2: Primary Control

Background

Primary control relates to the response to a frequency deviation by generator governors (aka. speed controls) and inertia that helps stabilize Interconnection frequency whenever there is a change in load-resource balance. Primary control is provided in the first few seconds following a frequency change and is maintained until it is replaced by AGC action (secondary control). Frequency response (or Beta), which also includes rotational inertia response from resources and load response from frequency dependent loads, is the more commonly used term for primary control. Beta (β) is defined by the total of all initial responses to a frequency excursion.

Figure 2.1 shows a trace of the WI's frequency that resulted from a generating unit trip. The graph plots frequency from 5 seconds prior to the loss of a large generator until 60 seconds thereafter.

NERC references three key events to describe such a disturbance. Value A is the pre-disturbance frequency, typically close to 60 Hz. Point C is the maximum excursion point, commonly referred to as the Nadir, which occurs about 10 seconds after the loss of generation in this WI example. Value B is the settling frequency of the Interconnection.

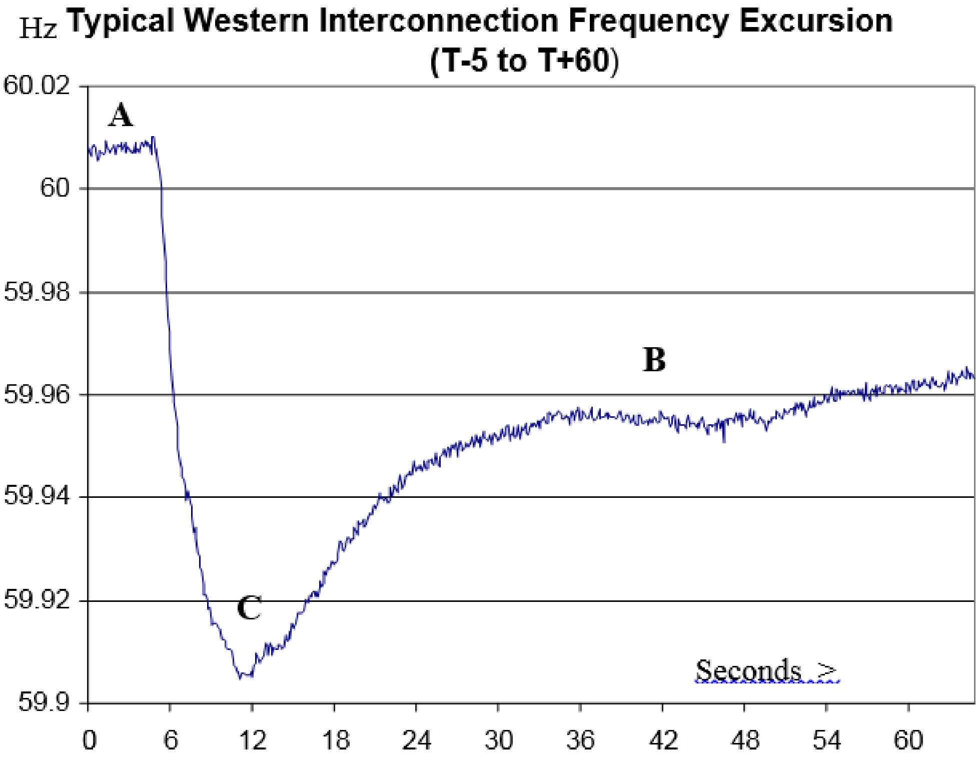


Figure 2.1: WI Frequency Excursion

As discussed earlier, there are two groups of "resources" that arrest a decline in frequency due to a loss of generation:

- A given portion of Interconnection demand is composed of motor load, which draws less energy when the motors slow down due to the lower frequency.
- Generators have governors that act much like cruise control on a car. If the generators on the Interconnection start to slow down with the frequency decline, their governors supply more energy to the generators' prime movers in order to speed them back up to nominal. The sensitivity of this response is controlled by the governor droop setting.

Inertial Response

Inertia quickly and autonomously opposes changes to both under and over frequency events. Having a large amount of inertia is useful for smoothing out power system frequency fluctuations. It is inertia combined with the response of frequency sensitive demand that determines how quickly the frequency decays following the loss of a large supply resource like a large generator or importing direct current tie-line. In an interconnection, more inertia leads to a slower drop in frequency, giving time for the other components of the control continuum to act in order to arrest, stabilize, and then recover frequency. In some sense, the inertia of the power system can be controlled by adjusting the amount and type of generators that are on-line. Inertia is commonly described in units of seconds: the energy that is stored is normalized by the electrical "size" of the resource. Since stored energy is a function of the square of the speed of rotation, low rotating mass, faster spinning resources might store more energy, yet they typically decelerate faster (thereby injecting more energy). These lighter and faster resources' contribution to slowing the fall of frequency is more "front-loaded" and they have smaller normalized inertia values than large-rotating-mass slow-spinning resources that have slower energy injection profiles. Faster response is also not always better because of interaction effects that can cause instability where resources might "bounce" in opposite directions.

For a discussion and graphical representation on how inertia opposes changes in under and over frequency excursions, see the *NERC Frequency Response Standard Background Document,* dated November 2012.[12]

Generator Governors (Speed Controls)

The most fundamental, front-line control of frequency in ac electric systems is the action of generator governors. Governors act to stabilize frequency following disturbances and act as an immediate buffer to load-resource imbalance. Governors operate in the time frame of milliseconds to seconds and operate independently from and much faster than system operator actions or those of AGC. They protect from the effects of frequency when too high, but the vast majority of their benefit comes from assisting when frequency has dropped too low, especially in cases where loss of generation causes abrupt decreases in Interconnection frequency.

Without governor action, loss of generation would result in frequency that would not stabilize until the load reduced to a point that matched the remaining generation output. As mentioned previously some load is reduced when the frequency is reduced mostly due to directly connected motors slowing down and consuming less power. This supply/demand balance point could occur at very low frequency and could result in cascading outages or complete frequency collapse, a very undesirable outcome in terms of the cost to society and potential equipment damage.

The combination of inertial response, governor response and load response – are the "beta" (β), or frequency response characteristic, of a BAA. This is the characteristic that AGC attempts to mimic in its use of the frequency bias ("B") parameter in determining ACE. The net of all BA frequency responses manifests as the Interconnection frequency response.

Droop

Governors cause generators to try and maintain a constant, stable system frequency (60 Hertz in North America). They do this by constantly governing (modulating) the amount of mechanical input energy to the shaft of the electric generator. The degree of this modulation is called "droop" and is measured in percent of frequency change to cause full generator capability to be exerted against the frequency error. A typical slope is 5%, meaning that the full output of the generator would be used (or attempt to be used) to counteract the frequency error if frequency error is 5% or 3 Hz. It should be noted that smaller droop percentages indicate increased sensitivity of response, e.g., a generator with a 4% droop would attempt to go to full output if the frequency changed by 2.4 Hz. Frequency errors are more typically in the range of 0.01% (.06 Hz, or 60 mHz), so governor action usually is a much smaller fraction of a unit's output capability. It must also be recognized that, while most generators can reduce output considerably in response

[12] https://www.nerc.com/comm/OC/RS%20Landing%20Page%20DL/Related%20Files/Bal-003-1_Background_Document_Clean_20121130.pdf

to their governor's actions, increasing output is more problematic since many generators may already be near the top of their output capability when low frequency causes their governor to request more output. Thus, if there is no headroom available on a generator's output, the governor will be able to do little to increase that output and help stabilize low frequency.

Deadband

The second general characteristic of governors is "deadband." This means that the governor ignores frequency error until it passes a threshold. When frequency error exceeds the threshold (which should not exceed the maximum deadband setting per Interconnection recommended in the NERC Reliability Guideline-Primary Frequency Control), the governor becomes active. It is worth noting that the deadband may be larger for older mechanical-style governors, and may have mechanical lash associated with it.

The calculated unit MW output change with a droop setting of 5% and deadband setting of 36 mHz based on the total resource capacity is shown in Figure 2.2

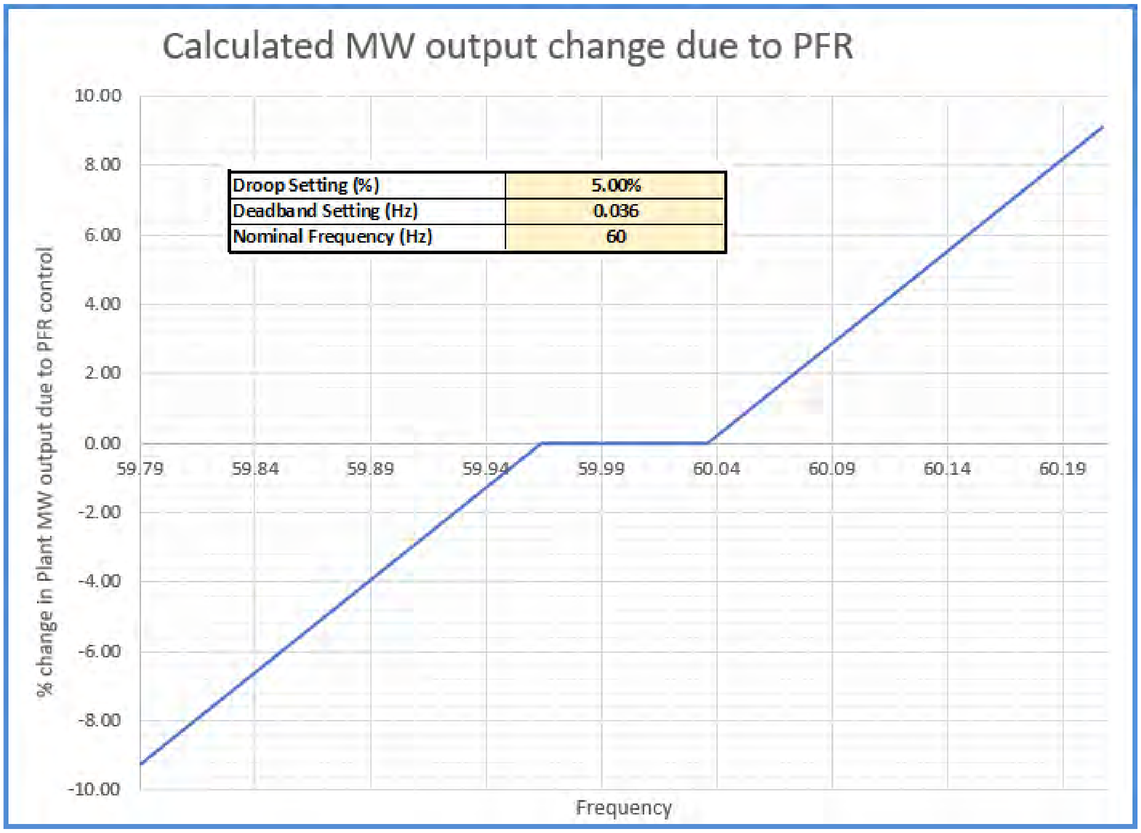


Figure 2.2: Calculated Resource %MW Output Change due to PFR

Calculating Frequency Response

Prior to current Reliability Standard requirements governing frequency response[13], calculation of frequency response was addressed by the NERC *Frequency Response Characteristic Survey Training Document*,[14] which included a form to guide the calculation for a given event. The calculation of the Frequency Response Characteristic (FRC) for a BA is to divide the change in Net Interchange Actual (NI_A) from pre-event (A point, see Figure 1.8 above) to the stabilizing period (B point, ~20-52 seconds after the event) by the change in interconnection frequency from pre-event to the stabilizing period. Although the terms in the FRC Training Document have changed over the years (e.g., Control Area is now Balancing Area), the calculation remains the same. This is often referred to as the A to B frequency response. With the advent of faster scanning tools over the years (e.g., Phasor Measurement Units), a similar response calculation can be made from the A point to the C point (nadir, if a generation loss or apex, if a load loss) of the frequency event.

Important Concept: The frequency response will normally be a negative value, reflecting the inverse relationship between the increase in MW output in response to the decrease in interconnection frequency for a frequency decline (e.g., a generator trip), or vice versa for a frequency increase (e.g., a load loss).

Under the current Reliability Standard requirements, the selection of events for evaluation and the calculation forms used to determine response are prescribed by the Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard[15], the Reliability Standard itself, its attachment and associated forms.

Frequency Response Profiles of the Interconnections

The amount of frequency decline from a generator trip varies based on a number of factors, e.g. time of day, season, and Interconnection loading. The observed frequency responses of the North American Interconnections as documented in the *2018 NERC State of Reliability* report are as follows:

• EI	-2,103 MW / 0.1Hz
• TI	-674 MW / 0.1 Hz
• WI	-1,539 MW / 0.1 Hz
• QI	-599 MW / 0.1 Hz

Important Note: These values are not normalized to adjust for starting frequency and/or resource loss size.

As noted above, the negative sign means there is an inverse relationship between generation loss and frequency. In other words, a loss of 1,000 MW would cause a frequency change (A to B) on the order of:

• EI	-0.048 Hz
• TI	-0.148 Hz
• WI	-0.065 Hz
• QI	-0.168 Hz

Conversely, if 1000 MW of load were lost in an Interconnection, the resulting frequency increase would be similar in magnitude as listed above.

[13] As of the release date of this document, the current applicable Reliability Standard is BAL-003-1.1

[14] https://www.nerc.com/comm/OC/RS%20Agendas%20Highlights%20and%20Minutes%20DL/Frequency_Response_Characteristic_Survey_19890101.pdf

[15] https://www.nerc.com/comm/OC/BAL0031_Supporting_Documents_2017_DL/Procedure_Clean_20121130.pdf

Figure 2.3 is a typical trace following the trip of a large generator in three of the Interconnections. Notice that governors in the East do not provide the "Point C to B" recovery of frequency as they do in the other Interconnections. The rate of frequency decline is much slower primarily due to its size, so frequency slowly drops until sufficient response stops the decline. In the early 2000s, there was typically a post-event decline in frequency, but this effect has been occurring less often.

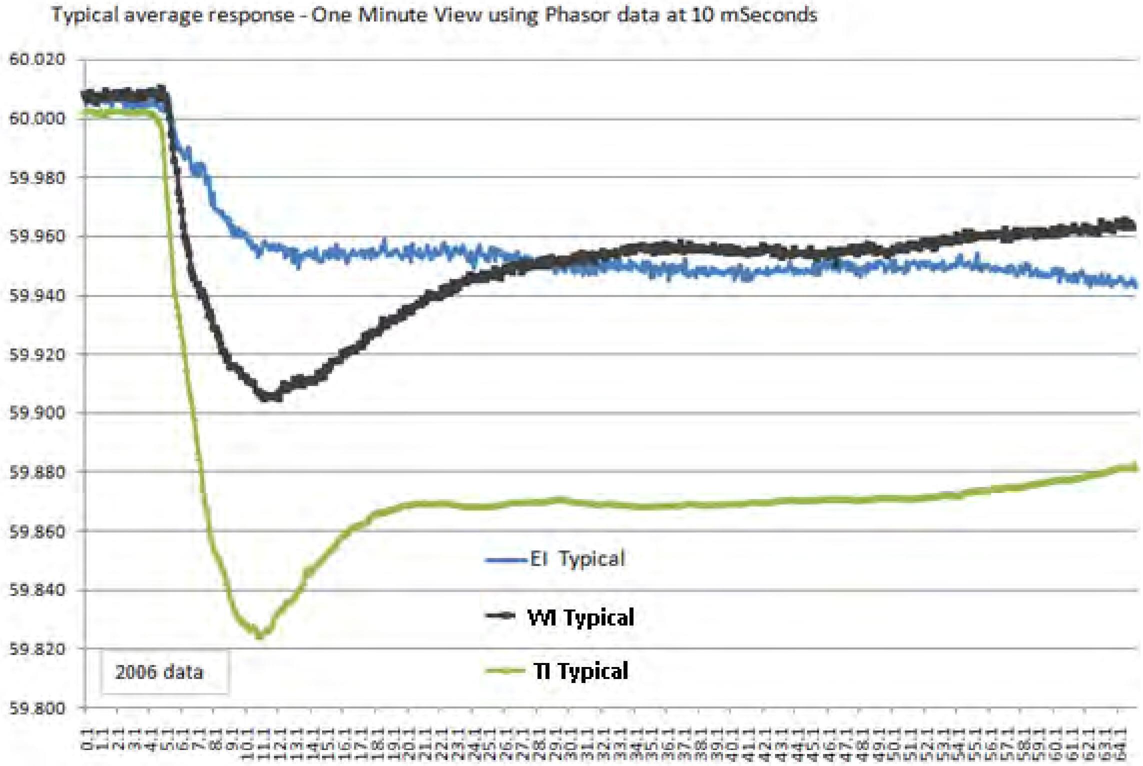


Figure 2.3: Typical Frequency Excursions

Important Concept: Following a large generator trip, frequency response will only stabilize the frequency of an Interconnection, arresting its decline. Frequency will not recover to scheduled frequency until the contingent BA replaces the lost generation through AGC and reserve deployment.

Figure 2.4 Shows the frequency at measured at various locations across the EI after a large generator trip. Note that the frequency disturbance is a chaotic event with complex dynamics, including fast transients bouncing about a much longer term trend. Also note that the time-scale tick-marks are every 5 seconds: the whole event has reached a stabilized frequency within 20 seconds.

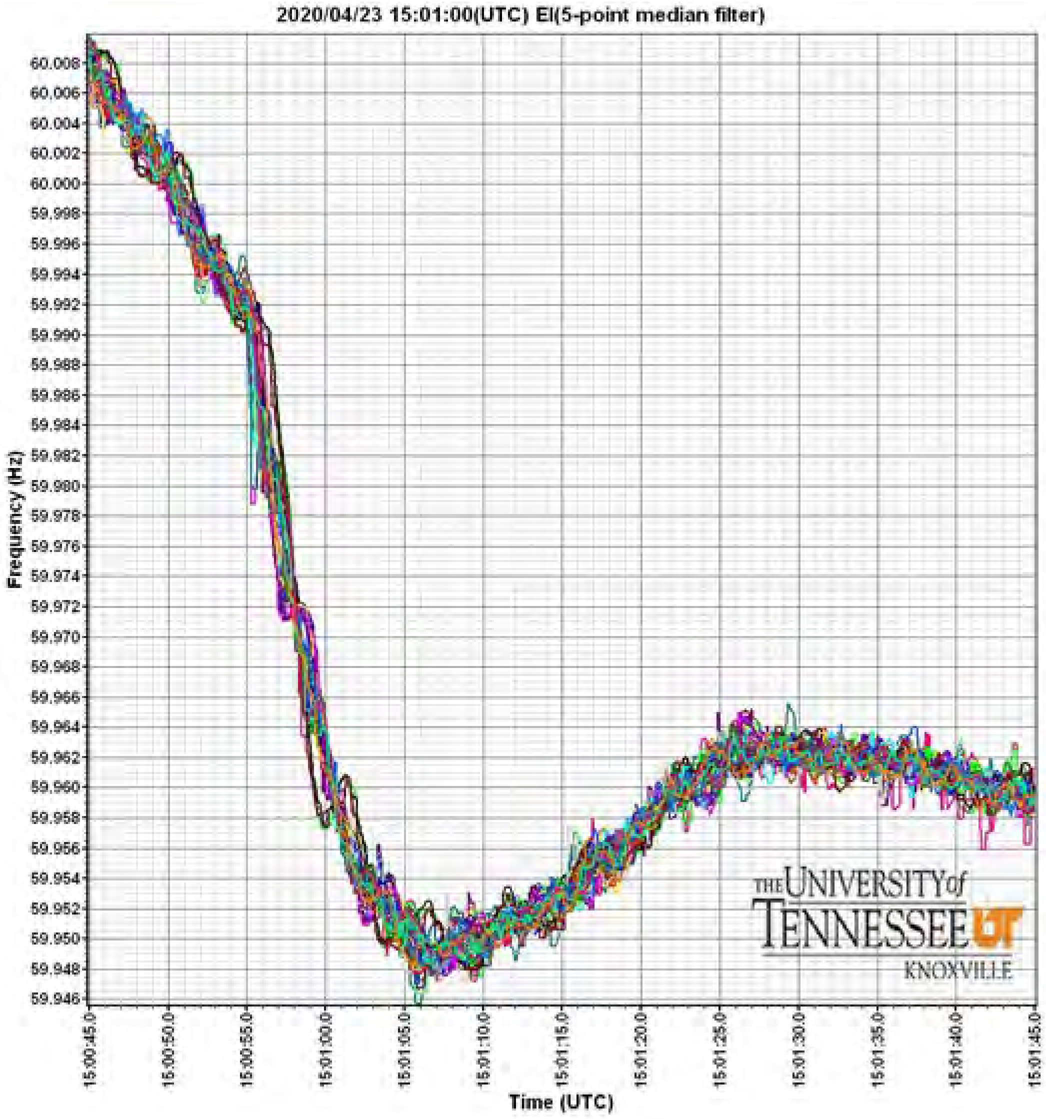


Figure 2.4: Frequency Excursion Measured at various locations in the EI

Annual Bias Calculation

The value in a BA properly stating its bias is to ensure its AGC control system does not cause unnecessary over-control of its generation.

The NERC RS posts quarterly lists of excursions that are available to the industry for everyone’s use for evaluating frequency response during the year. The subcommittee refines these quarterly lists into an official event list that is used in BAL-003 FRS forms.

Guidelines the RS uses in selecting and evaluating events for calculating bias and BAL-003 performance include the following:

- Events are dispersed throughout the year to get a good representation of “average” response.
- Pick frequency excursions large enough to actuate generator governors.
- The events should be relatively clean and generally have continuous drop from A to C.

- Starting frequency should be relatively stable and close to 60 Hz.

Estimating Load's Frequency Response

As discussed previously, motor load provides frequency response to the Interconnection. The rule of thumb is that this response is equal to 1–2% of load. Techniques have been developed to observe approximately how much "load" frequency response a BA has available. This technique is explained in **Figure 2.5**.

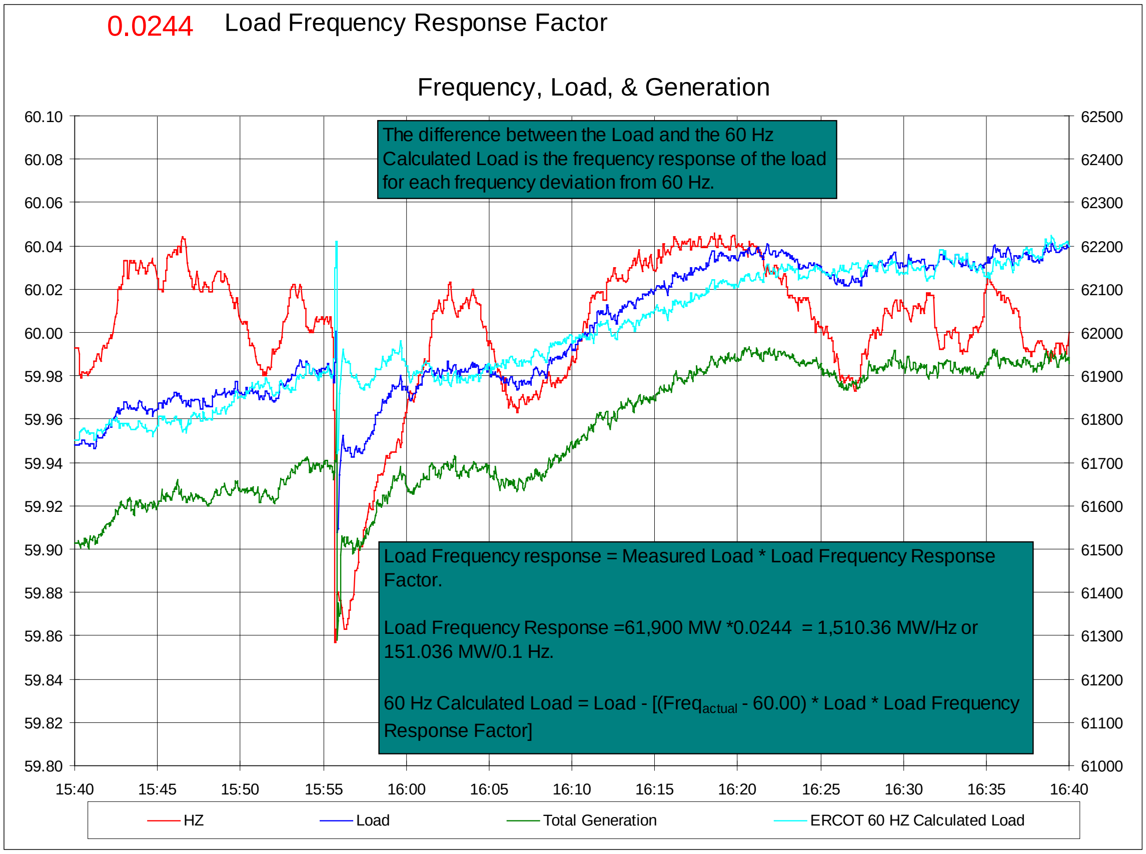


Figure 2.5: Observing Frequency Response of Load

The cyan trend in **Figure 2.5** above represents how much load would exist if frequency could be controlled to exactly 60.000 Hz all the time. The difference between the measured load, blue trend, and the cyan trend is the frequency response of load. For this event, a 759 MW resource was lost producing a frequency deviation of -0.118 Hz. This calculates to be

$$\frac{759\,MW}{0.118\,Hz * \left(\frac{10 * 0.1\,Hz}{Hz}\right)} = \frac{643\,MW}{0.1\,Hz} \text{ of frequency response.}$$

Of this response, 151.036 MW/0.1 Hz was provided by the load by multiplying the load by 0.00244, leaving the remainder (492.184 MW/0.1 Hz) provided by resource governor response. The post contingency total generation settled at 61,510 MW a difference of 178.222 MW below the pre-contingency generation. The generation-to-load mismatch post event is 178.222 MW plus replacement of the 580.777 MW of governor response (492.184 * 1.18 = 580.777) that will be withdrawn as frequency returns to 60.00 Hz. If this BA's bias in the ACE equation had been set exactly at 643 MW/0.1 Hz, ACE would equal -759 MW at the B point of this event. AGC would dispatch 759 MW to replace the frequency response of the governors and load, returning the Interconnection to balance at 60.00 Hz. This example is of a "single" BA Interconnection but the math works for multiple BA Interconnections as well.

By observing multiple events and adjusting the factor to produce a "60 Hz Load" value that maintains the pre- and post-event slope of load, a proper value can be determined. Larger deviation frequency events are beneficial to get a clear observation in addition to looking at many events. A factor between 0.010 and 0.025 would be reasonable depending on the ratio of motor load vs. non-motor load within the BAA boundaries.

The key points of primary control are as follows:

- Steady-state frequency is common throughout an Interconnection.
- If frequency is off schedule, generation is not in balance with total load.
- Arresting frequency deviations is the job of all BAs. This is achieved by provision of frequency response through the action of operating governors on generation and other resources able to provide frequency response (e.g., controllable load, storage, etc.).
- Frequency response is the sum of a BAs inertial response, natural load response and governor response of generators to frequency deviation within the BA Area.
- Frequency response arrests a frequency decline but does not bring it back to scheduled frequency. Returning to scheduled frequency occurs when the contingent BA restores its load-resource balance by using secondary control.
- Generators should be operated with their governors free to assist in stabilizing frequency.
- Frequency control during restoration is extremely important. That is why system operators should have knowledge of the generators' governor response capabilities during black start.
- All BAs have a frequency response characteristic based on the governor response of their units and the frequency-responsive nature of their load.
- The amount and rate of frequency deviation depends on the amount of imbalance in relation to the size of the Interconnection.
- Frequency bias is a negative number expressed in MW/0.1Hz.
- The preferred way to calculate frequency response is to observe the change in BA output for multiple events over a year.
- Under BAL-003-1.1 BA's should set its fixed bias to no less than the 100–125% of its natural frequency response or its percentage share of 0.9% of the Interconnection's non-coincidental peak load based upon all of the BAs within an Interconnection's non-coincident peak load values (whichever method is greater in absolute terms).
- BAs are allowed to employ variable frequency bias that more accurately reflects real-time operating condition.
- Governors were the first form of frequency control and remain in effect today; they act to oppose large changes in frequency.
- AGC supplements governor control by controlling actual tie flows and maintaining scheduled interchange at its desired value. It performs this function in the steady-state, seconds-to-minutes time frame after transient effects, including governor action, have taken place. If bias is greater than actual frequency response, AGC will supplement this response.
- ACE, the main input to AGC, requires frequency and energy interchange data (both actual and scheduled).
- While frequency response was declining in the 1990s, actions taken by the Industry appear to have stabilized the trend.
- BA or Interconnection frequency response should be measured for two reasons:
    - To gauge the area response to frequency deviations.

- As a basis for setting B.

Chapter 3: Secondary Control

Background

Secondary control is the combination of AGC and manual dispatch actions to maintain energy balance and scheduled frequency. In general, AGC utilizes maneuvering room while manual operator actions (e.g., communication to generators, purchases and sales, load management actions) keep repositioning the BAA so that AGC can respond to the remainder of the load and interchange schedule changes. NERC CPSs are intended to be the indicator of sufficiency of secondary control.

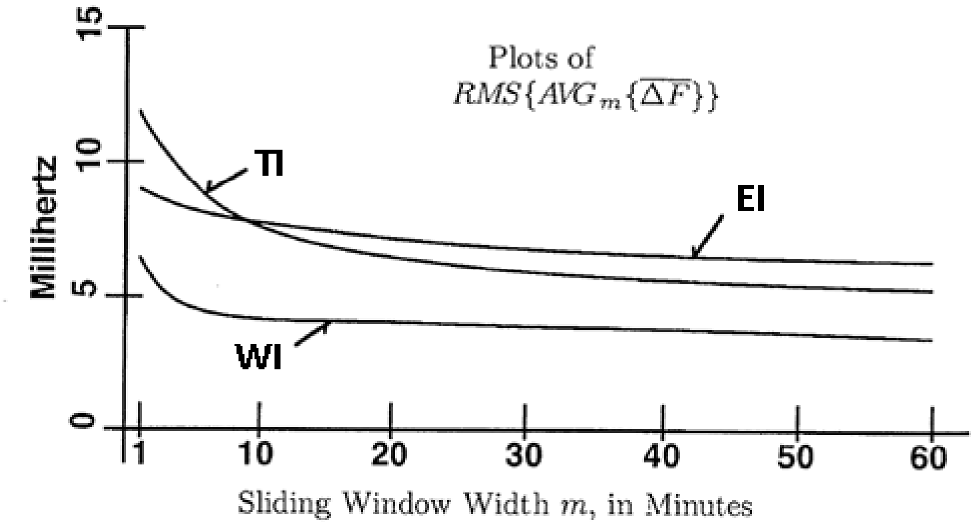
Maintaining an Acceptable Frequency Profile

One indicator of proper secondary control action is the distribution profile of steady-state Interconnection frequency. When the transition was made from the “A” criteria to CPS in 1997, the directive of the NERC Operating Committee was to not allow frequency variation to become any greater than it had been in the past. One measure of this is the root mean square (RMS) of frequency error from schedule. This by itself, however, is a measurement over an indefinite term and may not reveal problems at all averaging intervals. To adequately measure the frequency profile of an Interconnection, a statistical method was adopted in which period averages of RMS frequency error were measured and cataloged for periods of a large number of different values. In other words, the average of rolling N-minute RMS averages was computed for many values of N. This results in a defining profile as shown in **Figure 3.1** and **Figure 3.2.** Although other values could have been selected and ideally ALL values should be considered, the decision was made that the general profile would be maintained if the profile was anchored at two points in time (originally 1 minute and 10 minutes).

To set values for frequency performance, each Interconnection’s frequency error was observed by using the above method, and each one was characterized, particularly at their 10-minute interval average RMS frequency deviation from schedule. The EI measured 5.7 mHz at the 10-minute point. The 1-minute point used to set the CPS standard was derived from an “ideal” error characteristic by the ratio of square roots. This yields 5.7 * √(10) = 18.025 mHz. This value was rounded to the value in use today for the East, 18 mHz.

The same technique was used for the WI and TI. It is important to realize that CPS1 performance is only measured at this one “slice” (one-minute averaging) of the Interconnection’s frequency error characteristic. Because of this, there is no assurance that frequency variation will be constrained at other averaging points or converge on the ideal characteristic and become more random.

Initially, a 10-minute metric called CPS2 was developed to keep average ACE within specific bounds. CPS2 was originally used to help prevent excessive transmission flows due to large values of ACE. The problem with CPS2 was that it was not dependent on ACE’s impact on frequency. Additionally, CPS2 could cause control actions that moved against frequency. If a BA had very bad performance in one direction for five minutes, the BA could correct this by having equally bad performance in the opposite direction for the next five minutes. Finally, ACE could be totally unbounded for 10% of the month and it didn’t matter whether it was 1 or 1000 MW over the limit. CPS2 did not provide the correct signal for maintaining frequency. Ultimately, the industry adopted a frequency-sensitive longer term (i.e., 30 minute) measure called the BA ACE Limit (BAAL).



Frequency experience in the subject interconnections. Each ordinate point on these curves is the RMS value of the averages of $\overline{\Delta F}$ in windows of width m moved across the data string.

Figure 3.1: Interconnections with CPS actual-measured ΔF "period average"

Figure 3.1 Illustrates the actual-measured ΔF "period average" characteristic of the Interconnections with CPS was designed (EPRI report RP-3550, August, 1996). Note that these curves are flatter than what was ultimately selected as the epsilon limits in CPS1. The reason for this is that the standard needed to bound acceptable performance but not raise the bar and make it difficult to comply. For example, the 1-minute frequency variation in the East was about 10 mHz; if 10 mHz were chosen as Epsilon 1 in the East as opposed to the 18 mHz that was actually selected, it would mean that half the BAs in the East would have been out of compliance when the standard became active. Random (i.e., non-coincident) behavior of BAs in total is important in the above assumptions because the curves from which epsilon 1s were extrapolated start to deviate from the shape and predictability of the curves used to derive them as behavior becomes coincident (i.e., behaviors happening at the same time). Another way of saying this is that it becomes less and less valid to try to control frequency and measure performance at just one point on the sliding window continuum as coincidence creeps in. Prior to the adoption of the BAAL, the Interconnections would see wider frequency swings at specific times of day, particularly in the low direction. The swings, due primarily to load changes and large block Interchange Schedules, could occur under CPS2. The number and magnitude of frequency swings were reduced through a combination of tools that identified the contributing BAs as well as the adoption of BAAL.

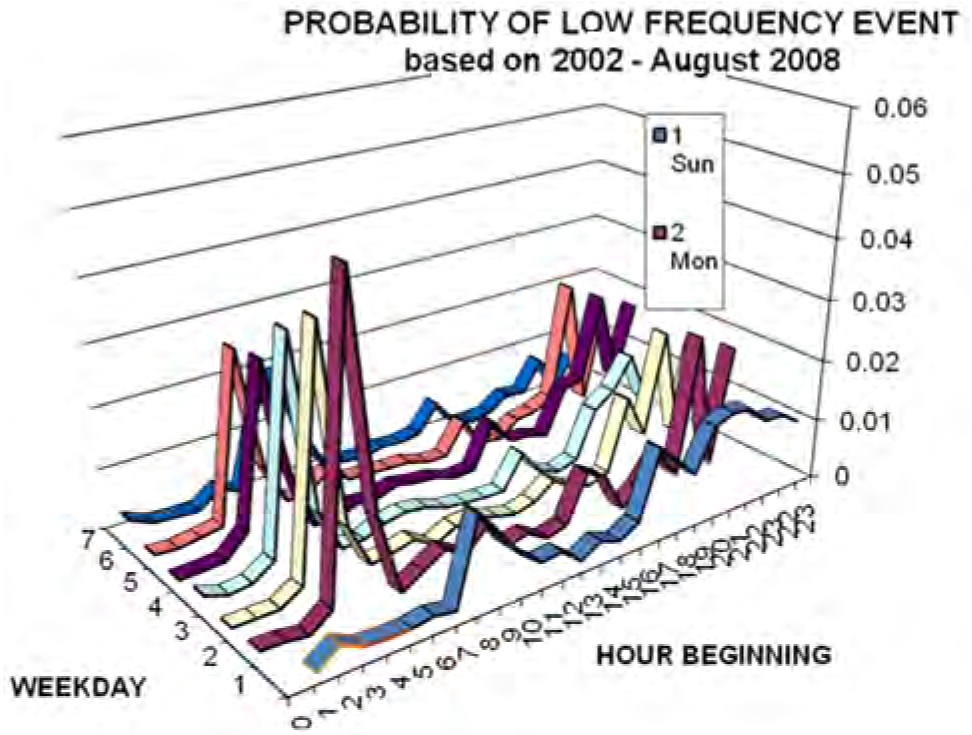


Figure 3.2: Probability Distribution for Low-Frequency Events vs. Time of Day

Control Performance Standard 1

In simple terms, CPS1 assigns each BA a share of the responsibility for control of steady-state Interconnection frequency. The amount of responsibility is directly related to BA frequency bias.

As mentioned previously, ACE is to a BA what frequency is to the Interconnection. Over-generation makes ACE go positive and frequency increase while negative ACE "drags" on Interconnection and decreases frequency. "Noisy" ACE tends to cause "noisy" frequency. CPS1 captures these relationships using statistical measures to determine each BA's contribution to such "noise" relative to what is deemed permissible.

The CPS1 equation can be simplified as follows:

- CPS1 (in percent) = 100* [2 – (a Constant[16])* (frequency error)*(ACE)]

Frequency error is deviation from scheduled frequency, normally 60Hz. Scheduled frequency is different during a time correction, but for the purposes of this discussion, assume scheduled frequency is 60 Hz.

Refer to the equation above. Any minute where the average frequency is exactly on schedule or BA ACE is zero, the quantity ((frequency error)*(ACE)) is zero. Therefore, CPS1 = 100* (2-0), or 200%. This is true whenever frequency is on schedule or ACE is zero.

For any one-minute average where ACE and frequency error are "out of phase," CPS1 is greater than 200%. For example, if frequency is low, but ACE is positive (tending to correct frequency error), the BA gets extra CPS1 points.

[16] The size of this constant changes over time for BAs with variable bias, but the effect can be ignored when considering minute-to-minute operation. It is equal to -10 * B / ε_1^2

Operating Tip: Frequency is generally low when load is increasing and high when load is dropping. Anticipating and staying slightly "ahead of the load" and on the assistive side of frequency correction with your generation will give your BA high CPS1 scores over the long run.

Conversely, if ACE is aggravating the frequency error, CPS1 will be less than 200%. CPS1 can even go negative.

TI and QI Note: The TI and QI operate as single BA's. ACE for a single BA Interconnection will always be "in phase" with frequency error; refer to the ACE review for verification. This means the largest CPS1 these BA's can achieve is 200%. This occurs whenever ACE or frequency error is zero. CPS1 for these BA's is a function of "frequency squared."

The CONSTANT in the equation above is sized such that the BA will get a CPS1 of 100% if the BA's ACE is proportionally as "noisy" as a benchmark frequency noise. The minimum acceptable rolling twelve-month score for CPS1 is 100%.

When CPS was established, each Interconnection was given a target or benchmark "frequency noise." This target noise is called Epsilon 1(ε1). Epsilon 1 is nothing more than a statistician's variable that means the RMS value of the one-minute averages of frequency.

The target values (in mHz of frequency noise) for each Interconnection are shown in **Table 3.1** below. The NERC RS monitors each Interconnection's frequency performance and can adjust the ε1 values should an Interconnection's frequency performance decline.

Table 3.1: Target Values of "One Minute Frequency Noise"

Interconnection	Epsilon 1 (ε1)
Eastern	18.0 mHz
Quebec	21.0 mHz
Western	22.8 mHz
Texas	30.0 mHz

The Epsilon 1 target initially set for each Interconnection was on the order of 1.6 times the historic frequency noise. This means a typical BAs performance would be around 160% for CPS1. If every BA in an Interconnection were performing with a CPS1 of 100%, it would result in an observed Interconnection frequency performance of ε1 (i.e.18mHz in the East).

Let's review how CPS1 data can be applied to measure the adequacy of control performance and the deployment of resource-provided services to meet load. NERC previously referred to these resources as interconnected operating services (ERSs). More recently, the term essential reliability services is used. These align somewhat to what FERC calls "ancillary services."

Figure 3.3 depicts ACE charts for one hour for four different BAs. Compare the charts for BAs 1 and 2. Both BAs show good performance for the hour. The difference between them is that the load in BA 2 is "noisier."

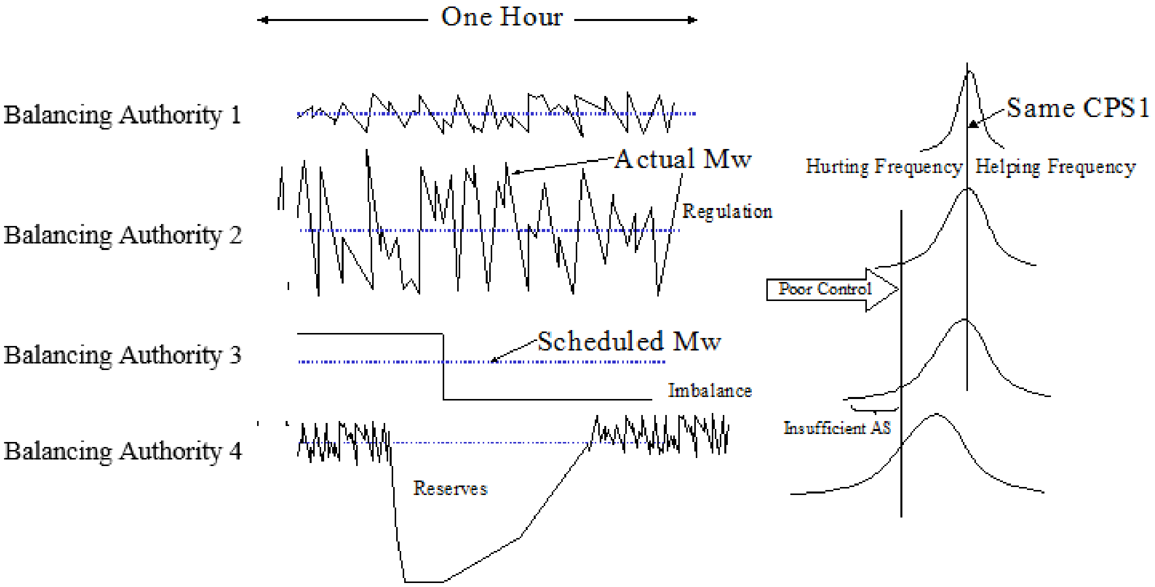


Figure 3.3: ERS/Ancillary Service Measured via CPS

The distributions to the right of the ACE charts show the individual one-minute CPS1 for both BAs for the hour. If frequency followed a normal pattern whereby it fluctuated +/- a few mHz from 60 Hz, the CPS1 curves for BA 1 and 2 would look like the distributions to the right of their ACE charts. Both curves would have the same average (about 160 percent CPS1), but BA 2's curve would be "wider."

Even though the average effect of BA 1 and 2 on the Interconnection is the same, BA 2 sometimes places a greater burden on the Interconnection as demonstrated by the size of the "left hand tail" of the CPS1 curve. A very long left tail implies poor control of some type (regulation in this case).

Now look at BA 3. It is a "generation only" BA that is selling 100 MW for the hour. The problem is that it is meeting this requirement by generating 200 MW for the first 30 minutes and 0 MW for the last half hour. Again, if frequency conditions are normal, half the time the BA will be helping frequency back towards 60 Hz and half the time the BA will be hurting frequency. This means the BA will get an "Interconnection average" CPS1 score of about 160% for the hour. The graph of its CPS1 for the hour will have wider tails, much like BA 2. The underlying problem in this case is imbalance, not regulation.

The ACE chart for BA 4 shows that a generator tripped offline during the hour. If the CPS1 one-minute averages are plotted, the curve will also have wider tails. If the unit that was lost was large, the curve will be "skewed" to the left even further. This is because the unit loss will pull frequency down while ACE is a large negative value.

In each case above, there was a deficiency in one of the energy-based ERSs. The "left tail" of the underlying CPS1 curve captured each situation.

Balancing Authority ACE Limit

In simple terms, BAAL assigns each BA a share of the responsibility for control of steady-state Interconnection frequency. The amount of responsibility is directly related to BA frequency bias and any deviation of Interconnection frequency from the Interconnections scheduled frequency.

The BAAL is calculated from the clock minutes averages of the data as follows:

Frequency Trigger Limits:

- FTL_{High} = Scheduled Frequency + 3*ε1
- FTL_{Low} = Scheduled Frequency - 3*ε1

As an example, for the EI (where epsilon1 = 0.018 mHz) and when the Interconnection is not in a time error correction (TEC) the FTL's are:

- FTL_{High} = 60.054 Hz
- FTL_{Low} = 59.946 Hz

Calculating the BAAL limits when actual frequency <> scheduled frequency:
As an example, for a BA with a frequency bias Setting = -1000MW/0.1Hz

- $BAAL_{Low} = (-10 * B * (FTL_{Low} - F_S)) * ((FTL_{Low} - F_S)/ (F_A-F_S))$
- $BAAL_{Low =} (-10*-1000* (59.946 – 60)) * (59.946 – 60)/ (F_A – 60))$

- $BAAL_{High} = (-10 * B * (FTL_{High} - F_S)) * ((FTL_{High} - F_S)/ (F_A-F_S))$
- $BAAL_{High =} (-10*-1000* (60.054 – 60)) * (60.054 – 60)/ (F_A – 60))$

Results with actual varying frequency are shown in **Table 3.2.**

Table 3.2: Varying Frequency Results

Actual Frequency	$BAAL_{High}$	$BAAL_{Low}$
60.09	324	NA
60.081	360	NA
60.072	405	NA
60.063	463	NA
60.054	540	NA
60.045	648	NA
60.036	810	NA
60.027	1080	NA
60.018	1620	NA
59.982	NA	-1080
59.973	NA	-720
59.964	NA	-540
59.955	NA	-432

Table 3.2: Varying Frequency Results		
Actual Frequency	**$\text{BAAL}_{\text{High}}$**	**BAAL_{Low}**
59.946	NA	-360
59.937	NA	-309
59.928	NA	-270
59.919	NA	-240
59.91	NA	-216

The BAAL limits plotted in **Figure 3.4** detail the acceptable operating area and the BAAL limit exceedance area.

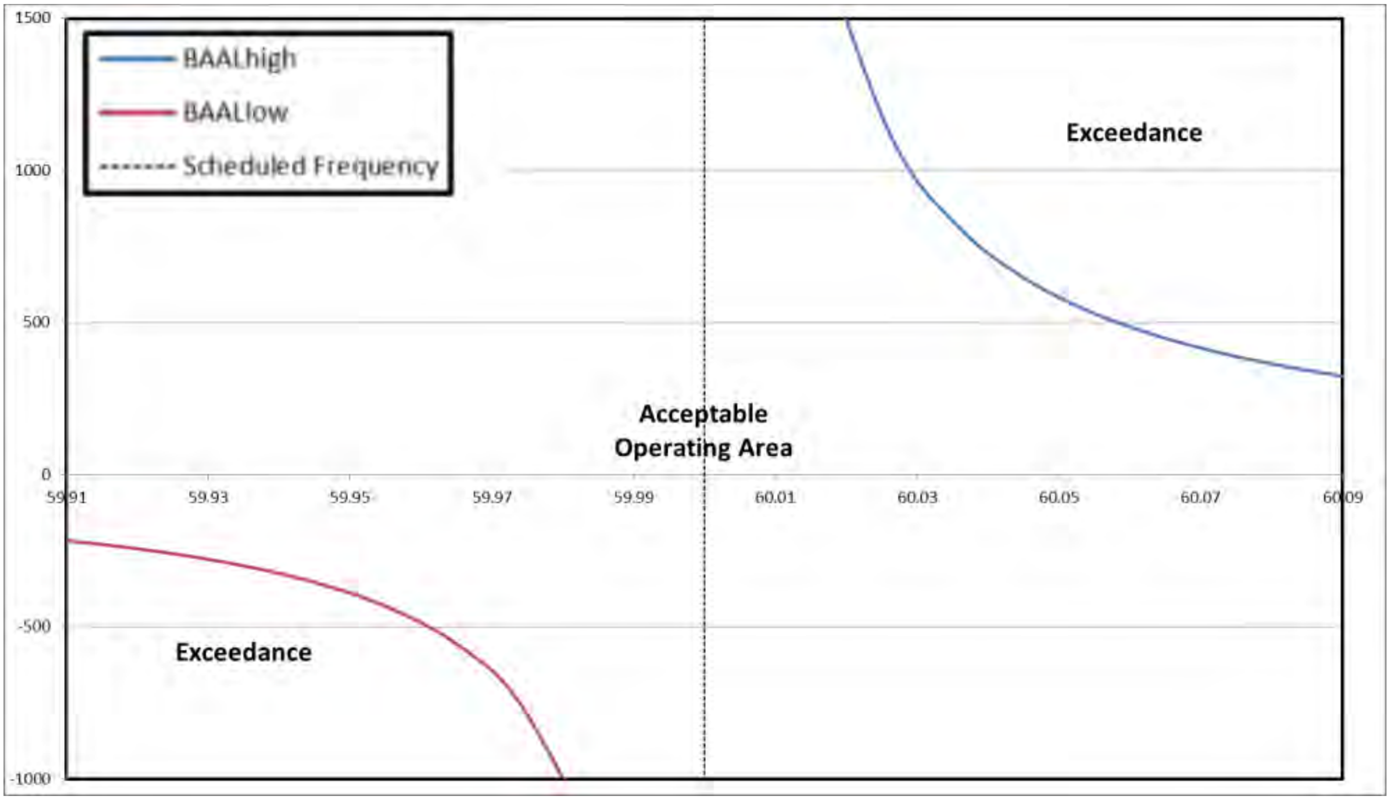


Figure 3.4: Acceptable Operating Area and the BAAL limit exceedance area

As a BA is operating and managing its ACE, the clock-minute averages of ACE are being evaluated against the BAAL limits.

CPS1 Equivalent Limit Derivation

BAAL is mathematically related to CPS1 as shown below:

- By definition; CF = $(\text{RACE}/(-10B) * (F_A - F_S)) / (\varepsilon_1{}^2)$, and CPS1 = 2-CF
- Substituting for CF; CPS1 = $2-(\text{RACE}/(-10B) * (F_A - F_S)) / (\varepsilon_1{}^2))$

- Regrouping terms; CPS1 = 2 - RACE * $((F_A - F_S)/ (-10B^* \varepsilon_1{}^2))$
- Substituting BAAL for RACE; CPS1 = 2 - 9 * $(-10B^* \varepsilon_1{}^2) / (F_A - F_S) * ((F_A - F_S)/(-10B^* \varepsilon_1{}^2))$
- Cancelling out terms; CPS1 = 2 – 9= -7 = -700%

Therefore, a one-minute CPS1 score more negative than -700% will equate to a BAAL exceedance for that one-minute period.

The minimum acceptable time frame for continuous BAAL minute exceedances shall not continue for greater than thirty minutes.

Quick Review

- CPS1 assigns each BA a share of the responsibility for control of Interconnection frequency.
- CPS1 is a yearly (i.e., rolling twelve month) standard that measures impact on frequency error with a 100% minimum allowable score.
- BAAL is a 30-minute standard intended to bind a BAs real-time impact on frequency.

Chapter 4: Tertiary Control

Tertiary Control generally follows disturbances and reserve deployment to reestablish resources for future contingencies. Reserve deployment and reserve restoration following a disturbance are common types of Tertiary Control. See the Operating Reserve Management Reliability Guideline for more information.

Understanding Reserves

There is often confusion when operators and planners talk about reserves. One major reason for misunderstanding is a lack of common definitions; NERC's definitions have changed over time. In addition, most NERC Regions developed their own definitions. Capacity obligations have historically been the purview of state and provincial regulatory bodies, meaning that there are many different expectations and obligations across North America.

In order to foster discussion and develop a more uniform understanding of the reserve data, the following definitions are provided in this reference. Refer to **Figure 4.1** to better understand the definitions.

Definitions:

(Capitalized terms are taken from NERC Glossary and lower case are not.)

Contingency Reserve: The provision of capacity deployed by the BA to respond to a Balancing Contingency Event and other contingency requirements (such as Energy Emergency Alerts as specified in the associated NERC Standards). This is the left column of Operating Reserves in Figure 4.1

frequency-responsive reserve: On-line generation with headroom that has been tested and verified to be capable of providing droop as described in the Primary Frequency Response guideline. Variable load that mirrors governor droop and dead-band may also be considered frequency responsive reserve.

Interruptible Load: Demand that the end-use customer makes available to its Load-Serving Entity via contract or agreement for curtailment that can be interrupted within 10 minutes.

Operating Reserve: That capability above firm system demand required to provide for regulation, load forecasting error, equipment forced and scheduled outages, and local area protection.

Operating Reserve–Spinning: Generation synchronized to the system and fully available to serve load within the Disturbance Recovery Period following the contingency event or Load fully removable from the system within the Disturbance Recovery Period following the contingency event deployable in 10 minutes.

Operating Reserve Supplemental: Generation (synchronized or capable of being synchronized to the system) that is fully available to serve load within the Disturbance Recovery Period following the contingency event or Load fully removable from the system within the Disturbance Recovery Period following the contingency event that can be removed from the system, within 10 minutes.

planning reserve: The difference between a BA's expected annual peak capability and its expected annual peak demand expressed as a percentage of the annual peak demand. See BAL-502-RF-03 for additional discussion.

Regulating Reserve: An amount of Operating Reserve – Spinning responsive to Automatic Generation Control, which is sufficient to provide normal regulating margin.

replacement reserve: NOTE: Each NERC Region sets times for reserve restoration, typically in the 60–90-minute range. The NERC default contingency reserve restoration period is 90 minutes after the disturbance recovery period.

Supplemental Reserve Service: Provides additional capacity from electricity generators that can be used to respond to a contingency within a short period, usually ten minutes. An ancillary service identified in FERC Order 888 as necessary to affect a transfer of electricity between purchasing and selling entities. This is effectively FERC's equivalent to NERC's Operating Reserve.

Much like parts kept in a storeroom, reserves are meant to be used when the need arises. Reserves can be low for short periods of time due to plant equipment problems and unit trips and can also be misstated

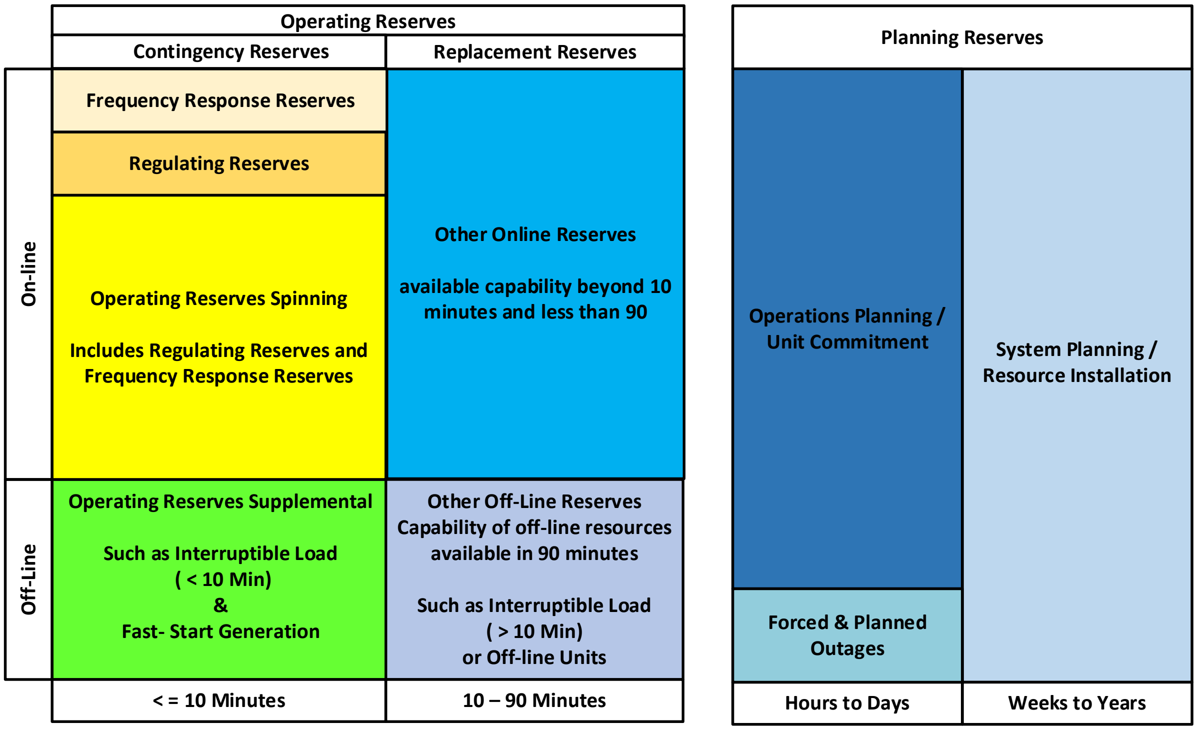

Operating Reserves
Contingency Reserves
Replacement Reserves
On-line
Off-Line
Frequency Response Reserves
Regulating Reserves
Operating Reserves Spinning
Includes Regulating Reserves and Frequency Response Reserves
Other Online Reserves
available capability beyond 10 minutes and less than 90
Operating Reserves Supplemental
Such as Interruptible Load (< 10 Min) & Fast- Start Generation
Other Off-Line Reserves Capability of off-line resources available in 90 minutes
Such as Interruptible Load (> 10 Min) or Off-line Units
< = 10 Minutes
10 – 90 Minutes
Planning Reserves
Operations Planning / Unit Commitment
Forced & Planned Outages
System Planning / Resource Installation
Hours to Days
Weeks to Years

Figure 4.1: Reserves Continuum

Chapter 5: Time Control and Inadvertent Interchange

Background

There is a strong interrelationship between control of time error and Inadvertent Interchange (aka. "inadvertent"). Time error occurs when one or more BAs has imprecise control or large resource losses occur, causing average actual frequency to deviate from scheduled frequency. The bias term in the ACE equation of the remaining BAs causes control actions that result in flows between BAAs in the opposite direction. The net accumulation of all these interchange errors is referred to as Inadvertent Interchange. Inadvertent interchange represents the amount by which actual flows between BAAs and the remainder of the Interconnection differs from the intended or scheduled flows.

Time Control

As noted earlier, frequency control and balancing control are not perfect. There will always be some errors in tie-line meters. Due to load and generation variation, net ACE in an Interconnection cannot be maintained at zero. This means that frequency will vary from 60 Hz over time.

An Interconnection may have a time control process to maintain the long-term average frequency at 60 Hz. While there are some differences in process, each Interconnection that exercises time control designates an RC as a "time monitor" to coordinate time control.

Time error corrections are initiated when long-term average frequency drifts from 60 Hz. In the EI, a 0.02Hz offset to scheduled frequency corrects 1.2 seconds on the clock for each hour of the time error correction, provided the offset scheduled frequency is achieved.

There has been an ongoing debate on the need for time error corrections. The number of time error corrections do provide a benchmark for the quality of frequency control and provide an early warning of chronic balancing problems. While the value of time control is debatable from a reliability perspective, nobody can say with assurance who or what would be impacted if NERC and NAESB halted the practice of manual time error corrections. This practice was removed from the NERC standards in 2017, but still remains in the NAESB standards.

Inadvertent Interchange

Inadvertent interchange is net imbalance of energy between a BA and the Interconnection. The formula for inadvertent interchange is:

- $NI_I = NI_A - NI_S$

where,

NI_A is net actual interchange. It is the algebraic sum of the hourly integrated energy on a BAs tie lines. Net actual interchange is positive for power leaving the system and negative for power entering.

NI_S is net scheduled interchange. It is defined as the mutually prearranged net energy to be delivered or received on a BAs tie lines. Net scheduled interchange is positive for power scheduled to be delivered from the system and negative for power scheduled to be received into the system.

Inadvertent interchange and can be divided into two categories, described below.

Primary Inadvertent

Primary inadvertent interchange is caused by problems or action from within a given BA. Primary inadvertent interchange occurs due to the following:

- Error in scheduled interchange
  - Improper entry of data (time, amount, direction, duration, etc.…)
  - Improper update in real-time (TLR miscommunication etc.…)
  - Ramp procedures
  - Miscellaneous (phantom schedules, selling off the ties, etc.…)
- Error in actual interchange (meter error)
  - Loss of telemetry
  - Differences between real-time power (MW, for ACE), and energy (MWh), integrated values
- Control error or offset
  - Load volatility and unpredictability
  - Generation outages
  - Generation uninstructed deviations
  - Physical rate-of-change-of-production limitations
  - Deliberate control offset (i.e. unilateral payback) to reduce inadvertent energy balances

Hourly primary inadvertent can be calculated for each BA by using the following formula:

$$(PII_{hourly}) = (1\text{-}Y) * (II_{actual} - Bi * \Delta TE/6)$$

- PII_{hourly} is the BAs primary inadvertent for an operating hour expressed in MWh
- Y is the ratio between a BAs frequency bias setting and the sum of all BAs frequency bias setting within an Interconnection
- Bi is the BAs frequency bias
- ΔTE is the change in time error within the Interconnection that occurred during the operating hour

Secondary Inadvertent

Balancing problems external to a BA will cause off-schedule frequency. If frequency is low, the bias term of the ACE equation will cause a BA to slightly over-generate after initial effects to stabilize frequency, such as governor response and load damping. Conversely, if frequency is high, the bias term of the ACE equation will cause slight under generation. This intentional outflow or inflow to stabilize frequency due to problems outside the BA causes deviation from the schedule and is called secondary inadvertent interchange.

Hourly secondary inadvertent can be derived by subtracting a BA’s hourly primary inadvertent from their hourly total inadvertent.

Quick Review: If one or more BAs have a control problem, it could result in a large primary inadvertent interchange. This may also cause off-nominal frequency, potentially spreading Secondary inadvertent interchange to the other BAs. The off-normal frequency then results in accumulated time error, potentially triggering time error corrections.

Chapter 6: Frequency Correction and Intervention

Background

There are several requirements in NERC reliability standards that tell the BA, Transmission Operator, and RC to monitor and control frequency. The standards do not provide specific guidance on what is normal frequency and under what conditions the operator should intervene.

As noted earlier in this document, this information is provided for guidance and understanding. It should not be used for compliance purposes and does not establish new requirements or obligations.

The BAAL is the ACE-frequency combination equivalent to instantaneous CPS1 of -700%. In general, if one or more of the RC's BAs is beyond the BAAL for more than 15 minutes, the RC should contact the BA to determine the underlying cause. As frequency diverges more from 60 Hz, the RC and BA should be more aggressive in their actions.

One of the primary responsibilities of the RCs is frequency protection. Suggested actions are outlined below.

1. Identify BAs within your area beyond BAAL. Direct correction and log. RCs to notify BAs.
2. Call Other RCs, communicate problem if known. Search for cause if none reported. Notify time monitor of findings. Time monitor to log. Direct BAs beyond BAAL to correct ACE.
3. Direct all BAs with ACE hurting frequency to correct. Time monitor to notify Resource Subcommittee after the fact.
4. Evaluate whether still interconnected. Direct emergency action.

Revision History

Date	Version Number	Reason/Comments
4-5-2011	1.0	Initial Version
5-11-2021	2.0	Resources Subcommittee Review

Appendix A: References

Cohn, N. (May 1982). Decomposition of Time Deviation and Inadvertent Interchange on Interconnected System, Parts I & II. *IEEE PAS, Vol. PAS-101, No. 5.*

Cohn, N. (1956). Some Aspects of Tie-Line Bias Control on Interconnected Power Systems, *AIEE Transactions, vol. 75, pt. III (Power Apparatus and Systems)*, 1415-1436.

Cohn, N. (1984). Recollections of the Evolution of Real-time Control Applications to Power Systems, *Automatica, vol. 20, no. 2*, 145-162.

Electric Power Research Institute (1992). *Impacts of Governor Response Changes on the Security of North American Interconnections*.

Electric Power Research Institute (1996). *Control Performance Standards and Procedures for Interconnected Operations, EPRI RP3555-10*.

Ingleson, J., & Nagle, M. (May, 1999). *Decline of Eastern Interconnection Frequency Response.* Prepared for the Fault and Disturbance Conference at Georgia Tech. Retrieved May 19, 2004 from http://truc.org/files/1999/fda1999_jwi_final.pdf.

Ingleson, J., & Ellis, D. (2005). *Tracking the Eastern Interconnection Frequency Governing Characteristic*. Summer, 2005 IEEE/PES.

Jaleeli, N. & VanSlyck, L.S. (August 1999). NERC's New Control Performance Standards. IEEE T-PWRS Vol. 14, No. 3, pp 1092-1099.

Jaleeli, N., VanSlyck, L. S., Ewart, D. N., Fink, L. H. and Hoffmann, A. G. (August 1992). Understanding Automatic Generation Control. IEEE T-PWRS Vol. 7, No. 3, pp 1106-1122.

Kirby, B., Dyer, J., Martinez, C., Shoureshi, R., Guttromson, R., & Dagle, J. (December 2002). *Frequency Control Concerns In The North American Electric Power System, ORNL/TM-2003/41*. Oak Ridge, TN: Oak Ridge National Laboratory.
Lindahl, S.(2002). *Verification of Governor Response during Normal Operation*. Retrieved November 5, 2003 from http://www.eeh.ee.ethz.ch/downloads/psl/research/psdpc/.

Moran, F. & Williams, D.R. (April 1968). Automatic control of power-system frequency by machine controllers, *Proceeding of the IEE, vol. 115, no. 4*, 606-614.

Moran, F., Bain, D.K.S., & Sohal, J.S. (July 1968). Development of the equipment required for the loading of turbogenerators under automatic power-system control, *Proceedings of the IEE, vol. 115, no 7*, 1067-1075.

NAESB WEQ Manual Time Error Correction Standards - WEQBPS – 004-000

NERC (2002, August 28). *Frequency Excursion Task Force Report*. North American Electric Reliability Council.

NERC (2006). *Frequency Response Characteristic Survey Training Document.* North American Electric Reliability Council.

NERC Frequency Response Standard White Paper, April 6, 2004

NERC (2004). *Inadvertent Interchange Accounting Training Document*.

NERC (2004). Performance *Standard Training Document*. North American Electric Reliability Council.

NERC (2004). *Area Interchange Error Survey Training Document*. North American Electric Reliability Council.

NERC. *Area Interchange Error Reports*. Available at www.nerc.com/~filez/aie.html.

NERC Joint Inadvertent Interchange Task Force (2001). *Draft Guiding Principles for an Inadvertent Interchange Standards*. North American Electric Reliability Council.

NERC (2005). *Reliability Standards for the Bulk Electric Systems of North America*. North American Electric Reliability Council.

UCTE. *Policy 1 — Load-Frequency Control and Performance*. Draft Operating Standard for Europe. Retrieved November 5, 2003 from http://europa.eu.int/comm/energy/.

VanSlyck, L.S., Jaleeli, N. & Kelley, W.R. (May, 1989). Implications of Frequency Control Bias Settings on Interconnected System Operation and Inadvertent Energy Accounting. *IEEE Transactions on Power Systems*, *vol. 4*, *no. 2*, 712-723.

U.S.-Canada Power System Outage Task Force (2004, April 5*). Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Balancing and Frequency Control

Reference Document

Prepared by the NERC Resources Subcommittee

~~September 29, 2020~~May 11, 2021

RELIABILITY | RESILIENCE | SECURITY

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

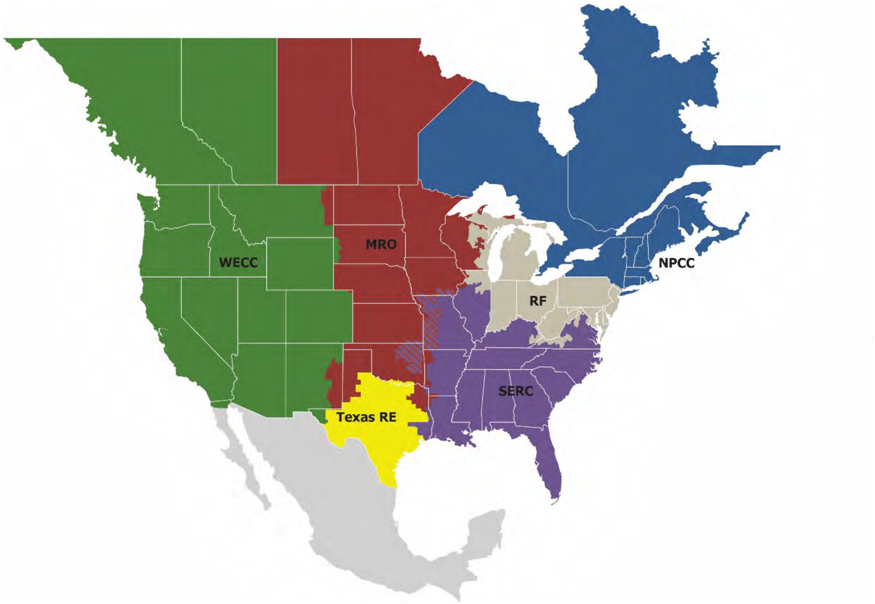
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



The Six Regional Entities	
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Background

The NERC Resources Subcommittee (RS) drafted this reference document at the request of the NERC Operating Committee as part of a series on operating and planning reliability concepts. The document covers balancing and frequency control concepts, issues, and recommendations. Send questions and suggestions for changes and additions to balancing@nerc.com.

Note to Trainers

Trainers are encouraged to develop and share materials based on this reference. The RS will post supporting information on the RS website.[1]

Disclaimer

This document is intended to explain the concepts and issues of balancing and frequency control. The goal is to provide an understanding of the fundamentals. Nothing in this document is intended to be used for compliance purposes or to establish obligations.

[1] https://www.nerc.com/comm/OC/Pages/Resources-Subcommittee.aspx

Chapter 1: Balancing Fundamentals

Balancing and Frequency Control Basics

The power system of North America is divided into four major Interconnections (see **Figure 1.1**). These Interconnections can be thought of as independent electrical islands. The four Interconnections consist of the following:

- **Western** Interconnection (WI)**:** Generally everything west of the Rockies
- **Texas** Interconnection (TI)**:** Operated by the Electric Reliability Council of Texas (ERCOT)
- **Eastern** Interconnection (EI)**:** Generally everything east of the Rockies except Texas and Quebec
- **Quebec** Interconnection (QI)**:** Operated by Hydro Quebec TransEnergie

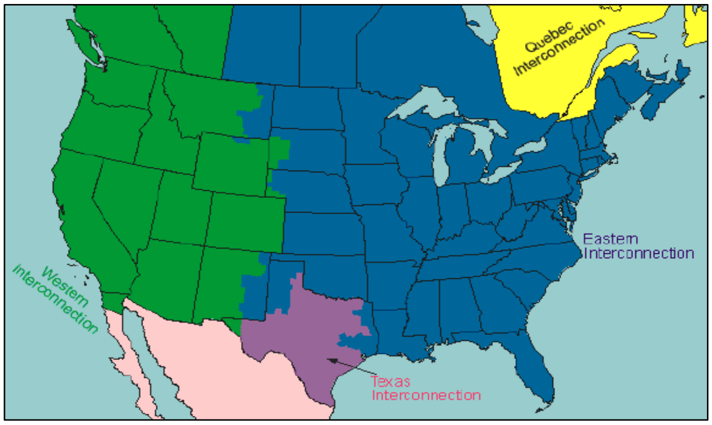


Figure 1.1: North American Interconnections

Each Interconnection can be viewed as a single large machine with every generator pulling together to supply electricity to all customers. This occurs as the electric generating units rotate (in steady-state) ~~near synchronism~~synchronously. The "speed" (rotational speed) of the Interconnection is frequency measured in cycles per second, or Hertz (Hz). When the total Interconnection supply exceeds customer demand, frequency increases beyond the scheduled value (typically 60 Hz[2]) until energy balance is achieved. Conversely, when there is a temporary supply deficiency, frequency declines until a balance between supply and demand is restored.

Commented [sjr1]: I think this is correct. As frequency falls, all machines giving up inertia are still in sync. Bill?

Commented [BH2R1]: I am okay with this change

During normal operations it is typical for there to be small mismatches between total demand and total supply, so the frequency of each Interconnection varies above and below nominal on a continuous basis. Regardless of whether the variations are above or below scheduled frequency, the supply-demand balance is restored due to frequency sensitive demands and supply resources that change output in response to frequency changes. For example, some electric devices (e.g., electric motors) use more energy if driven at a higher frequency and less at a lower frequency. Most generating units are also equipped with governors that cause the generator to inject more energy into the Interconnection when frequency is lower than nominal and slightly less energy when the frequency is higher than nominal.

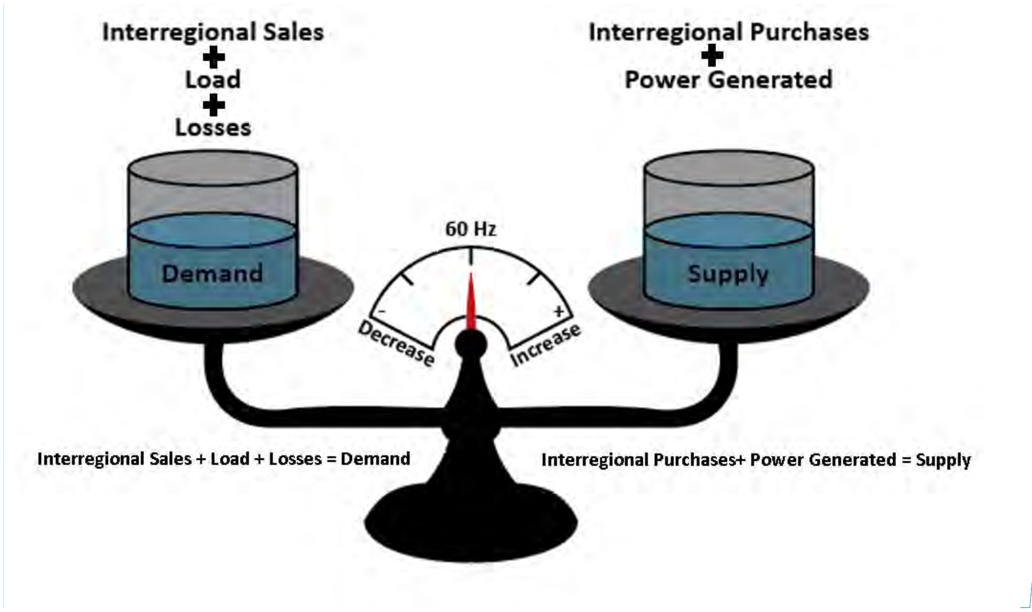
[2] Nominal frequency (termed "scheduled frequency") is sometimes intentionally offset by a small amount via a mechanism called time error corrections to correct for sustained periods of high or low frequency.

Balancing Authorities (BAs) balance generation and load within their Balancing Authority Areas (BAAs) of the Interconnections. See **Figure 1.2** for an example of BAAs across North America. The BAs dispatch generating resources in order to meet their BAA demand and manage the supply/demand balance. Some BAs also control demand to maintain the supply/demand balance.

Figure 1.2: North American Balancing Authorities and Regions

The number of BAs in an Interconnection varies; Texas and Quebec are single BA Interconnections while the Eastern and the Western are multi-BA Interconnections. Each BA in an Interconnection is connected via high voltage transmission lines (called tie-lines) to neighboring BAs. The Reliability Coordinators (RCs) oversee the BA operations and coordination. BAs are responsible for the supply/demand balance within their BAA while RCs are responsible for the wide area health of the Interconnection.

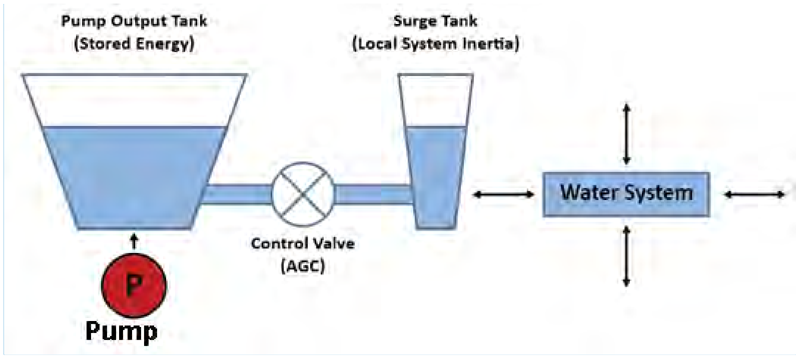
Frequency will be constant in an Interconnection when there is a balance between supply and demand, including various electrical losses. This balance is depicted in **Figure 1.3**.



Commented [BH3]: I replaced

Figure 1.3: Generation | Demand Balance

Each supply resource embedded in an interconnected system has its own characteristics (e.g., ramp rates, fuel supply, output controllability and sustainability). From a simplified viewpoint, a supply resource can be analogized to a water pump with storage and control as shown in **Figure 1.4**. In this example, the pump's output fills an open storage tank similar to a swimming pool. The water depth in the tank needs to be controlled to within very tight limits: too much water accumulating will cause the pool to overflow, and too little water will cause other problems. The control valve changes average output to meet system demand in a manner analogous to automatic generation control (AGC). The surge tank on the final output is analogous to the rotational inertia of the generator.



Commented [BH4]: I replaced

Figure 1.4: Generator | Pump Analogy

To understand how Interconnection frequency is controlled, it may help to visualize a traditional water utility that is composed of a delivery system, customers, and several pumping stations as depicted in **Figure 1.5**. If a municipality operates its own system, it needs sufficient pumps (supply) to maintain the water level in the pumping stations' storage tanks (frequency) to serve its customers. When demand exceeds supply, the water levels in the pumping station tanks will drop prompting the pumps to respond. Water level (frequency) is the primary parameter that must be controlled in an independent system.

In the early history of the power system, utilities quickly learned the benefits ~~delivered ~~in reliability and realized reduced expense associated with maintaining operating reserves by connecting to neighboring systems. In our water utility example, an independent utility must have pumping stations in standby that are equivalent to its largest on-line pump if it wants to maintain the water level in case there is a problem with the largest pumping station. However, if utilities are connected together via tie-lines, reliability and economics are improved because of the larger resource capacity of the combined system and the ability to share capacity when needed.

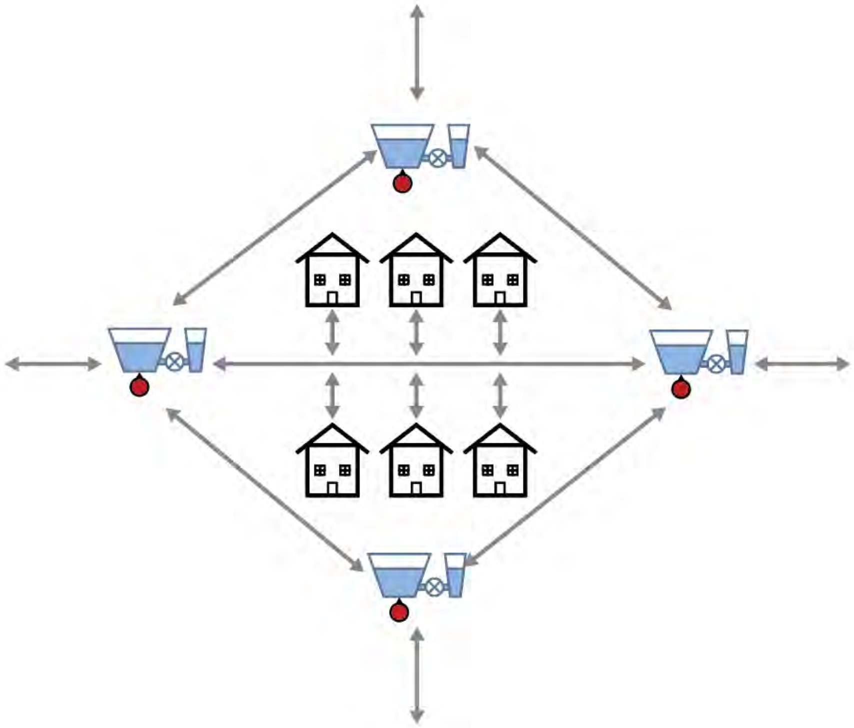


Figure 1:5: BA Analogy

Once the systems are interconnected, the steady state frequency (i.e. water level) is the same throughout. If one BA in the electric grid loses a generating resource, then there may be a drop in frequency. This drop in frequency~~but it~~ is less than in an independent system because the overall resource capacity of the interconnected system is much greater. The BA that needs~~ed~~ energy could purchase it from others provided that the interconnected system can reliably accommodate the additional flow. Purchasing and/or selling energy between BAs is known as Interchange.

There are two inputs to the BAs control process:[3]

- **Interchange Error:** the net outflow or inflow compared to the scheduled sales or purchases (The units of interchange error are in megawatts.)
- **Frequency Error:** the difference between actual and nominal frequency (The units of frequency error are hertz.)

Frequency bias is used to translate the frequency error into megawatts. Frequency bias is the BAs obligation to provide or absorb energy to assist in maintaining frequency. In other words, if frequency goes low, each BA is asked to contribute a small amount of extra generation in proportion to its system's relative size.

Each BAA uses ~~a~~ a common source~~meters~~ on the tie-lines with its neighbors for control and accounting. There will be an agreed upon meter at each BA boundary that both neighboring BAs use to perform balancing operations and accounting. Thus, all supply, load, and transmission lines in an Interconnection fall within the metered bounds of a BA.

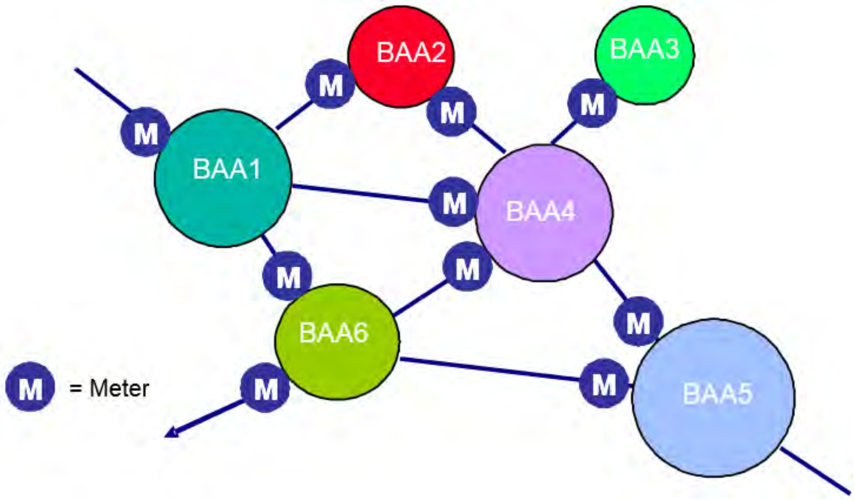


Figure 1:6: Interconnected BA Areas

If the BA is not buying or selling energy,[4] and its supply is exactly equal to the demand and losses within its metered boundary (BAA), the net of its tie line meters will be zero (assuming that the frequency of the system is at nominal). If the BA chooses to buy energy (e.g., 100 Megawatt hours (MWh)), it tells its control system to allow 100 MWh to flow in (by, for example, allowing 100 MW to flow in for one hour). Conversely, the seller will tell its control system to allow 100 MWh to flow out by allowing the corresponding 100 MW to flow out for one hour. If all BAs behave this

[3] There are two control inputs in multi-BA Interconnections. Texas and Quebec are single BA Interconnections and need only control to frequency.

[4] In most cases, BA's do not buy and sell energy. Transactions now are arranged by wholesale marketing agents that represent load or generation within the BA.

way, the Interconnection remains in balance and frequency remains stable. Variations in the supply/demand balance cause frequency to vary from its nominal value. Problems on the grid, such as congestion that prevents the ability to meet schedules, equipment faults that dictate rapid unilateral adjustments of generation, loss of load, incorrect schedules, or poor control cause changes in frequency. Maintaining Interconnection frequency near its nominal value can therefore be thought of as a fundamental indicator of the health of the power system.

Demand and supply are constantly changing within all BAAs. This means that a BA will usually have some unintentional outflow or inflow at any given instant. This mismatch in meeting a BA's internal obligations, along with the small additional "bias" obligation to maintain frequency, is represented via a real-time value called Area Control Error (ACE), with units of MW.

System operators at each BA fulfill their NERC obligations by monitoring ACE and keeping the value within limits that are generally proportional to BA size. This balancing is typically accomplished through a combination of adjustments of supply resources, purchases and sales of electricity with other BAs, and possibly adjustments of demand.

Conceptually, ACE is to a BA what frequency is to the Interconnection. Over-generation makes ACE go positive and puts upward pressure on Interconnection frequency. A large negative ACE can cause Interconnection frequency to drop. A highly variable or "noisy" ACE tends to contribute to similarly "noisy" frequency. However, the effect of ACE on frequency depends on how ACE is correlated (or anti-correlated) with frequency error. Over-frequency error tends to be made larger when ACE indicates over-generation, and is made smaller when ACE indicates under-generation. Under-frequency error has the opposite relationship. This principle is captured in the way Control Performance Standard 1 (CPS1) measures performance. Accumulation of frequency error over time results in the Interconnection's time error. For better overall Interconnection performance, the Western Interconnection (WI) uses automatic time error correction (ATEC) that allows BAs to make incremental corrections that are caused by under/over performing ACE.

Control Continuum

Figure 1.7 demonstrates that Balancing and frequency control occur over a continuum of time using different resources that have some overlap in timeframes of occurrence.

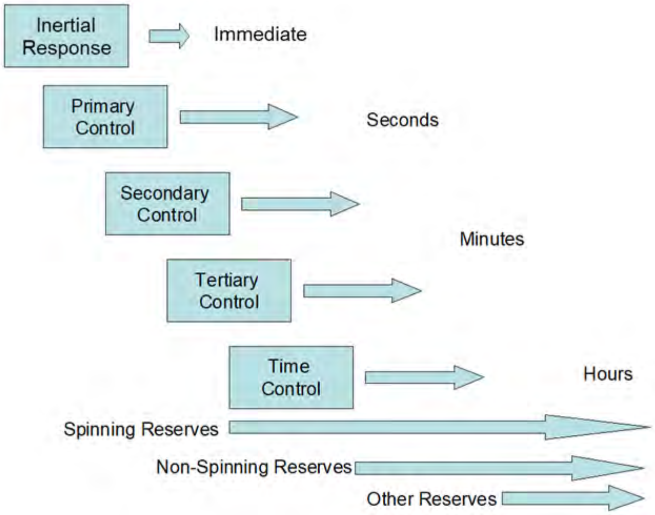


Figure 1.7: Control Continuum

A primary focus of the controls in the control continuum is to maintain nominal frequency under all conditions. One common operating condition is the loss of a (sometimes large) generator. This causes the frequency to drop which then requires the various pieces of the control continuum to recover the frequency to nominal. A stylized example is shown in figure 1.8. The frequency event is somewhat arbitrarily divided into 4 phases: the Arresting Period (when frequency decline is arrested), the Rebound Period (where frequency begins to recover towards nominal), the Stabilizing period (where frequency is stabilized), and the Recovery period (where frequency is recovered to nominal).

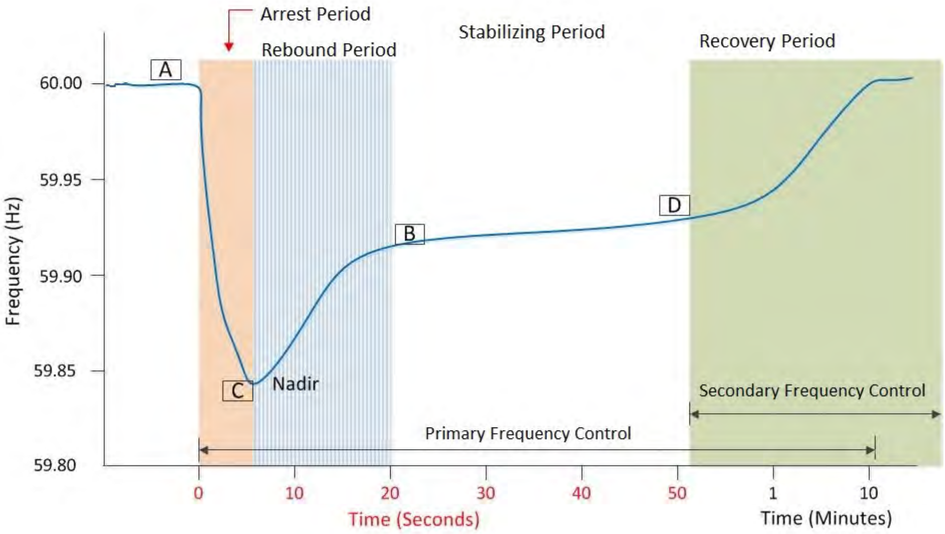


Figure 1.8: Typical Frequency Trend for the Loss of a Generating Resource

Four points of particular interest are shown in Figure 1.8: Point A is defined as the pre-disturbance frequency; Point C or Nadir is the maximum deviation due to loss of resource; Point B is defined as the stabilizing frequency and; Point D is the time the contingent BA begins the recovery from the loss of resource.

Inertial Control

Inertial control is more of an effect than an actual control since it is governed by physical principles for most resources and emulated by others. The rotating mass in a typical generator combined with the speed at which it is rotating creates a large amount of stored energy. If a decelerating force is applied (e.g., a large drop in system frequency), energy is transferred from the rotating mass and into the system. One analogy is that of a bicycle wheel and brake. If the wheel is first set spinning and then the brake is applied, the energy from the wheel flows into the braking surfaces. The contact surfaces of the brake will heat up due to the transformation of energy from the wheel into heat.

This is the same principle for the inertia effect in the power system. A sudden increase in the braking force is applied by a decrease in the amount of energy being injected into the system (e.g., losing a large generator or addition of a large load). When the mismatch between injected and consumed energy occurs, energy flows from the rotating masses of the connected resources into the power system. The propagation of this effect across an Interconnection happens within a handful of seconds.

Resources that are not directly coupled via an alternating current connection to the power system (e.g., inverter-based resources) are not typically governed by the same physical principles and therefore might not possess inertia per se from the perspective of the power system. Instead, inertia can be emulated to varying degrees of success by using sensing and control.

Primary Control

Primary control is more commonly known as primary frequency response (PFR). PFR also includes inertial response described under ~~i~~Inertial ~~c~~Control above as well as other types of frequency response actions, as described in the Primary Frequency Control Guideline.[5] PFR is autonomous; it does not require external inputs and begins to occur within the first few seconds following a change in system frequency (disturbance) to stabilize the Interconnection. Frequency response is provided by the following:

- **Governor Action:** Resource governors are like cruise controls for cars. They sense changes in local system frequency and adjust the energy output of the resource to counteract that change. Some resources do not have “governors” per se but instead can emulate governor action to varying degrees of success by using sensing and control actions.
- **Demand Response:** The speed of directly-connected motors in an Interconnection will change in direct proportion to frequency changes. As frequency drops, motors will turn slower and consume less energy.

  Rapid reduction of system load may also be affected by automatic operation of under-frequency relays which interrupt predefined loads within fractions of seconds or within seconds of frequency reaching a predetermined value. Such reduction of load may be contractually represented as interruptible load or may be provided in the form of resources procured as reliability or Ancillary services. As a safety net, percentages of firm load may be dropped by under-frequency load shedding programs to ensure stabilization of the systems under severe disturbance scenarios.

[5] PFC (v 2.0 approved by the Operating Committee 6/4/2019)

The most common type of a frequency disturbance in an Interconnection is associated with the loss of a generator, causing a decline in frequency; this happens on a daily basis and must be considered. In general, the amount of frequency-responsive, synchronized and unloaded generation ~~with~~ (a.k.a. headroom) in an Interconnection will directly influence the amount of available frequency response because this is the amount of supply that is connected, ready, and able to immediately increase output when needed. Inverter-based resources, especially those coupled with storage or headroom, may also be able to contribute to frequency response.

It is important to note that primary control will not return frequency to nominal, but only arrest and stabilize it. Other control components are used to restore frequency to nominal.

Operating Tip: Frequency response is particularly important during disturbances and islanding situations. System operators should be aware of their frequency responsive resources. Blackstart units must be able to autonomously participate in frequency control; this is especially important during system restoration.

Secondary Control

Secondary control typically includes the balancing services deployed in the “minutes” time frame. However, some resources (e.g., hydroelectric generation or fast electrical storage) can respond faster in many cases. Secondary control is accomplished using the BA’s supervisory control and data acquisition (SCADA) and energy management systems (EMSs)[6], and the manual actions taken by the dispatcher to provide additional adjustments. Secondary control also includes some initial reserve deployment for disturbances.

In short, secondary control maintains the minute-to-minute balance throughout the day and is used to keep ACE within CPS bounds and thereby maintain Interconnection frequency close to its scheduled value (usually 60 Hz) following a disturbance. Secondary control is provided by both Operating Reserve – Spinning and Supplemental. During frequency disturbances, secondary control returns the frequency to nominal once primary control has arrested and stabilized it.

The most common means of exercising secondary control is through an EMS’s AGC (Automatic Generation Control). AGC operates in conjunction with SCADA systems; SCADA gathers information about an electric power system, particularly system frequency, generator outputs, and actual interchange between the BA and its neighbors. Using system frequency and net actual interchange and knowledge of net scheduled interchange and upcoming changes, it is possible to determine the BA’s energy balance (i.e., its ACE) within its Interconnection. Most SCADA systems poll data points sequentially for electric system data, with a typical periodicity of two to six seconds. Because of this, data is naturally slightly out of perfect time sync, but is of sufficient quality to permit balancing and good frequency control.

AGC computes a BAA’s ACE from interchange and frequency data. ACE indicates whether a system is in balance or is in need of an adjustment to generation resources. AGC software generally sends signals that cause resources performing secondary control to move to oppose the ACE. Some AGC systems use pulses for raise/lower signals while other AGC systems use MW set points.

The degree of success of AGC in complying with balancing and frequency control is manifested in a BA’s control performance statistics that are described in greater detail later in this document.

Tertiary Control

Tertiary Control encompasses actions taken to get resources in place to handle current and future contingencies. Reserve deployment and reserve restoration following a disturbance are common types of Tertiary Control.

[6] Terms most often associated with this are “load-frequency control” or “automatic generation control”

Time Control

Frequency and balancing control are not perfect. There will always be occasional errors in tie-line meters whether due to instrument transducer inaccuracy, problems with SCADA hardware or software, or communications errors. Due to these errors and normal load and generation variation, ACE in an Interconnection cannot be maintained at zero. In fact, the average value of ACE over many time frames is non-zero. ACE must be managed such that its magnitude is relatively small. There is no operational reason to force ACE to be an independently randomly distributed variable. This means that frequency is never maintained at exactly 60 Hz for any appreciable length of time and average frequency over time usually is not exactly 60 Hz.

Each Interconnection has a time control process that can be used to maintain the long-term average frequency at 60 Hz. While there are some differences in process, each Interconnection designates a RC as a "time monitor" to provide Time Control.

The time monitor compares a clock driven off Interconnection frequency against the "official time"[7] provided by the National Institute of Standards and Technology. If average frequency drifts, it creates a Time Error between these two clocks. The ~~Quebec Interconnection (~~QI~~)~~ and ~~Texas Interconnection (~~TI~~)~~ operate so that Time Error is automatically minimized or eliminated while the WI operates to automatically mitigate accumulated Time Error through its ATEC. If the Time Error gets too large ~~I~~in the EI and WI, the Time Monitor may notify BAs in the Interconnection to manually correct the situation.

For example, if frequency has been running 2 mHz high (i.e., 60.002 Hz), a clock using Interconnection frequency as a reference will gain 1.2 seconds in a 10-hour interval:

$$\frac{(60.002\text{ Hz} - 60.000\text{ Hz})}{60\ Hz} * 10\ hr * 3600\frac{sec}{hr} = 1.2\ sec$$

If the Time Error accumulates to a predetermined initiation value (e.g., +10 sec in the Eastern Interconnection (EI)) the Time Monitor will send notices for all BAs in the Interconnection to offset their scheduled frequency by -0.02 Hz (Scheduled Frequency = 59.98 Hz). This offset, known as Time Error Correction, will be maintained until Time Error has decreased below the termination threshold (e.g., +6 sec).

A positive offset (i.e., Scheduled Frequency = 60.02 Hz) would be used if average frequency was low and Time Error reached its initiation value (e.g., -10 seconds). Manual time error corrections are no longer required by NERC Reliability ~~s~~Standards but each Interconnection may elect to perform manual time error correction. See the *NERC Time Monitoring Reference Document (Version ~~4~~5)* on manual time error correction for additional information.[8]

Control Continuum

Table 1.1 summarizes the discussion on the control continuum and identifies the service that provides the control and the NERC standard that addresses the adequacy of the service. Current issues, good practices, and recommendations on balancing and frequency control are discussed later.

Table 1.1: Control Continuum Summary

Control	Ancillary Service/ERS	Timeframe	NERC Measurement
Inertial Control	Inertial Control	0–12 Seconds	N/A

[7] The Official NIST US Time: https://www.time.gov/

[8] ~~NAESB WEQ Manual Time Error Correction Standards - WEQBPS – 004-000: https://www.naesb.org//pdf2/weq_bklet_011505_tec_mc.pdf~~ https://naesb.org/pdf4/weq_bps062520w1.pdf

Primary Control	Frequency Response	10–60 Seconds	FRM
Secondary Control	Regulation	1–10 Minutes	CPS1 – DCS - BAAL
Tertiary Control	Imbalance/Reserves	10 Minutes–Hours	BAAL - DCS
Time Control	Time Error Correction	Hours	N/A

Area Control Error (ACE) Review

The CPSs are based on measures that limit the magnitude and direction of the BAs Reporting ACE. The equation for Reporting ACE is as follows:

- Reporting ACE = $(NI_A – NI_S) – 10B (F_A – F_S) – I_{ME}$
- Reporting ACE (WI) = $(NI_A – NI_S) – 10B (F_A – F_S) – I_{ME} +I_{ATEC}$

where:

- NI_A is Actual Net Interchange,
- NI_S is Scheduled Net Interchange,
- B is BA Bias Setting
- F_A is Actual Frequency,
- F_S is Scheduled Frequency,
- I_{ME} is Interchange (tie line) Metering Error
- I_{ATEC} is ATEC (WI only)

NI_A is the algebraic sum of tie line flows between the BA and the Interconnection. NI_S is the net of all scheduled transactions with other BAs. In most areas, flow into a BA is defined as negative; flow out is positive.

The difference between net actual interchange and net scheduled interchange (N_{IA} - N_{IS}) represents the so-called "inadvertent" error associated with meeting schedules without consideration for frequency error or bias. If it is used by itself for control, it would be referred to as "flat tie line" control.

The term 10B (F_A - F_S) is the BAs obligation to support frequency. B is the BAs frequency bias stated in MW/0.1 Hz (B's sign is negative). The "10" converts the bias setting to MW/Hz. F_S is normally 60 Hz but may be offset ± 0.02 Hz for time error corrections. Control using "10B (F_A - F_S)" by itself is called "flat frequency" control.

I_{ME} is a correction factor for meter error. The meters that measure instantaneous[9] flow are not always as accurate as the hourly meters on tie lines. BAs are expected to check the error between the integrated instantaneous and the hourly meter readings. If there is a metering error, a value should be added to compensate for the estimated error; this value is I_{ME}. This term should normally be very small or zero.

I_{ATEC} is an ACE offsetting term for automatic timer error correction in the WI. BAs correct for any delta Time Error that they are responsible for each hour.

Reporting ACE is calculated in Real-time, at least as frequently as every six seconds, by the responsible entity's Energy Management System (EMS) predominantly based on source data automatically collected by that system. Also, the data must be updated at least every six seconds for continuous scan telemetry and updated as needed for report-by-exception telemetry. See the Integrating Reporting ACE Guideline for more detail on the components of ACE and the calculation frequency.

Here is a simple example: Assume a BA with a bias of -50 MW/0.1 Hz is purchasing 300 MW. The actual flow into the BA is 310 MW. Frequency is 60.01 Hz. Assume no time correction, metering error or ATEC.

[9] Instantaneous, as used herein, refers to measurements that are as close to real-time as is possible within the limits of data acquisition and conversion equipment.

- ACE = (-310 – -300) – 10*(-50) * (60.01 – 60.00) = (-10) – (-5) = -5 MW.

The BA should be generating 5 MW more to meet its obligation to the Interconnection. Even though it may appear counterintuitive to increase generation when frequency is high, the reason is that this BA is more energy-deficient at this moment (-10 MW) than its bias obligation to reduce frequency (-5 MW). The decision on when or if to correct the -5 MW ACE would be driven by CPS compliance.

A distinction can be drawn between reporting ACE, which measures the effect of a BA on the Interconnection, and Control ACE. At any given time, a BA might use a control ACE that is different from reporting ACE because AGC resources respond to control ACE, and this difference might be used, for example, to cause AGC resources to assist in "paying down" accumulated inadvertent energy or some other purpose.[10]

Bias (B) vs. Frequency Response (Beta)

There is often confusion in the industry when discussing frequency bias and frequency response. Even though there are similarities between the two terms, frequency bias (B) is not the same as frequency response (β).

Frequency response, defined in the NERC Glossary,[11] is the mathematical expression of the net change in a BA's net actual interchange for a change in Interconnection frequency. It is a fundamental reliability characteristic provided by a combination of governor action and demand response. Frequency response represents the actual MW contribution by inertial control and primary control to stabilize frequency following a disturbance.

Bias is an approximation of β used in the ACE equation. Bias (B) is designed to prevent AGC withdrawal of frequency support following a disturbance. If B and β were exactly equal, a BA would see no change in ACE following a frequency decline even though it provided a MW contribution to stabilize frequency.

Bias and frequency response are both expressed as negative numbers. In other words, as frequency drops, MW output (β) or desired output (B) increases. Both are measured in MW/0.1 Hz

Important Note: When people talk about frequency response and bias, they often discuss them as positive values (e.g., as "our bias is 50MW/0.1Hz"). Frequency response and bias are actually negative values.

Early research (Cohn) found that it is better to be over-biased (i.e., absolute value of B greater than the absolute value of β) than to be under-biased.

[10] Bilateral or Unilateral payback of inadvertent is not allowed in the WI. ATEC is used by BAs in the WI to control primary inadvertent accumulation while automatically correcting time error.

[11] Select from list found at: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

Chapter 2: Primary Control

Background

Primary control relates to the response to a frequency deviation by generator governors (aka. speed controls) and inertia that helps stabilize Interconnection frequency whenever there is a change in load-resource balance. Primary control is provided in the first few seconds following a frequency change and is maintained until it is replaced by AGC action (secondary control). Frequency response (or Beta), which also includes rotational inertia response from resources and load response from frequency dependent loads, is the more commonly used term for primary control. Beta (β) is defined by the total of all initial responses to a frequency excursion.

Figure 2.1 shows a trace of the WI's frequency that resulted from a generating unit trip. The graph plots frequency from 5 seconds prior to the loss of a large generator until 60 seconds thereafter.

NERC references three key events to describe such a disturbance. Value A is the pre-disturbance frequency, typically close to 60 Hz. Point C is the maximum excursion point, commonly referred to as the Nadir, which occurs about 10 seconds after the loss of generation in this WI example. Value B is the settling frequency of the Interconnection.

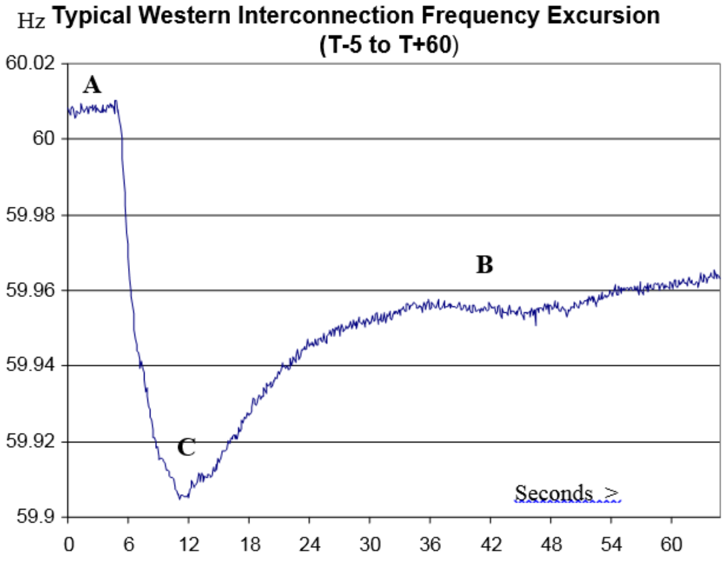


Figure 2.1: WI Frequency Excursion

As discussed earlier, there are two groups of "resources" that arrest a decline in frequency due to a loss of generation:

- A given portion of Interconnection demand is composed of motor load, which draws less energy when the motors slow down due to the lower frequency.
- Generators have governors that act much like cruise control on a car. If the generators on the Interconnection start to slow down with the frequency decline, their governors supply more energy to the generators' prime movers in order to speed them back up to nominal. The sensitivity of this response is controlled by the governor droop setting.

Inertial Response

Inertia quickly and autonomously opposes changes to both under and over frequency events. Having a large amount of inertia is useful for smoothing out power system frequency fluctuations. It is inertia combined with the response of frequency sensitive demand that determines how quickly the frequency decays following the loss of a large supply resource like a large generator or importing direct current tie-line. In an interconnection, more inertia leads to a slower drop in frequency, giving time for the other components of the control continuum to act in order to arrest, stabilize, and then recover frequency. In some sense, the inertia of the power system can be controlled by adjusting the amount and type of generators that are on-line. Inertia is commonly described in units of seconds: the energy that is stored is normalized by the electrical "size" of the resource. Since stored energy is a function of the square of the speed of rotation, low rotating mass, faster spinning resources might store more energy, yet they typically decelerate faster (thereby injecting more energy). These lighter and faster resources' contribution to slowing the fall of frequency is more "front-loaded" and they have smaller normalized inertia values than large-rotating-mass slow-spinning resources that have slower energy injection profiles. Faster response is also not always better because of interaction effects that can cause instability where resources might "bounce" in opposite directions.

For a discussion and graphical representation on how inertia opposes changes in under and over frequency excursions, see the *NERC Frequency Response Standard Background Document,* dated November 2012.[12]

Generator Governors (Speed Controls)

The most fundamental, front-line control of frequency in ac electric systems is the action of generator governors. Governors act to stabilize frequency following disturbances and act as an immediate buffer to load-resource imbalance. Governors operate in the time frame of milliseconds to seconds and operate independently from and much faster than system operator actions or those of AGC. They protect from the effects of frequency when too high, but the vast majority of their benefit comes from assisting when frequency has dropped too low, especially in cases where loss of generation causes abrupt decreases in Interconnection frequency.

Without governor action, loss of generation would result in frequency that would not stabilize until the load reduced to a point that matched the remaining generation output. As mentioned previously some load is reduced when the frequency is reduced mostly due to directly connected motors slowing down and consuming less power. This supply/demand balance point could occur at very low frequency and could result in cascading outages or complete frequency collapse, a very undesirable outcome in terms of the cost to society and potential equipment damage.

The combination of inertial response, governor response and load response – are the "beta" (β), or frequency response characteristic, of a BAA. This is the characteristic that AGC attempts to mimic in its use of the frequency bias ("B") parameter in determining ACE. The net of all BA frequency responses manifests as the Interconnection frequency response.

Droop

Governors cause generators to try and maintain a constant, stable system frequency (60 Hertz in North America). They do this by constantly governing (modulating) the amount of mechanical input energy to the shaft of the electric generator. The degree of this modulation is called "droop" and is measured in percent of frequency change to cause full generator capability to be exerted against the frequency error. A typical slope is 5%, meaning that the full output of the generator would be used (or attempt to be used) to counteract the frequency error if frequency error is 5% or 3 Hz. It should be noted that smaller droop percentages indicate increased sensitivity of response, e.g., a generator with a 4% droop would attempt to go to full output if the frequency changed by 2.4 Hz. Frequency errors are more typically in the range of 0.01% (.06 Hz, or 60 mHz), so governor action usually is a much smaller fraction of a unit's output capability. It must also be recognized that, while most generators can reduce output considerably in response

[12] https://www.nerc.com/comm/OC/RS%20Landing%20Page%20DL/Related%20Files/Bal-003-1_Background_Document_Clean_20121130.pdf

to their governor's actions, increasing output is more problematic since many generators may already be near the top of their output capability when low frequency causes their governor to request more output. Thus, if there is no "headroom" available on a generator's output, the governor will be able to do little to increase that output and help stabilize low frequency.

Deadband

The second general characteristic of governors is "deadband." This means that the governor ignores frequency error until it passes a threshold. When frequency error exceeds the threshold (which should not exceed the maximum deadband setting per Interconnection recommended in the NERC Reliability Guideline-Primary Frequency Control), the governor becomes active. It is worth noting that the deadband may be larger for older mechanical-style governors, and may have mechanical lash associated with it.

The calculated unit MW output change with a droop setting of 5% and deadband setting of 36 mHz based on the total resource capacity is shown in Figure 2.2

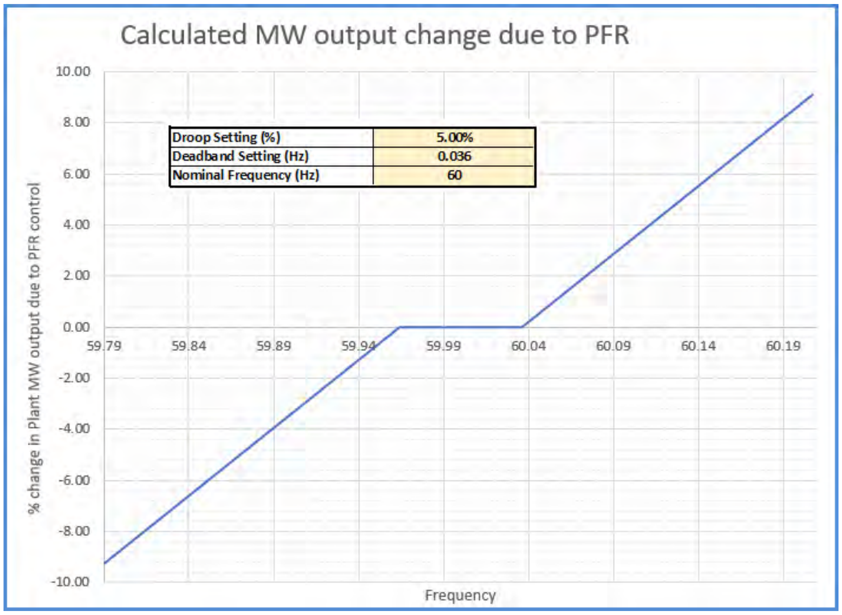


Figure 2.2: Calculated Resource %MW Output Change due to PFR

Calculating Frequency Response

Prior to current Reliability Standard requirements governing frequency response[13], calculation of frequency response was addressed by the NERC *Frequency Response Characteristic Survey Training Document*,[14] which included a form to guide the calculation for a given event. The calculation of the Frequency Response Characteristic (FRC) for a BA is to divide the change in Net Interchange Actual (NI_A) from pre-event (A point, see Figure 1.8 above) to the stabilizing period (B point, ~20-52 seconds after the event) by the change in interconnection frequency from pre-event to the stabilizing period. Although the terms in the FRC Training Document have changed over the years (e.g., Control Area is now Balancing Area), the calculation remains the same. This is often referred to as the A to B frequency response. With the advent of faster scanning tools over the years (e.g., Phasor Measurement Units), a similar response calculation can be made from the A point to the C point (nadir, if a generation loss or apex, if a load loss) of the frequency event.

Important Concept: The frequency response will normally be a negative value, reflecting the inverse relationship between the increase in MW output in response to the decrease in interconnection frequency for a frequency decline (e.g., a generator trip), or vice versa for a frequency increase (e.g., a load loss).

Under the current Reliability Standard requirements, the selection of events for evaluation and the calculation forms used to determine response are prescribed by the Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard[15], the Reliability Standard itself, its attachment and associated forms.

Frequency Response Profiles of the Interconnections

The amount of frequency decline from a generator trip varies based on a number of factors, e.g. time of day, season, and Interconnection loading. The observed frequency responses of the North American Interconnections as documented in the *2018 NERC State of Reliability* report are as follows:

- EI -2,103 MW / 0.1Hz
- TI -674 MW / 0.1 Hz
- WI -1,539 MW / 0.1 Hz
- QI -599 MW / 0.1 Hz

Important Note: These values are not normalized to adjust for starting frequency and/or resource loss size.

As noted above, the negative sign means there is an inverse relationship between generation loss and frequency. In other words, a loss of 1,000 MW would cause a frequency change (A to B) on the order of:

- EI -0.048 Hz
- TI -0.148 Hz
- WI -0.065 Hz
- QI -0.168 Hz

Conversely, if 1000 MW of load were lost in an Interconnection, the resulting frequency increase would be similar in magnitude as listed above.

[13] As of the release date of this document, the current applicable Reliability Standard is BAL-003-1.1

[14] https://www.nerc.com/comm/OC/RS%20Agendas%20Highlights%20and%20Minutes%20DL/Frequency_Response_Characteristic_Survey_19890101.pdf

[15] https://www.nerc.com/comm/OC/BAL0031_Supporting_Documents_2017_DL/Procedure_Clean_20121130.pdf

Figure 2.3 is a typical trace following the trip of a large generator in three of the Interconnections. Notice that governors in the East do not provide the “Point C to B” recovery of frequency as they do in the other Interconnections. The rate of frequency decline is much slower primarily due to its size, so frequency slowly drops until sufficient response stops the decline. In the early 2000s, there was typically a post-event decline in frequency, but this effect has been occurring less often.

Commented [BH5]: I replaced

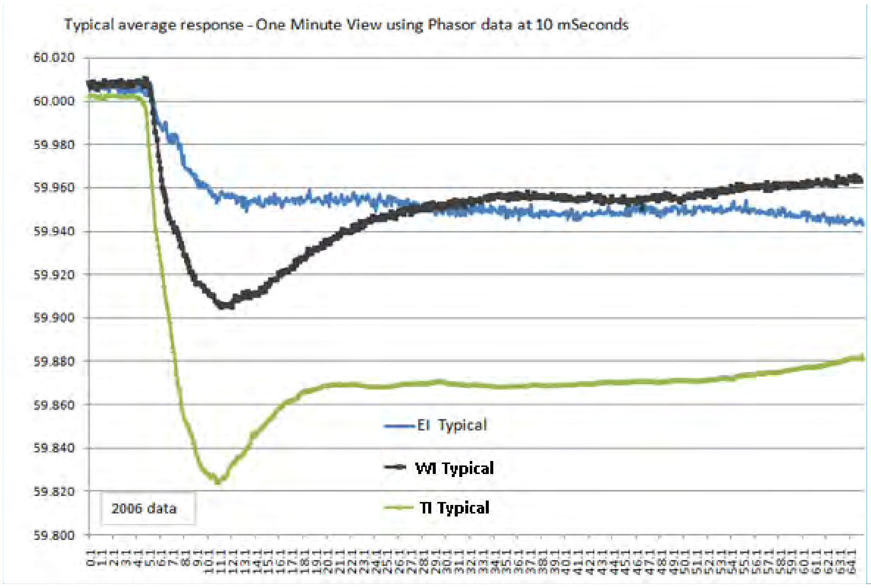
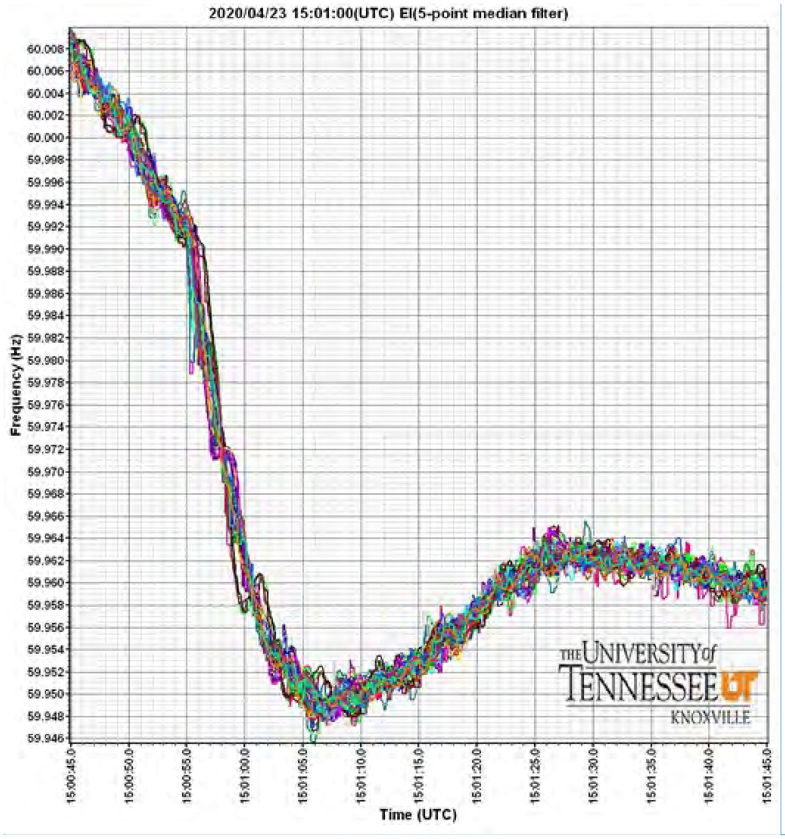


Figure 2.3: Typical Frequency Excursions

Important Concept: Following a large generator trip, frequency response will only stabilize the frequency of an Interconnection, arresting its decline. Frequency will not recover to scheduled frequency until the contingent BA replaces the lost generation through AGC and reserve deployment.

Figure 2.4 Shows the frequency at measured at various locations across the EI after a large generator trip. Note that the frequency disturbance is a chaotic event with complex dynamics, including fast transients bouncing about a much longer term trend. Also note that the time-scale tick-marks are every 5 seconds: the whole event has reached a stabilized frequency within 20 seconds.



Commented [BH6]: I replaced

Figure 2.4: Frequency Excursion Measured at various locations in the EI

Annual Bias Calculation

The value in a BA properly stating its bias is to ensure its AGC control system does not cause unnecessary over-control of its generation.

The NERC RS posts quarterly lists of excursions that are available to the industry for everyone's use for evaluating frequency response during the year. The subcommittee refines these quarterly lists into an official event list that is used in BAL-003 FRS forms.

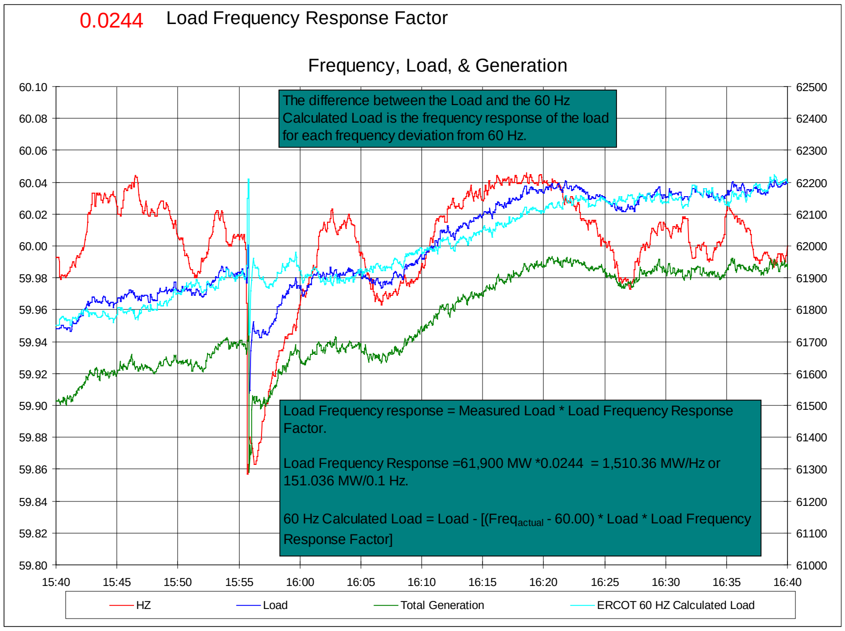
Guidelines the RS uses in selecting and evaluating events for calculating bias and BAL-003 performance include the following:

- Events are dispersed throughout the year to get a good representation of "average" response.
- Pick frequency excursions large enough to actuate generator governors.
- The events should be relatively clean and generally have continuous drop from A to C.

- Starting frequency should be relatively stable and close to 60 Hz.

Estimating Load's Frequency Response

As discussed previously, motor load provides frequency response to the Interconnection. The rule of thumb is that this response is equal to 1–2% of load. Techniques have been developed to observe approximately how much "load" frequency response a BA has available. This technique is explained in **Figure 2.5**.



0.0244 Load Frequency Response Factor

The difference between the Load and the 60 Hz Calculated Load is the frequency response of the load for each frequency deviation from 60 Hz.

Load Frequency response = Measured Load * Load Frequency Response Factor.

Load Frequency Response =61,900 MW *0.0244 = 1,510.36 MW/Hz or 151.036 MW/0.1 Hz.

60 Hz Calculated Load = Load - [(Freq$_{actual}$ - 60.00) * Load * Load Frequency Response Factor]

Figure 2.5: Observing Frequency Response of Load

The cyan trend in **Figure 2.5** above represents how much load would exist if frequency could be controlled to exactly 60.000 Hz all the time. The difference between the measured load, blue trend, and the cyan trend is the frequency response of load. For this event, a 759 MW resource was lost producing a frequency deviation of -0.118 Hz. This calculates to be

$$\frac{759\,MW}{0.118\,Hz * \left(\frac{10 * 0.1\,Hz}{Hz}\right)} = \frac{643\,MW}{0.1\,Hz}$$ of frequency response.

Of this response, 151.036 MW/0.1 Hz was provided by the load by multiplying the load by 0.00244, leaving the remainder (492.184 MW/0.1 Hz) provided by resource governor response. The post contingency total generation settled at 61,510 MW a difference of 178.222 MW below the pre-contingency generation. The generation-to-load mismatch post event is 178.222 MW plus replacement of the 580.777 MW of governor response (492.184 * 1.18 = 580.777) that will be withdrawn as frequency returns to 60.00 Hz. If this BA's bias in the ACE equation had been set exactly at 643 MW/0.1 Hz, ACE would equal -759 MW at the B point of this event. AGC would dispatch 759 MW to replace the frequency response of the governors and load, returning the Interconnection to balance at 60.00 Hz. This example is of a "single" BA Interconnection but the math works for multiple BA Interconnections as well.

By observing multiple events and adjusting the factor to produce a "60 Hz Load" value that maintains the pre- and post-event slope of load, a proper value can be determined. Larger deviation frequency events are beneficial to get a clear observation in addition to looking at many events. A factor between 0.010 and 0.025 would be reasonable depending on the ratio of motor load vs. non-motor load within the BAA boundaries.

The key points of primary control are as follows:

- Steady-state frequency is common throughout an Interconnection.
- If frequency is off schedule, generation is not in balance with total load.
- Arresting frequency deviations is the job of all BAs. This is achieved by provision of frequency response through the action of operating governors on generation and other resources able to provide frequency response (e.g., controllable load, storage, etc.).
- Frequency response is the sum of a BAs inertial response, natural load response and governor response of generators to frequency deviation within the BA Area.
- Frequency response arrests a frequency decline but does not bring it back to scheduled frequency. Returning to scheduled frequency occurs when the contingent BA restores its load-resource balance by using secondary control.
- Generators should be operated with their governors free to assist in stabilizing frequency.
- Frequency control during restoration is extremely important. That is why system operators should have knowledge of the generators' governor response capabilities during black start.
- All BAs have a frequency response characteristic based on the governor response of their units and the frequency-responsive nature of their load.
- The amount and rate of frequency deviation depends on the amount of imbalance in relation to the size of the Interconnection.
- Frequency bias is a negative number expressed in MW/0.1Hz.
- The ~~typical (best)~~preferred way to calculate frequency response is to observe the change in BA output for multiple events over a year.
- Under BAL-003-1.1 BA's should set its fixed bias to no less than the 100–125% of its natural frequency response or its percentage share of 0.9% of the Interconnection's non-coincidental peak load based upon all of the BAs within an Interconnection's non-coincident peak load values (whichever method is greater in absolute terms).
- BAs are allowed to employ variable frequency bias that more accurately reflects real-time operating condition.
- Governors were the first form of frequency control and remain in effect today; they act to oppose large changes in frequency.
- AGC supplements governor control by controlling actual tie flows and maintaining scheduled interchange at its desired value. It performs this function in the steady-state, seconds-to-minutes time frame after transient effects, including governor action, have taken place. If bias is greater than actual frequency response, AGC will supplement this response.
- ACE, the main input to AGC, requires frequency and energy interchange data (both actual and scheduled).
- While frequency response was declining in the 1990s, actions taken by the Industry appear to have stabilized the trend.
- BA or Interconnection frequency response should be measured for two reasons:
    - To gauge the area response to frequency deviations.

- As a basis for setting B.

Chapter 3: Secondary Control

Background

Secondary control is the combination of AGC and manual dispatch actions to maintain energy balance and scheduled frequency. In general, AGC utilizes maneuvering room while manual operator actions (e.g., ~~phone calls~~communication to generators, purchases and sales, load management actions) keep repositioning the BAA so that AGC can respond to the remainder of the load and interchange schedule changes. NERC CPSs are intended to be the indicator of sufficiency of secondary control.

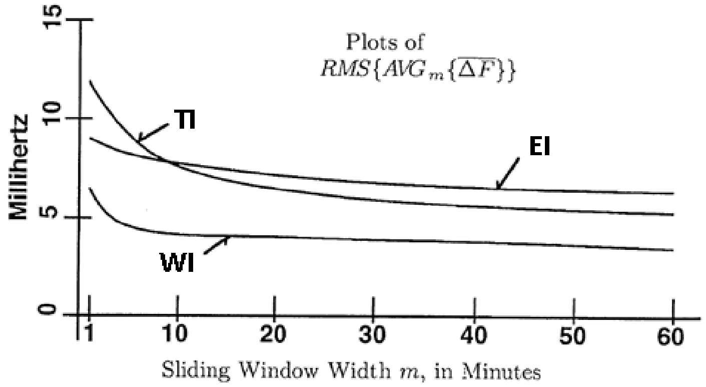
Maintaining an Acceptable Frequency Profile

One indicator of proper secondary control action is the distribution profile of steady-state Interconnection frequency. When the transition was made from the "A" criteria to CPS in 1997, the directive of the NERC Operating Committee was to not allow frequency variation to become any greater than it had been in the past. One measure of this is the root mean square (RMS) of frequency error from schedule. This by itself, however, is a measurement over an indefinite term and may not reveal problems at all averaging intervals. To adequately measure the frequency profile of an Interconnection, a statistical method was adopted in which period averages of RMS frequency error were measured and cataloged for periods of a large number of different values. In other words, the average of rolling N-minute RMS averages was computed for many values of N. This results in a defining profile as shown in **Figure 3.1** and **Figure 3.2.** Although other values could have been selected and ideally ALL values should be considered, the decision was made that the general profile would be maintained if the profile was anchored at two points in time (originally 1 minute and 10 minutes).

To set values for frequency performance, each Interconnection's frequency error was observed by using the above method, and each one was characterized, particularly at their 10-minute interval average RMS frequency deviation from schedule. The EI measured 5.7 mHz at the 10-minute point. The 1-minute point used to set the CPS standard was derived from an "ideal" error characteristic by the ratio of square roots. This yields 5.7 * √(10) = 18.025 mHz. This value was rounded to the value in use today for the East, 18 mHz.

The same technique was used for the WI and TI. It is important to realize that CPS1 performance is only measured at this one "slice" (one-minute averaging) of the Interconnection's frequency error characteristic. Because of this, there is no assurance that frequency variation will be constrained at other averaging points or converge on the ideal characteristic and become more random.

Initially, a 10-minute metric called CPS2 was developed to keep average ACE within specific bounds. CPS2 was originally used to help prevent excessive transmission flows due to large values of ACE. The problem with CPS2 was that it was not dependent on ACE's impact on frequency. Additionally, CPS2 could cause control actions that moved against frequency. If a BA had very bad performance in one direction for five minutes, the BA could correct this by having equally bad performance in the opposite direction for the next five minutes. Finally, ACE could be totally unbounded for 10% of the month and it didn't matter whether it was 1 or 1000 MW over the limit. CPS2 did not provide the correct signal for maintaining frequency. Ultimately, the industry adopted a frequency-sensitive longer term (i.e., 30 minute) measure called the BA ACE Limit (BAAL).

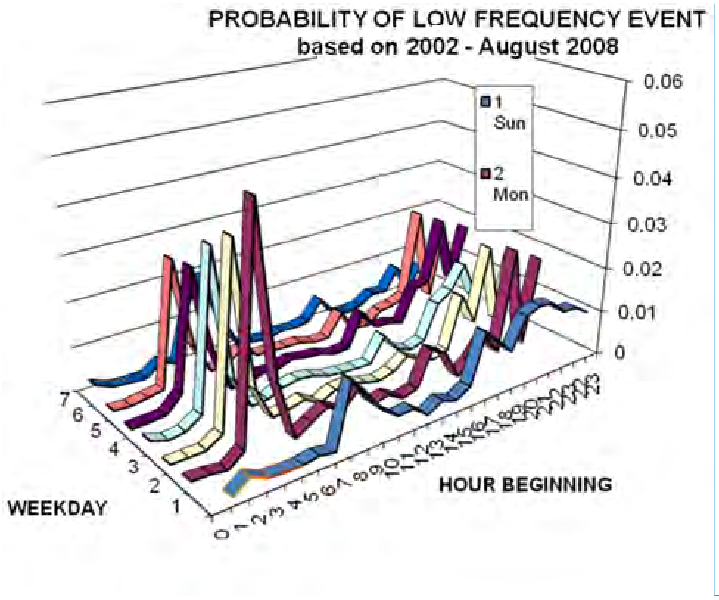


Frequency experience in the subject interconnections. Each ordinate point on these curves is the RMS value of the averages of $\overline{\Delta F}$ in windows of width m moved across the data string.

Figure 3.1: Interconnections with CPS actual-measured ΔF "period average"

Commented [BH7]: I replaced

Figure 3.1 Illustrates the actual-measured ΔF "period average" characteristic of the Interconnections with CPS was designed (EPRI report RP-3550, August, 1996). Note that these curves are flatter than what was ultimately selected as the epsilon limits in CPS1. The reason for this is that the standard needed to bound acceptable performance but not raise the bar and make it difficult to comply. For example, the 1-minute frequency variation in the East was about 10 mHz; if 10 mHz were chosen as Epsilon 1 in the East as opposed to the 18 mHz that was actually selected, it would mean that half the BAs in the East would have been out of compliance when the standard became active. Random (i.e., non-coincident) behavior of BAs in total is important in the above assumptions because the curves from which epsilon 1s were extrapolated start to deviate from the shape and predictability of the curves used to derive them as behavior becomes coincident (i.e., behaviors happening at the same time). Another way of saying this is that it becomes less and less valid to try to control frequency and measure performance at just one point on the sliding window continuum as coincidence creeps in. Prior to the adoption of the BAAL, the Interconnections would see wider frequency swings at specific times of day, particularly in the low direction. The swings, due primarily to load changes and large block Interchange Schedules, could occur under CPS2. The number and magnitude of frequency swings were reduced through a combination of tools that identified the contributing BAs as well as the adoption of BAAL.



Commented [BH8]: I replaced

Figure 3.2: Probability Distribution for Low-Frequency Events vs. Time of Day

Control Performance Standard 1

In simple terms, CPS1 assigns each BA a share of the responsibility for control of steady-state Interconnection frequency. The amount of responsibility is directly related to BA frequency bias.

As mentioned previously, ACE is to a BA what frequency is to the Interconnection. Over-generation makes ACE go positive and frequency increase while negative ACE "drags" on Interconnection and decreases frequency. "Noisy" ACE tends to cause "noisy" frequency. CPS1 captures these relationships using statistical measures to determine each BA's contribution to such "noise" relative to what is deemed permissible.

The CPS1 equation can be simplified as follows:

- CPS1 (in percent) = 100* [2 – (a Constant[16])* (frequency error)*(ACE)]

Frequency error is deviation from scheduled frequency, normally 60Hz. Scheduled frequency is different during a time correction, but for the purposes of this discussion, assume scheduled frequency is 60 Hz.

Refer to the equation above. Any minute where the average frequency is exactly on schedule or BA ACE is zero, the quantity ((frequency error)*(ACE)) is zero. Therefore, CPS1 = 100* (2-0), or 200%. This is true whenever frequency is on schedule or ACE is zero.

For any one-minute average where ACE and frequency error are "out of phase," CPS1 is greater than 200%. For example, if frequency is low, but ACE is positive (tending to correct frequency error), the BA gets extra CPS1 points.

[16] The size of this constant changes over time for BAs with variable bias, but the effect can be ignored when considering minute-to-minute operation. It is equal to -10 * B / ε_1^2

Operating Tip: Frequency is generally low when load is increasing and high when load is dropping. Anticipating and staying slightly “ahead of the load” and on the assistive side of frequency correction with your generation will give your BA high CPS1 scores over the long run.

Conversely, if ACE is aggravating the frequency error, CPS1 will be less than 200%. CPS1 can even go negative.

TI and QI Note: The TI and QI operate as single BA’s. ACE for a single BA Interconnection will always be “in phase” with frequency error; refer to the ACE review for verification. This means the largest CPS1 these BA’s can achieve is 200%. This occurs whenever ACE or frequency error is zero. CPS1 for these BA’s is a function of “frequency squared.”

The CONSTANT in the equation above is sized such that the BA will get a CPS1 of 100% if the BA’s ACE is proportionally as “noisy” as a benchmark frequency noise. The minimum acceptable rolling twelve-month score for CPS1 is 100%.

When CPS was established, each Interconnection was given a target or benchmark “frequency noise.” This target noise is called Epsilon 1(ε1). Epsilon 1 is nothing more than a statistician’s variable that means the RMS value of the one-minute averages of frequency.

The target values (in mHz of frequency noise) for each Interconnection are shown in **Table 3.1** below. The NERC RS monitors each Interconnection’s frequency performance and can adjust the ε1 values should an Interconnection’s frequency performance decline.

Table 3.1: Target Values of "One Minute Frequency Noise"

Interconnection	Epsilon 1 (ε1)
Eastern	18.0 mHz
Quebec	21.0 mHz
Western	22.8 mHz
Texas	30.0 mHz

The Epsilon 1 target initially set for each Interconnection was on the order of 1.6 times the historic frequency noise. This means a typical BAs performance would be around 160% for CPS1. If every BA in an Interconnection were performing with a CPS1 of 100%, it would result in an observed Interconnection frequency performance of ε1 (i.e.18mHz in the East).

Let’s review how CPS1 data can be applied to measure the adequacy of control performance and the deployment of resource-provided services to meet load. NERC previously referred to these resources as interconnected operating services (ERSs). More recently, the term essential reliability services is used. These align somewhat to what FERC calls “ancillary services.”

Figure 3.3 depicts ACE charts for one hour for four different BAs. Compare the charts for BAs 1 and 2. Both BAs show good performance for the hour. The difference between them is that the load in BA 2 is “noisier.”

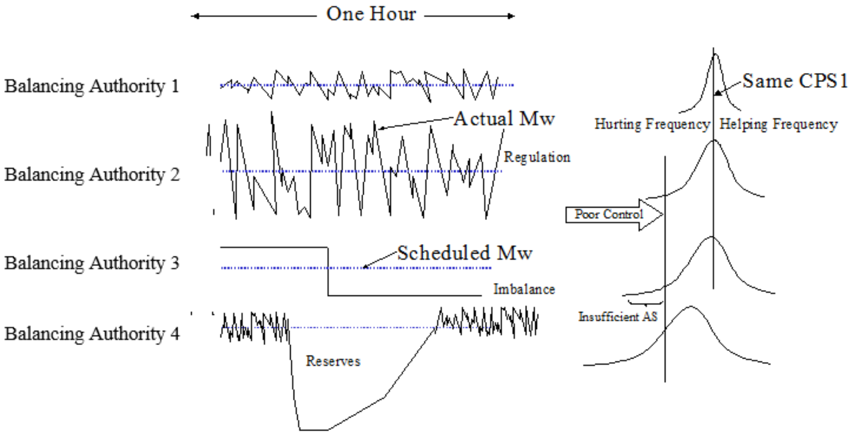


Figure 3.3: ERS / Ancillary Service Measured via CPS

The distributions to the right of the ACE charts show the individual one-minute CPS1 for both BAs for the hour. If frequency followed a normal pattern whereby it fluctuated +/- a few mHz from 60 Hz, the CPS1 curves for BA 1 and 2 would look like the distributions to the right of their ACE charts. Both curves would have the same average (about 160 percent CPS1), but BA 2's curve would be "wider."

Even though the average effect of BA 1 and 2 on the Interconnection is the same, BA 2 sometimes places a greater burden on the Interconnection as demonstrated by the size of the "left hand tail" of the CPS1 curve. A very long left tail implies poor control of some type (regulation in this case).

Now look at BA 3. It is a "generation only" BA that is selling 100 MW for the hour. The problem is that it is meeting this requirement by generating 200 MW for the first 30 minutes and 0 MW for the last half hour. Again, if frequency conditions are normal, half the time the BA will be helping frequency back towards 60 Hz and half the time the BA will be hurting frequency. This means the BA will get an "Interconnection average" CPS1 score of about 160% for the hour. The graph of its CPS1 for the hour will have wider tails, much like BA 2. The underlying problem in this case is imbalance, not regulation.

The ACE chart for BA 4 shows that a generator tripped offline during the hour. If the CPS1 one-minute averages are plotted, the curve will also have wider tails. If the unit that was lost was large, the curve will be "skewed" to the left even further. This is because the unit loss will pull frequency down while ACE is a large negative value.

In each case above, there was a deficiency in one of the energy-based ERSs. The "left tail" of the underlying CPS1 curve captured each situation.

Balancing Authority ACE Limit

In simple terms, BAAL assigns each BA a share of the responsibility for control of steady-state Interconnection frequency. The amount of responsibility is directly related to BA frequency bias and any deviation of Interconnection frequency from the Interconnections scheduled frequency.

The BAAL is calculated from the clock minutes averages of the data as follows:

Frequency Trigger Limits:

- FTL_{High} = Scheduled Frequency + 3*ε1
- FTL_{Low} = Scheduled Frequency - 3*ε1

As an example, for the EI (where epsilon1 = 0.018 mHz) and when the Interconnection is not in a time error correction (TEC) the FTL's are:

- FTL_{High} = 60.054 Hz
- FTL_{Low} = 59.946 Hz

Calculating the BAAL limits when actual frequency <> scheduled frequency:
As an example, for a BA with a frequency bias Setting = -1000MW/0.1Hz

- $BAAL_{Low}$ = (-10 * B * (FTL_{Low} - F_S)) * ((FTL_{Low} - F_S)/ (F_A-F_S))
- $BAAL_{Low =}$ (-10*-1000* (59.946 – 60)) * (59.946 – 60)/ (F_A – 60))

- $BAAL_{High}$ = (-10 * B * (FTL_{High} - F_S)) * ((FTL_{High} - F_S)/ (F_A-F_S))
- $BAAL_{High =}$ (-10*-1000* (60.054 – 60)) * (60.054 – 60)/ (F_A – 60))

Results with actual varying frequency are shown in **Table 3.2**.

Table 3.2: Varying Frequency Results

Actual Frequency	$BAAL_{High}$	$BAAL_{Low}$
60.09	324	NA
60.081	360	NA
60.072	405	NA
60.063	463	NA
60.054	540	NA
60.045	648	NA
60.036	810	NA
60.027	1080	NA
60.018	1620	NA
59.982	NA	-1080
59.973	NA	-720
59.964	NA	-540
59.955	NA	-432

Table 3.2: Varying Frequency Results

Actual Frequency	$BAAL_{High}$	$BAAL_{Low}$
59.946	NA	-360
59.937	NA	-309
59.928	NA	-270
59.919	NA	-240
59.91	NA	-216

The BAAL limits plotted in **Figure 3.4** detail the acceptable operating area and the BAAL limit exceedance area.

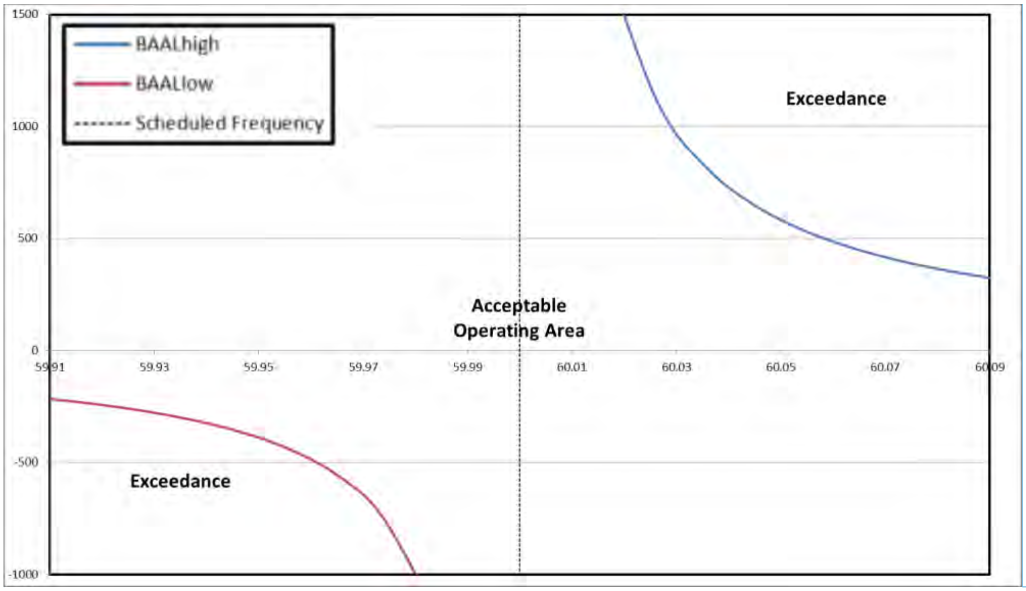


Figure 3.4: Acceptable Operating Area and the BAAL limit exceedance area

Commented [BH9]: I replaced

As a BA is operating and managing its ACE, the clock-minute averages of ACE are being evaluated against the BAAL limits.

CPS1 Equivalent Limit Derivation

BAAL is mathematically related to CPS1 as shown below:

- By definition; CF = (RACE/(-10B) *(F_A - F_S))/ (ε_1 ^{2}), and CPS1 = 2-CF
- Substituting for CF; CPS1 = 2-(RACE/(-10B) *(F_A - F_S))/ (ε_1 ^{2}))

- Regrouping terms; $CPS1 = 2 - RACE * ((F_A - F_S)/ (-10B* \varepsilon_1{}^2))$
- Substituting BAAL for RACE; $CPS1 = 2 - 9 * (-10B* \varepsilon_1{}^2) / (F_A - F_S) * ((F_A - F_S)/(-10B* \varepsilon_1{}^2))$
- Cancelling out terms; CPS1 = 2 – 9= -7 = -700%

Therefore, a one-minute CPS1 score more negative than -700% will equate to a BAAL exceedance for that one-minute period.

The minimum acceptable time frame for continuous BAAL minute exceedances shall not continue for greater than thirty minutes.

Quick Review

- CPS1 assigns each BA a share of the responsibility for control of Interconnection frequency.
- CPS1 is a yearly (i.e., rolling twelve month) standard that measures impact on frequency error with a 100% minimum allowable score.
- BAAL is a 30-minute standard intended to bind a BAs real-time impact on frequency.

Chapter 4: Tertiary Control

Tertiary Control generally follows disturbances and reserve deployment to reestablish resources for future contingencies. Reserve deployment and reserve restoration following a disturbance are common types of Tertiary Control. See the Operating Reserve Management Reliability Guideline for more information.

Understanding Reserves

There is often confusion when operators and planners talk about reserves. One major reason for misunderstanding is a lack of common definitions; NERC's definitions have changed over time. In addition, most NERC Regions developed their own definitions. Capacity obligations have historically been the purview of state and provincial regulatory bodies, meaning that there are many different expectations and obligations across North America.

In order to foster discussion and develop a more uniform understanding of the reserve data, the following definitions are provided in this reference. Refer to **Figure 4.1** to better understand the definitions.

Definitions:

(Capitalized terms are taken from NERC Glossary and lower case are not.)

Contingency Reserve: The provision of capacity deployed by the BA to ~~meet~~ respond to a Balancing Contingency Event and other contingency requirements (such as Energy Emergency Alerts as specified in the associated NERC Standards). This is the left column of Operating Reserves in Figure 4.1

frequency-responsive reserve: On-line generation with headroom that has been tested and verified to be capable of providing droop as described in the Primary Frequency Response guideline. Variable load that mirrors governor droop and dead-band may also be considered frequency responsive reserve.

Interruptible Load: Demand that the end-use customer makes available to its Load-Serving Entity via contract or agreement for curtailment that can be interrupted within 10 minutes.

Operating Reserve: That capability above firm system demand required to provide for regulation, load forecasting error, equipment forced and scheduled outages, and local area protection.

Operating Reserve–Spinning: Generation synchronized to the system and fully available to serve load within the Disturbance Recovery Period following the contingency event or Load fully removable from the system within the Disturbance Recovery Period following the contingency event deployable in 10 minutes.

Operating Reserve Supplemental: Generation (synchronized or capable of being synchronized to the system) that is fully available to serve load within the Disturbance Recovery Period following the contingency event or Load fully removable from the system within the Disturbance Recovery Period following the contingency event that can be removed from the system, within 10 minutes.

planning reserve: The difference between a BA's expected annual peak capability and its expected annual peak demand expressed as a percentage of the annual peak demand. See BAL-502-RF-03 for additional discussion.

Regulating Reserve: An amount of Operating Reserve – Spinning responsive to Automatic Generation Control, which is sufficient to provide normal regulating margin.

replacement reserve: NOTE: Each NERC Region sets times for reserve restoration, typically in the 60–90-minute range. The NERC default contingency reserve restoration period is 90 minutes after the disturbance recovery period.

Supplemental Reserve Service: Provides additional capacity from electricity generators that can be used to respond to a contingency within a short period, usually ten minutes. An ancillary service identified in FERC Order 888 as necessary to affect a transfer of electricity between purchasing and selling entities. This is effectively FERC's equivalent to NERC's Operating Reserve.

Much like parts kept in a storeroom, reserves are meant to be used when the need arises. Reserves can be low for short periods of time due to plant equipment problems and unit trips and can also be misstated

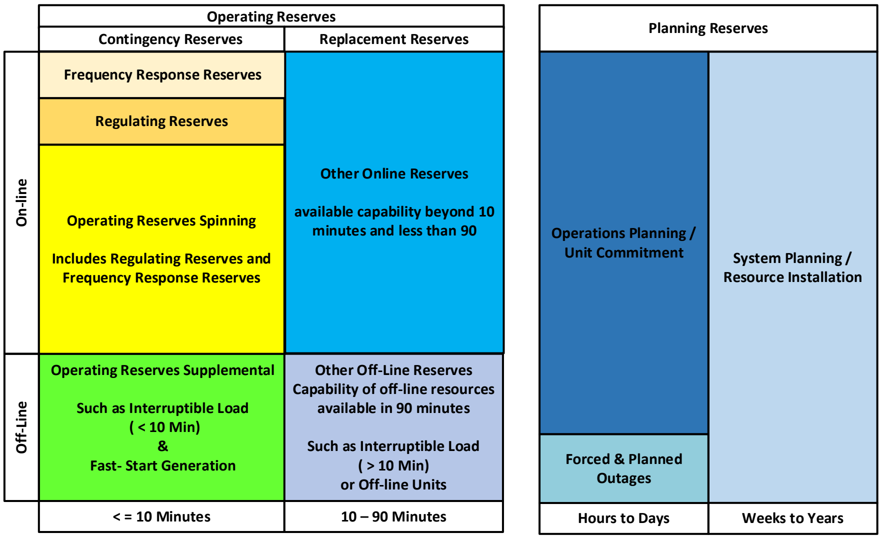

Operating Reserves
Contingency Reserves
Replacement Reserves
Planning Reserves
On-line
Off-Line
Frequency Response Reserves
Regulating Reserves
Operating Reserves Spinning
Includes Regulating Reserves and Frequency Response Reserves
Other Online Reserves
available capability beyond 10 minutes and less than 90
Operating Reserves Supplemental
Such as Interruptible Load
(< 10 Min)
&
Fast- Start Generation
Other Off-Line Reserves
Capability of off-line resources available in 90 minutes
Such as Interruptible Load
(> 10 Min)
or Off-line Units
Operations Planning / Unit Commitment
Forced & Planned Outages
System Planning / Resource Installation
< = 10 Minutes
10 – 90 Minutes
Hours to Days
Weeks to Years

Figure 4.1: Reserves Continuum

Chapter 5: Time Control and Inadvertent Interchange

Background

There is a strong interrelationship between control of time error and Inadvertent Interchange (aka. “inadvertent”). Time error occurs when one or more BAs has imprecise control or large resource losses occur, causing average actual frequency to deviate from scheduled frequency. The bias term in the ACE equation of the remaining BAs causes control actions that result in flows between BAAs in the opposite direction. The net accumulation of all these interchange errors is referred to as Inadvertent Interchange. Inadvertent interchange represents the amount by which actual flows between BAAs and the remainder of the Interconnection differs from the intended or scheduled flows.

Time Control

As noted earlier, frequency control and balancing control are not perfect. There will always be some errors in tie-line meters. Due to load and generation variation, net ACE in an Interconnection cannot be maintained at zero. This means that frequency will vary from 60 Hz over time.

An Interconnection may have a time control process to maintain the long-term average frequency at 60 Hz. While there are some differences in process, each Interconnection that exercises time control designates an RC as a “time monitor” to coordinate time control.

Time error corrections are initiated when long-term average frequency drifts from 60 Hz. In the EI, a 0.02Hz offset to scheduled frequency corrects 1.2 seconds on the clock for each hour of the time error correction, provided the offset scheduled frequency is achieved.

There has been an ongoing debate on the need for time error corrections. The number~~s~~ of time error corrections do provide a benchmark for the quality of frequency control and provide an early warning of chronic balancing problems. While the value of time control is debatable from a reliability perspective, nobody can say with assurance who or what would be impacted if NERC and NAESB halted the practice of manual time error corrections. This practice was removed from the NERC standards in 2017, but still remains in the NAESB standards.

Inadvertent Interchange

Inadvertent interchange is net imbalance of energy between a BA and the Interconnection. The formula for inadvertent interchange is:

- $NI_I = NI_A - NI_S$

where,

NI_A is net actual interchange. It is the algebraic sum of the hourly integrated energy on a BAs tie lines. Net actual interchange is positive for power leaving the system and negative for power entering.

NI_S is net scheduled interchange. It is defined as the mutually prearranged net energy to be delivered or received on a BAs tie lines. Net scheduled interchange is positive for power scheduled to be delivered from the system and negative for power scheduled to be received into the system.

Inadvertent interchange and can be divided into two categories, described below.

Primary Inadvertent

Primary inadvertent interchange is caused by problems or action from within a given BA. Primary inadvertent interchange occurs due to the following:

- Error in scheduled interchange
  - Improper entry of data (time, amount, direction, duration, etc.…)
  - Improper update in real-time (TLR miscommunication etc.…)
  - Ramp procedures
  - Miscellaneous (phantom schedules, selling off the ties, etc.…)
- Error in actual interchange (meter error)
  - Loss of telemetry
  - Differences between real-time power (MW, for ACE), and energy (MWh), integrated values
- Control error or offset
  - Load volatility and unpredictability
  - Generation outages
  - Generation uninstructed deviations
  - Physical rate-of-change-of-production limitations
  - Deliberate control offset (i.e. unilateral payback) to reduce inadvertent energy balances

Hourly primary inadvertent can be calculated for each BA by using the following formula:

$(PII_{hourly}) = (1-Y) * (II_{actual} - Bi * \Delta TE/6)$

- PII_{hourly} is the BAs primary inadvertent for an operating hour expressed in MWh
- Y is the ratio between a BAs frequency bias setting and the sum of all BAs frequency bias setting within an Interconnection
- Bi is the BAs frequency bias
- ΔTE is the change in time error within the Interconnection that occurred during the operating hour

Secondary Inadvertent

Balancing problems external to a BA will cause off-schedule frequency. If frequency is low, the bias term of the ACE equation will cause a BA to slightly over-generate after initial effects to stabilize frequency, such as governor response and load damping~~, stabilize frequency~~. Conversely, if frequency is high, the bias term of the ACE equation will cause slight under generation. This intentional outflow or inflow to stabilize frequency due to problems outside the BA causes deviation from the schedule and is called secondary inadvertent interchange.

Hourly secondary inadvertent can be derived by subtracting a BA’s hourly primary inadvertent from their hourly total inadvertent.

Quick Review: If one or more BAs have a control problem, it could result in a large primary inadvertent interchange. This may also cause off-nominal frequency, potentially spreading Secondary inadvertent interchange to the other BAs. The off-normal frequency then results in accumulated time error, potentially triggering time error corrections.

Chapter 6: Frequency Correction and Intervention

Background

There are several requirements in NERC reliability standards that tell the BA, Transmission Operator, and RC to monitor and control frequency. The standards do not provide specific guidance on what is normal frequency and under what conditions the operator should intervene. ~~The trigger points below are designed for the EI. There may be differences in the other Interconnections based on their field trial experience.~~

As noted earlier in this document, this information is provided for guidance and understanding. It should not be used for compliance purposes and does not establish new requirements or obligations.

The BAAL is the ACE-frequency combination equivalent to instantaneous CPS1 of -700%. In general, if one or more of the RC's BAs is beyond the BAAL for more than 15 minutes, the RC should contact the BA to determine the underlying cause. As frequency diverges more from 60 Hz, the RC and BA should be more aggressive in their actions.

One of ~~T~~the primary responsibilities~~y~~ of the RCs is frequency protection. Suggested actions are outlined below.

1. Identify BAs within your area beyond BAAL. Direct correction and log. RCs to notify BAs.
2. Call Other RCs, communicate problem if known. Search for cause if none reported. Notify time monitor of findings. Time monitor to log. Direct BAs beyond BAAL to correct ACE.
3. Direct all BAs with ACE hurting frequency to correct. Time monitor to notify Resource Subcommittee after the fact.
4. Evaluate whether still interconnected. Direct emergency action.

Revision History

Date	Version Number	Reason/Comments
4-5-2011	1.0	Initial Version
~~9-29-2020~~5-11-2021	2.0	Resources Subcommittee Review

Appendix A: References

Cohn, N. (May 1982). Decomposition of Time Deviation and Inadvertent Interchange on Interconnected System, Parts I & II. *IEEE PAS, Vol. PAS-101, No. 5*.

Cohn, N. (1956). Some Aspects of Tie-Line Bias Control on Interconnected Power Systems, *AIEE Transactions, vol. 75, pt. III (Power Apparatus and Systems)*, 1415-1436.

Cohn, N. (1984). Recollections of the Evolution of Real-time Control Applications to Power Systems, *Automatica, vol. 20, no. 2*, 145-162.

Electric Power Research Institute (1992). *Impacts of Governor Response Changes on the Security of North American Interconnections*.

Electric Power Research Institute (1996). *Control Performance Standards and Procedures for Interconnected Operations, EPRI RP3555-10*.

Ingleson, J., & Nagle, M. (May, 1999). *Decline of Eastern Interconnection Frequency Response.* Prepared for the Fault and Disturbance Conference at Georgia Tech. Retrieved May 19, 2004 from http://truc.org/files/1999/fda1999_jwi_final.pdf.

Ingleson, J., & Ellis, D. (2005). *Tracking the Eastern Interconnection Frequency Governing Characteristic*. Summer, 2005 IEEE/PES.

Jaleeli, N. & VanSlyck, L.S. (August 1999). NERC's New Control Performance Standards. IEEE T-PWRS Vol. 14, No. 3, pp 1092-1099.

Jaleeli, N., VanSlyck, L. S., Ewart, D. N., Fink, L. H. and Hoffmann, A. G. (August 1992). Understanding Automatic Generation Control. IEEE T-PWRS Vol. 7, No. 3, pp 1106-1122.

Kirby, B., Dyer, J., Martinez, C., Shoureshi, R., Guttromson, R., & Dagle, J. (December 2002). *Frequency Control Concerns In The North American Electric Power System, ORNL/TM-2003/41*. Oak Ridge, TN: Oak Ridge National Laboratory.
Lindahl, S.(2002). *Verification of Governor Response during Normal Operation*. Retrieved November 5, 2003 from http://www.eeh.ee.ethz.ch/downloads/psl/research/psdpc/.

Moran, F. & Williams, D.R. (April 1968). Automatic control of power-system frequency by machine controllers, *Proceeding of the IEE, vol. 115, no. 4*, 606-614.

Moran, F., Bain, D.K.S., & Sohal, J.S. (July 1968). Development of the equipment required for the loading of turbogenerators under automatic power-system control, *Proceedings of the IEE, vol. 115, no 7*, 1067-1075.

NAESB WEQ Manual Time Error Correction Standards - WEQBPS – 004-000

NERC (2002, August 28). *Frequency Excursion Task Force Report*. North American Electric Reliability Council.

NERC (2006). *Frequency Response Characteristic Survey Training Document.* North American Electric Reliability Council.

NERC Frequency Response Standard White Paper, April 6, 2004

NERC (2004). *Inadvertent Interchange Accounting Training Document*.

NERC (2004). Performance *Standard Training Document*. North American Electric Reliability Council.

NERC (2004). *Area Interchange Error Survey Training Document*. North American Electric Reliability Council.

NERC. *Area Interchange Error Reports*. Available at www.nerc.com/~filez/aie.html.

NERC Joint Inadvertent Interchange Task Force (2001). *Draft Guiding Principles for an Inadvertent Interchange Standards*. North American Electric Reliability Council.

NERC (2005). *Reliability Standards for the Bulk Electric Systems of North America*. North American Electric Reliability Council.

UCTE. *Policy 1 — Load-Frequency Control and Performance*. Draft Operating Standard for Europe. Retrieved November 5, 2003 from http://europa.eu.int/comm/energy/.

VanSlyck, L.S., Jaleeli, N. & Kelley, W.R. (May, 1989). Implications of Frequency Control Bias Settings on Interconnected System Operation and Inadvertent Energy Accounting. *IEEE Transactions on Power Systems, vol. 4, no. 2*, 712-723.

U.S.-Canada Power System Outage Task Force (2004, April 5*). Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*.

Organization(s)	Page #	Line / Paragraph	Comment	Proposed Change	NERC RS Response
PJM	Page 32		There has been an ongoing debate on the need for time error corrections. The numbers of time error corrections do provide a benchmark for the quality of frequency control and provide an early warning of chronic balancing problems. While the value of time control is debatable from a reliability perspective, nobody can say with assurance who or what would be impacted if NERC and NAESB halted the practice of manual time error corrections. This practice was removed from the standards in 2017.	The TEC was removed from the NERC Standards, but TEC is still in the NAESB Standards. Requesting this clarification to either follow this sentence or change the sentence to reflect the change: "This practice was removed from the standards in 2017"	revised
City of Tallahassee (TAL)	30	Contingency Reserves	First sentence grammatically incorrect	"...deployed by the BA to ~~meet~~ respond to a Balancing..."	revised
Reliability First	1	First bullet items	This document later refers to the defined interconnections separately and references an acronym. It may be helpful to include the applicable acronyms here instead.	For example, 'Western' could be changed to 'Western Interconnection (WI)'.	revised, and corrected where defined elsewhere
Reliability First	1	First paragraph under Figure 1.1	Replace "near synchronism" with "synchronously"	This occurs as the electric generating units rotate (in steady-state) synchronously.	revised
Reliability First	3	Figure 1.3	With Load written above Losses, it first appears that Load is grey and Losses are blue. This is not the intent. Can the image be changed so it does not like a stacked graph image?	This could be remedied by having Load & Losses in the same line on the graph image.	revised to provide clarity on the container or capacity size
Reliability First	3	Figure 1.4	The red circle with a P represents the pump. Just to ensure this is clear, it may be helpful to label the pump without a symbol/acronym.	Label the pump as "Pump"	revised
Reliability First	3	Last paragraph	Suggested wording change.	Remove the word "delivered" in the sentence	revised
Reliability First	4	Paragraph after Figure 1:5	Suggested wording change for the sentence that starts with "If one BA"	If one BA in the electric grid loses a generating resource, then there may be a drop in frequency. This drop in frequency is less then in an independent system, because the overall resource capacity of the interconnected system in much greater.	revised
Reliability First	4	Last sentence in paragraph after Figure 1:5	The BA that needs energy can purchase it from others, provide that the interconnected system can reliably accommodate the additional flow		revised
Reliability First	5	Second paragraph	The first sentence references "common meters", but these meters are actually required to have a reduced error/increased accuracy when compared to meters typically used on the electric grid.	Recommend to remove the word "common"	revised to reflect common sources as required by BAL-005 for meters and allocated values
Reliability First	5	First paragraph under Figure 1.6	Suggested wording change. Change "such as congestion" to "an inability to meet scheduled interchanges", since congestion alone may not have an direct impact to frequency.	Problems on the grid, such as an inability to meet scheduled interchanges, ….	revised
Reliability First	8	First paragraph	Suggested wording change. Reference the inertial response section differently and add the word "as" after "well"	PFR also includes inertial response described under the previous inertial control section as well as……	revised
Reliability First	8	First paragraph after bullets	Suggested wording change. The loss of a generator may not happen on a daily basis, so it is recommended to replace "on a daily basis" with "frequently"	The most common type of a frequency disturbance in an Interconnection is associated with the loss of a generator, causing a decline in frequency; this happens frequently and must be considered…..	leave as is. Frequently does not describe how often.
Reliability First	8	First paragraph after bullets	Suggested wording change. It is recommended to remove the word "frequency-responsive" or put synchronized in parenthesis.	In general, the amount of frequency-responsive (synchronized) and…..	revised and added IBR clarification
Reliability First	10	Second paragraph	Suggested wording change. Change "standards" to "NERC Reliability Standards"	….no longer required by NERC Reliability Standards but….	revised
Reliability First	17	Figure 2.3	In Figure 2.3, WECC and ERCOT labels are not consistent with verbiage used in document, suggest changing to WI and TI, respectively. Figure 2.3 displays results for WI, EI, and TI, but does not show QI.	In Figure 2.3, change WECC to WI, EROT to TI, and add QI.	revised

Reliability First	18	Figure 2.4	Can a graph without the missing data point just before 13:36.05 be used? Or explain it?		revised
Reliability First	19	Last paragraph	Suggested number format change. Add a zero to ".00244"	0.00244	revised
Reliability First	20	11th bullet	Suggested wording change. Remove "The typical (best) way" with "A preferred method"	A preferred method to calculate…..	revised
Reliability First	21	First bullet	It seems like these should be more context added here regarding the actions taken by industry to stabilize the trend. This may be better served as talking points in a conclusion paragraph.		leave as is, PFR analysis is addressed in the SOR
Reliability First	22	First paragraph	Suggested wording change. Replace "phone calls" with "communications"	….while manual operator actions (e.g., communications to generators,…..	revised
Reliability First	23	Figure 3.1	In Figure 3.1, WSCC, East, and ERCOT labels are not consistent with verbiage used in document, suggest changing to WI, EI, and TI, respectively. Figure 3.1 displays results for WI, EI, and TI, but does not show QI.	In Figure 3.1, change WSCC to WI, East to EI, ERCOT to TI, and add QI.	revised
Reliability First	24	Figure 3.2	Figure 3.2 title overlaps with graph, which make it difficult to read.	Add background to figure title or relocate above figure	revised
Reliability First	28	Figure 3.4	Legend associated with Figure 3.4 is difficult to read. Consider making the Legend larger.		revised
Reliability First	30	Contingency Reserve definition	Suggested wording change. Change "meet respond" to "meet response"	….by the BA to meet response to a…..	revised
Reliability First	31	Planning reserve definition	ReliabilityFirst has a regional specific Reliability Standard, BAL-502-RF-03, that pertains to guidance around performance of a planning resource adequacy analysis. It may be helpful to use this as a reference for considerations when performing this type of planning assessment.		added reference
Reliability First	31	Figure 4.1	This table is very helpful with providing additional context regarding the terms identified in the Definitions section of the document. It would be helpful to add some verbiage associated with the figure to explain the purpose and the differences between terms.	As a high-level example……The various terms associated with this guideline document represent distinct conditions pertaining to reserve management and assessment. Figure 4.1 clearly shows the differing types of reserves between the operating and planning environment and potential availability based on time or generating unit operational status.	leave as is, this matches and refers to the Operating Reserves Management Guideline
Reliability First	32	Last paragraph before Inadvertent Interchange	Suggested wording change. Change "numbers" to "number"	The number of time error corrections…..	revised
Reliability First	32	Last paragraph before Inadvertent Interchange	Add context or description to verbiage for the statement, "This practice was removed from the standards in 2017."	Need to specify NERC standards. This may still be a NAESB standard.	revised
Reliability First	33	Paragraph after Secondary Inadvertent	Suggested wording change.	If frequency is low, the bias term of the ACE equation will cause a BA to slightly over-generate after initial effects to stabilize frequency, such as governor response and load damping.	revised
Reliability First	34	Chapter 6	Why are there only EI trigger points discussed here? Can trigger points be added to other Interconnections?		removed reference to trigger points
Reliability First	34	Chapter 6	Suggested wording change in regard to the statement "The primary responsibility of the RCs"	An important responsibility of the RCs is frequency protection.	revised
Bonneville Power Administration	10	line 3-4 of para 2	The incorrect version of the NERC Time Monitoring Reference Document (version 4) is referenced.	Version 5 is the most recent, noting the WECC Interconnection time monitor as California ISO – RC West. Version 4 still refers to Peak Reliability.	revised
Bonneville Power Administration	10	Footer 8	The document link in the footer is incorrect.	The reference should be linked to the NERC Time Monitoring Reference Document (Version 5), not the NAESB WEQ Manual Time Error Correction BPS.	the updated NAESB link points to the NERC doc
Bonneville Power Administration	11	Bullet 9	The description of the term 'IATEC' as 'ATEC is WI only' is being discussed in a SAR for the ACE equation to remove the 'WI only' reference to ATEC. This would allow other interconnections to adopt an ATEC program.	If that SAR introduces changes, this reference document will also require updating.	noted

Agenda Item 6
Reliability and Security
Technical Committee Meeting
June 8, 2021

Reliability Guideline: Inadvertent Interchange

Action

Accept to post document for a 45-day comment period.

Summary

The Reliability Guideline: Inadvertent Interchange is a three-year review of an existing guideline that has been updated. Guideline Metrics section has been added in addition to the content update. The RS is requesting that this document be accepted to post for a 45-day comment period.

Reliability Guideline

Inadvertent Interchange

Applicability

Balancing Authorities (BAs)

Introduction and Purpose

It is in the public interest for NERC to develop guidelines that are useful for maintaining or enhancing the reliability of the Bulk Electric System (BES).

The Technical Committees of NERC—Operating Committee (OC), Planning Committee (PC) and the Critical Infrastructure Protection Committee (CIPC)—in accordance with their charters[1] are authorized by the NERC Board of Trustees (Board) to develop Reliability (OC and PC) and Security Guidelines (CIPC). These guidelines establish a voluntary code of practice on a particular topic for consideration and use by BES users, owners, and operators. These guidelines are coordinated by the technical committees and include the collective experience, expertise and judgment of the industry. The objective of this reliability guideline is to distribute key practices and information on specific issues critical to appropriately maintaining BES reliability. Reliability guidelines are not to be used to provide binding norms or create parameters by which compliance to standards are monitored or enforced. While the incorporation of guideline practices are strictly voluntary, reviewing, revising, or developing a program using these practices is highly encouraged to promote and achieve appropriate BES reliability.

This reliability guideline is intended to provide recommended practices for the management of Inadvertent Interchange (also referred to herein as inadvertent) accounting. With the goal of ensuring that, over the long term, BA Areas do not excessively depend on another BA Area in the Interconnection for meeting their demand or Interchange obligations.

Metrics

Pursuant to the Commission's Order on January 19, 2021, *North American Electric Reliability Corporation*, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review consistent with the RSTC Charter.

Baseline Metrics

- Performance of the BPS prior to and after a Reliability Guideline, as reflected in NERC's State of Reliability Report and Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments);
- Use and effectiveness of a Reliability Guideline as reported by industry via survey; and

[1] http://www.nerc.com/comm/OC/Related%20Files%20DL/OC_Charter_December_2016.pdf
http://www.nerc.com/comm/CIPC/Related%20Files%20DL/CIPC%20Charter%20BoT%20approved%205-05-2016.pdf
http://www.nerc.com/comm/PC/Related%20Files%202013/NERC_PC_Charter_2016_FINAL.pdf

- Industry assessment of the extent to which a Reliability Guideline is addressing risk as reported via survey.

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure and evaluate its effectiveness.

- No additional metrics

Background

The purpose of this document is to explain inadvertent accounting and support the Inadvertent Interchange accounting activities. The guideline is an aid to NERC, the Regions and Balancing Authorities, but does not set out compliance obligations nor is intended to be used as an auditor resource. Included within this document are accounting practices that every BA within NERC should follow. These practices provide a method for isolating and eliminating the source(s) of accounting errors. They may also be used as an aid in identifying the poor control performance that contributes to inadvertent accumulations.

Responsibilities

NERC OC - Resources Subcommittee (RS)

Provide oversight of the Inadvertent Interchange reporting process as implemented by the BA and Regional Administrators from each Regional Entity.

Balancing Authorities

Account for, calculate and report Inadvertent Interchange. Each BA is obligated to maintain its Inadvertent Interchange accounting within two periods, namely, On-Peak and Off-Peak. All hourly Schedules and Schedule changes are confirmed between the involved BA Areas prior to implementation in regard to common magnitude, rate of change, starting time, and ending time. As a double check, Interchange Schedules are also confirmed for the previous day.

Each BA must submit in a timely manner a monthly summary of Inadvertent Interchange to the NERC Inadvertent Interchange Reporting Tool (IIRT). Each BA must appoint one submitter and may appoint as many as five backup submitters. Each submitter may only modify the unlocked data for their BA only. The submitter is the only person who may alter the data in the tool, except under extenuating circumstances accepted by the chair of the NERC Resources Subcommittee (RS).

Regional Administrators (RA)

A single RA (and backup) is established voluntarily, for each Region to help maintain the data in the IIRT (https://inadvertent.nerc.net/webhub/) by ensuring the BAs have effectively reported Inadvertent Interchange data.

Tasks to be performed by the RA are as follows:

- If all the BAs in the Region do not have disputes, lock the IIRT on or around the 22nd calendar day of each month for the previous month's data. If disputes exist in the Region on or around the 22nd calendar day of the month, the RA should lock the tool in a timely matter once they are resolved.

Please refer to the Adjustments for Error section for further information regarding how BAs can make adjustments to data after the Tool has been locked for the month.

- Assist in dispute resolution when at least one BA in the RA's Region cannot agree on a Scheduled Net Interchange (NI_S) or Actual Net Interchange (NI_A) with at least one other BA.
- Verify total of BA's monthly actual and scheduled On-Peak and Off-Peak balances within the Region reflect zero after data submittals are complete.
  - If the balances do not equal zero, communicate with BAs to identify the root cause and assist in resolving the imbalance.
- Report, as necessary or by request, to the NERC RS on a quarterly basis the status of the Region inadvertent reporting by BA via email or at the RS meeting. For the Western Interconnect this reporting is handled by WECC not the RA. Please refer to the Managing the Interconnection Balance section for reports available through the IIRT.
- Provide, as necessary or by request, quarterly reports in January, April, July, and October for the prior quarter.
- Monitor BA in the Region's Inadvertent balance to ensure it does not exceed the recommended limits. (See Managing the Balancing Authorities' Balance section).

RAs shall report issues that may arise to the RS on no less than a quarterly basis. Questions about RA responsibilities can be directed to the chair of RS. RAs may only unlock and lock data and may only do so for the BAs in their region. RAs may view all the data for their interconnection. The chair (or designee) of the RS is considered a super-RA and has visibility of and lock/unlock capability for all BAs. Neither the chair of the RS (or designee), nor the RAs may modify the data for any BA. Under extenuating circumstances accepted by the chair of the RS, the IIRT Maintainer (IIRTM) may modify the data in the tool.

Inadvertent Interchange Reporting Tool Maintainer (IIRTM)

The IIRTM shall ensure that the data in the IIRT is maintained accurately (including incorporating changes in data due to changes in BA configurations) and shall repair any errors identified by the chair of the RS as soon as practicable.

Definitions

Please refer to the Glossary of Terms used in NERC Reliability Standards as posted on the NERC website for the definitions associated with the capitalized terms used in this document.

Guideline Details:

Inadvertent Interchange Accounting Procedure

Each BA shall calculate and record hourly Inadvertent Interchange which includes all AC and DC tie lines that connect to its Adjacent BA Areas in the same Interconnection and interchange served by jointly owned generators for On-Peak and Off-Peak periods.

Adjacent BA Areas shall operate to a common Net Interchange Schedule and Actual Net Interchange value and shall record these hourly quantities, with like values but opposite sign.

In order to ensure that each BA can agree to a common Scheduled Net Interchange and Actual Net Interchange, it is recommended that each BA, by the end of the next business day, agree with its adjacent BA to the hourly values of Net Interchange Schedule and hourly integrated megawatt-hour values of Actual Net Interchange.

Each BA needs to use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month in order to submit a monthly summary of Inadvertent Interchange to the IIRT. The values should be populated in the IIRT no later than the 15th calendar day of the following month.

These values are reported in the Central prevailing time zone and should only include agreed to values between by the Source BA, Sink BA and all Intermediate BAs. If the BAs cannot come to agreed values they should populate the actual interchange and schedule interchange they have at the time.

Differences

If BAs cannot mutually agree to a common Actual Net Interchange or Scheduled Net Interchange with like values but opposite signs by the 15th calendar day of the following month they need to contact their RA and advise them of the situation. The BAs need to provide to the RA a description of the cause for the dispute and the plan for correcting the discrepancy including the timeline for the completion. This includes instances where the BAs need additional time for reconciliation. In circumstances where an RA does not exist, the involved BAs should resolve their differences to meet the NERC and North American Energy Standards Board (NAESB) standards.

Documentation should be saved for the parties' involved up to 24 months after the difference has been resolved.

Adjustments for Error

A BA may make after-the-fact corrections to the agreed-to monthly accounting data only as needed to reflect actual operating conditions (e.g. a meter being used for control was sending bad data). After-the-fact corrections to scheduled or actual values can only be made with agreement of the impacted Adjacent BAs, by making equal, but opposite, adjustments.

If changes need to occur after the data has been locked, email a request form (See Appendix A) to the RA including the following information:

- The month and year for which a change needs to be made.
- Whether the change is for NI_A or NI_S.
- Explanation for the change.
- Agreements to the change from all BAs involved.

- Whether the change is On-Peak or Off-Peak.

In circumstances where an RA does not exist, the involved BAs should resolve their differences to meet the NERC and NAESB standards.

Managing the Balancing Authorities' Balance

Eastern Interconnection

Each BA's accumulated Inadvertent Interchange for both the monthly On-Peak period and the monthly Off-Peak period, individually, should not exceed 150% of the previous calendar year's average of integrated hourly peak Demand and integrated hourly peak generation (1.5*((average hourly peak for preceding calendar year + hourly peak generation)/2)). If the BA's balance does exceed 150% of the previous calendar year's average of integrated hourly Peak Demand and integrated hourly peak generation, it is expected that the BA should start a form of inadvertent payback method that includes a target of driving their balance towards zero in accordance with the NAESB requirements.

Western Interconnection

Each BA Area's accumulated Primary Inadvertent Interchange must be managed in accordance with BAL-004-WECCRequirement R1.

Dissolution of Balancing Authorities

When a BA deregisters, presumably to transfer its load and generation into another BA, its Inadvertent Interchange balance should be accurately accounted for to keep the Interconnection in balance. In the event the deregistering BA is being absorbed by more than one BA, the deregistering BA Inadvertent Interchange balance must be apportioned among the absorbing BAs.

The transfer of the inadvertent balance needs to occur the month *after* the dissolving BA is decommissioned.

The dissolving BA inadvertent balance will need to reflect *zero* in the IIRT. The new or acquiring BA would absorb the inadvertent balance of the dissolving BA.

The dissolving BA should contact the NERC RS, to discuss the necessary changes. This acts as a notification to the IIRTM so that an adjustment can be made to the IIRT.

The month after the dissolving BA's balance has been transitioned to the new BA(s) the IIRTM should remove that BA from the list of BAs that must report into the IIRT

Historical data will remain in the IIRT for the dissolving BA.

Below are examples for inadvertent accounting changes:

Example #1:

BA dissolving into a single BA

BA 1 last day of operation as a BA is June 30, 2012. They are being absorbed by BA 2 as of July 1, 2012 0000. BA 1 inadvertent balance will be taken to zero in the IIRT once they are no longer a BA.

BA1 has finished their end of the month check out for the month of June 2012 they report their remaining inadvertent balance, On-Peak and Off-Peak, to BA 2.

For the month of July 2012 BA 1 and BA2 would report the accumulated inadvertent numbers between the two of them in the Actual columns, taking BA 1 inadvertent balance to zero and increasing (in magnitude) BA 2 inadvertent balance by the agreed to amount.

As of June
BA 1 On peak Inadvertent Interchange = -300
BA 1 Off Peak Inadvertent Interchange = 500

For July
BA 1 would report on peak actual of 300 with an off peak actual value of -500.

BA 2 would report on peak actual of -300 with an off peak actual value of 500.

This would take BA 1 inadvertent balance to zero for both On-Peak and Off-Peak and adjust BA 2 inadvertent balance by the amount absorbed from BA 1.

For BA 1 these should be the only numbers reported in July 2012. Going forward BA 1 would no longer report values in the IIRT.

<u>Example #2:</u>
One BA dissolving into two BAs
BA 1 last day of operation as a BA is June 30, 2012. They are being split between two BAs (BA 2 and BA 3) as of July 1, 2012 0000. The three BAs have agreed to split the inadvertent 50/50 between BA 2 and BA 3.

BA 1 inadvertent balance will be taken to zero in the IIRT once they are no longer a BA.

BA1 has finished their end of the month check out for the month of June 2012 they report their remaining inadvertent balance, On-Peak and Off-Peak, to BA 2 and BA 3.

For the month of July 2012 BA 1, BA 2 and BA 3 would report the accumulated inadvertent numbers between the three of them in the Actual columns, taking BA 1 inadvertent balance to zero and increasing (in magnitude) BA 2 and BA 3 inadvertent balance by the agreed-to amount.

As of June
BA 1 On peak Inadvertent Interchange = -1000
BA 1 Off Peak Inadvertent Interchange = 5000

For July

BA 2 would take the following

On peak = -500
Off peak = 2500

BA 3 would take the following:

On peak = -500
Off peak = 2500

In the NERC Tool BA 1 would report with BA 2 an on peak value of 500 and off peak value of -2500. BA 2 would report with BA 1 on peak of -500 and off peak value of 2500.

In the NERC Tool BA 1 would report with BA 3 an on peak value of 500 and off peak value of -2500. BA 3 would report with BA 1 on peak of -500 and off peak value of 2500.

This will take BA 1 inadvertent accounting balance to zero for both on and off peak and adjust BA 2 and BA 3 by the agreed to amount.

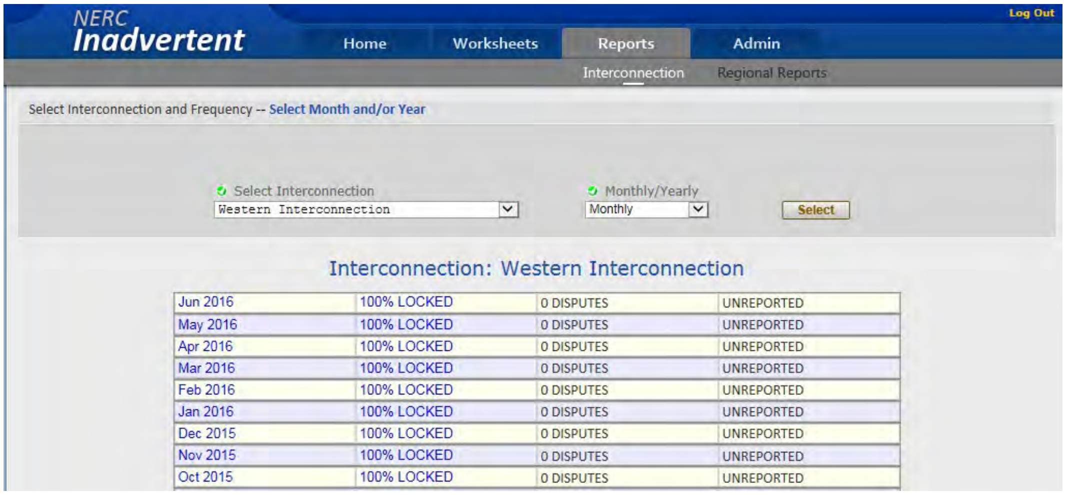
Creation of Balancing Authorities

Please refer to Housekeeping Task for New, Reconfigured or Retiring Balancing Authorities located on the NERC website.

Managing the Interconnection Balance

On a monthly basis, the summation of the Regions On-Peak and Off-Peak balances sum to zero in the IIRT. The IIRT has the capability to provide inadvertent reports. The Inadvertent Interchange reports can be located by following the steps below:

1. Go to the Reports tab on the top of the screen/Select the correct Interconnection and select Monthly under Monthly/Yearly. Once the screen has loaded, select the desired month by clicking on the blue hyperlink.



Select Interconnection and Frequency -- Select Month and/or Year

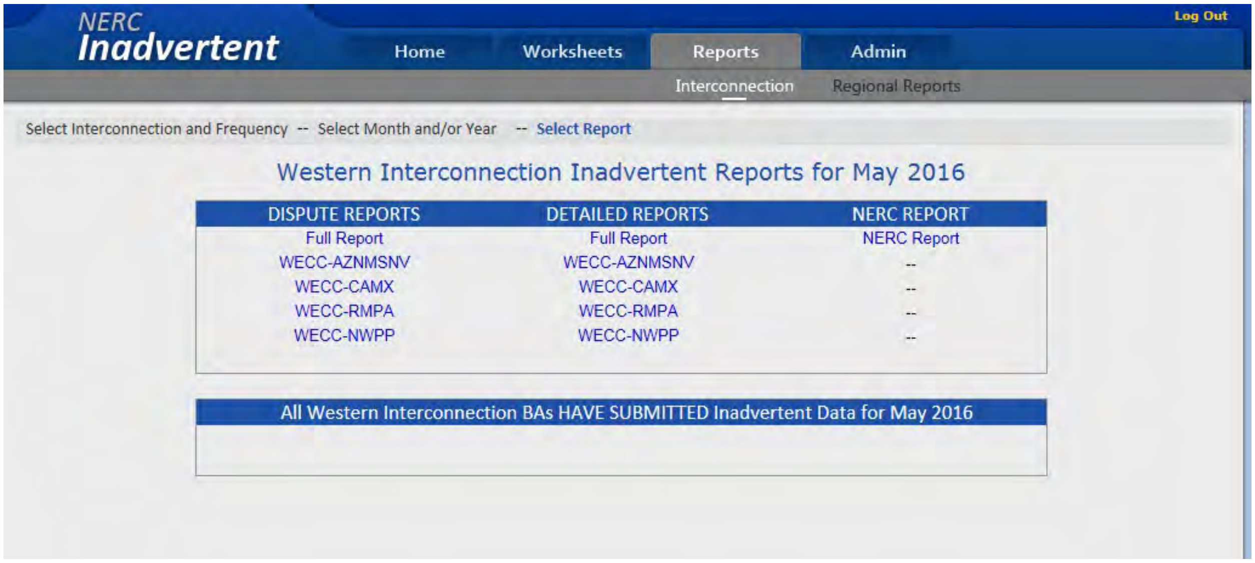
Select Interconnection: Western Interconnection

Monthly/Yearly: Monthly

Interconnection: Western Interconnection

Jun 2016	100% LOCKED	0 DISPUTES	UNREPORTED
May 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Apr 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Mar 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Feb 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Jan 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Dec 2015	100% LOCKED	0 DISPUTES	UNREPORTED
Nov 2015	100% LOCKED	0 DISPUTES	UNREPORTED
Oct 2015	100% LOCKED	0 DISPUTES	UNREPORTED

2. Click on the NERC Report link.

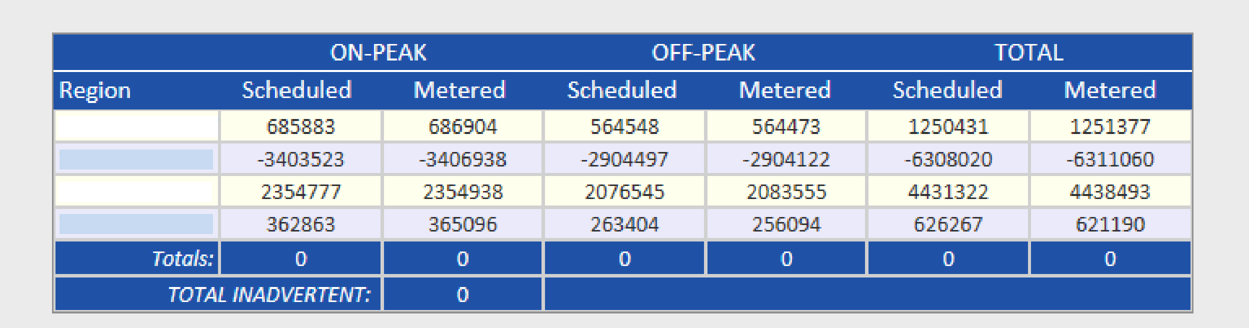

NERC
Inadvertent
Log Out
Home
Worksheets
Reports
Admin
Interconnection
Regional Reports
Select Interconnection and Frequency -- Select Month and/or Year -- Select Report

Western Interconnection Inadvertent Reports for May 2016

DISPUTE REPORTS	DETAILED REPORTS	NERC REPORT
Full Report	Full Report	NERC Report
WECC-AZNMSNV	WECC-AZNMSNV	--
WECC-CAMX	WECC-CAMX	--
WECC-RMPA	WECC-RMPA	--
WECC-NWPP	WECC-NWPP	--

All Western Interconnection BAs HAVE SUBMITTED Inadvertent Data for May 2016

3. Once the report is open, scroll to the bottom of the page and verify that the On Peak and Off Peak Totals net to zero between the Regions. Also verify the Total Inadvertent for the month is zero.



	ON-PEAK		OFF-PEAK		TOTAL	
Region	Scheduled	Metered	Scheduled	Metered	Scheduled	Metered
	685883	686904	564548	564473	1250431	1251377
	-3403523	-3406938	-2904497	-2904122	-6308020	-6311060
	2354777	2354938	2076545	2083555	4431322	4438493
	362863	365096	263404	256094	626267	621190
Totals:	0	0	0	0	0	0
TOTAL INADVERTENT:		0				

If the balance does not equal zero, the RA should investigate the root cause of the non-zero value and assist in resolving the imbalance. If the RA is unable to determine the cause of the discrepancy then the RA or the BA should contact the Chair of the NERC RS for assistance.

Inadvertent Interchange Payback Options

Eastern Interconnection

Please refer to the NAESB Wholesale Electric Quadrant (WEQ) Standard, Version 003, WEQ-007, entitled, Inadvertent Interchange Payback. The Federal Energy Regulatory Commission (FERC) approved Version 003 on September 18, 2014 in Order No. 676-H.[2]

Western Interconnection

[2] *Standards for Business Practices and Communication Protocols for Public Utilities*, 148 FERC ¶ 61,205 (2014).

Please refer to BAL-004-WECC. The only payback method allowed in the Western Interconnection is through automatic time error correction (ATEC); as described in the definition of Reportable ACE in the NERC Glossary of Terms.

Related Documents and Links:

NERC Operating Committee Charter

Revision History

Date	Version Number	Reason/Comments
7/27/2016	1.0	Initial Version – Inadvertent Interchange
12/13/2017	1.1	Addressed Industry Comments
12/14/2020	1.2	Triennial Review, add specificity around roles, account for dissolution of IIWG

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Appendix A

Request to Unlock NERC Inadvertent Interchange Tool Form

*This form must be completed and sent to the RA if the NERC Tool needs to be unlocked

Company: ______________________________

Name: ______________________________

Date: ______________________________

1. State the Month and Year of the requested change

Month: ____________ Year: ____________

2. Changes affect

□ Net Actual Interchange (NI_A)

□ Net Schedule Interchange (NI_S)

□ Both

3. Please explain the reason for the change request

____

____

____

____

4. List the names and contact information for each Balancing Authority (BA) representative who are in agreement with the change.

____

____

____

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Formatted: Numbering: Continuous

Reliability Guideline

Inadvertent Interchange

Applicability

Balancing Authorities (BAs)

Introduction and Purpose

It is in the public interest for NERC to develop guidelines that are useful for maintaining or enhancing the reliability of the Bulk Electric System (BES).

The Technical Committees of NERC—Operating Committee (OC), Planning Committee (PC) and the Critical Infrastructure Protection Committee (CIPC)—in accordance with their charters[1] are authorized by the NERC Board of Trustees (Board) to develop Reliability (OC and PC) and Security Guidelines (CIPC). These guidelines establish a voluntary code of practice on a particular topic for consideration and use by BES users, owners, and operators. These guidelines are coordinated by the technical committees and include the collective experience, expertise and judgment of the industry. The objective of this reliability guideline is to distribute key practices and information on specific issues critical to appropriately maintaining BES reliability. Reliability guidelines are not to be used to provide binding norms or create parameters by which compliance to standards are monitored or enforced. While the incorporation of guideline practices are strictly voluntary, reviewing, revising, or developing a program using these practices is highly encouraged to promote and achieve appropriate BES reliability.

Formatted: Underline

Formatted: Underline

Formatted: Underline

Commented [A1]: This boilerplate will need to be replaced

This reliability guideline is intended to provide recommended practices for the management of Inadvertent Interchange (also referred to herein as inadvertent) accounting. With the goal of ensuring that, over the long term, BA Areas do not excessively depend on another BA Area in the Interconnection for meeting their demand or Interchange obligations.

Metrics

Pursuant to the Commission's Order on January 19, 2021, *North American Electric Reliability Corporation*, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review consistent with the RSTC Charter.

Baseline Metrics

- Performance of the BPS prior to and after a Reliability Guideline, as reflected in NERC's State of Reliability Report and Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments);

[1] http://www.nerc.com/comm/OC/Related%20Files%20DL/OC_Charter_December_2016.pdf
http://www.nerc.com/comm/CIPC/Related%20Files%20DL/CIPC%20Charter%20BoT%20approved%205-05-2016.pdf
http://www.nerc.com/comm/PC/Related%20Files%202013/NERC_PC_Charter_2016_FINAL.pdf

- Use and effectiveness of a Reliability Guideline as reported by industry via survey; and
- Industry assessment of the extent to which a Reliability Guideline is addressing risk as reported via survey.

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure and evaluate its effectiveness.

- No additional metrics

Background

The purpose of this document is to explain inadvertent accounting and ~~supports~~support the Inadvertent Interchange ~~Accounting~~accounting activities. The guideline is an aid to NERC, the Regions and Balancing Authorities, but does not set out compliance obligations nor is intended to be used as an auditor resource. Included within this document are accounting practices that every BA within NERC should follow. These practices provide a method for isolating and eliminating the source(s) of accounting errors. They may also be used as an aid in identifying the poor control performance that contributes to inadvertent accumulations.

Responsibilities

NERC OC - Resources Subcommittee (RS)

Provide oversight of the Inadvertent Interchange reporting process as implemented by the BA and Regional Administrators from each Regional Entity.

Balancing Authorities

Account for, calculate and report Inadvertent Interchange. Each BA is obligated to maintain its Inadvertent Interchange accounting within two periods, namely, On-Peak and Off-Peak. All hourly Schedules and Schedule changes are confirmed between the involved BA Areas prior to implementation in regard to common magnitude, rate of change, starting time, and ending time. As a double check, Interchange Schedules are also confirmed for the previous day.

Each BA must submit in a timely manner a monthly summary of Inadvertent Interchange to the NERC Inadvertent Interchange Reporting Tool~~.~~ (IIRT). Each BA must appoint one submitter and may appoint as many as five backup submitters. Each submitter may only modify the unlocked data for their BA only. The submitter is the only person who may alter the data in the tool, except under extenuating circumstances accepted by the chair of the NERC Resources Subcommittee (RS).

Regional Administrators (RA)

~~An~~A single RA (and backup) is established voluntarily, for each Region to help maintain the ~~NERC Inadvertent Interchange Reporting Tool~~data in the IIRT (https://inadvertent.nerc.net/webhub/) by ensuring the BAs have effectively reported Inadvertent Interchange ~~Data~~data.

Tasks to be performed by the RA are as follows:

Formatted: Heading 2, Left

Formatted: Font: Not Bold

- ~~Lock~~If all the ~~NERC Inadvertent Interchange Reporting Toolon~~BAs in the Region do not have disputes, lock the IIRT on or around the 22nd calendar day of each month for the previous month's data. If disputes exist in the Region on or around the 22nd calendar day of the month, the RA should lock the tool in a timely matter once they are resolved. Please refer to the Adjustments for Error section for further information regarding how BAs can make adjustments to data after the Tool has been locked for the month.
- Assist in dispute resolution when ~~two BAs~~at least one BA in the RA's Region cannot agree on a Scheduled Net Interchange (NI_S) or Actual Net Interchange (NI_A~~).~~) with at least one other BA.
- Verify ~~Interconnection's~~total of BA's monthly actual and scheduled On-Peak and Off-Peak balances within the Region reflect zero after data submittals are complete.
    - If the ~~balance does~~balances do not equal zero, communicate with BAs to identify the root cause and assist in resolving the imbalance.
- Report, as necessary or by request, to the NERC RS on a quarterly basis the status of the Region inadvertent reporting by BA via email or at the RS meeting. For the Western Interconnect this reporting is handled by WECC not the RA. Please refer to the Managing the Interconnection Balance section for reports available through the IIRT.
- Provide, as necessary or by request, quarterly reports in January, April, July, and October for the prior quarter.
- Monitor ~~BA's~~BA in the Region's Inadvertent balance to ensure it does not exceed the recommended limits. (See Managing the Balancing Authorities' Balance section~~)~~).

Formatted: Superscript

RAs shall report issues that may arise to the RS on no less than a quarterly basis. Questions about RA responsibilities can be directed to the chair of RS. RAs may only unlock and lock data and may only do so for the BAs in their region. RAs may view all the data for their interconnection. The chair (or designee) of the RS is considered a super-RA and has visibility of and lock/unlock capability for all BAs. Neither the chair of the RS (or designee), nor the RAs may modify the data for any BA. Under extenuating circumstances accepted by the chair of the RS, the IIRT Maintainer (IIRTM) may modify the data in the tool.

Inadvertent Interchange Reporting Tool Maintainer (IIRTM)

The IIRTM shall ensure that the data in the IIRT is maintained accurately (including incorporating changes in data due to changes in BA configurations) and shall repair any errors identified by the chair of the RS as soon as practicable.

Definitions

Please refer to the Glossary of Terms used in NERC Reliability Standards as posted on the NERC website for the definitions associated with the capitalized terms used in this document.

Guideline Details:

Inadvertent Interchange Accounting Procedure

Each BA shall calculate and record hourly Inadvertent Interchange which includes all AC and DC tie lines that connect to its Adjacent BA Areas in the same Interconnection and interchange served by jointly owned generators for On-Peak and Off-Peak periods.

Adjacent BA Areas shall operate to a common Net Interchange Schedule and Actual Net Interchange value and shall record these hourly quantities, with like values but opposite sign.

In order to ensure that each BA can agree to a common Scheduled Net Interchange and Actual Net Interchange, it is recommended that ~~the BAs~~each BA, by the end of the next business day, agree with its adjacent BA to the hourly values of Net Interchange Schedule and hourly integrated megawatt-hour values of Actual Net Interchange.

~~The~~Each BA needs to use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month in order ~~for the BAs~~ to submit a monthly summary of Inadvertent Interchange to the ~~NERC reporting tool.~~IIRT. The values should be populated in the ~~NERC tool~~IIRT no later than the 15th calendar day of the following month.

These values are reported in the Central prevailing time zone and should only include agreed to values between by the Source BA, Sink BA and all Intermediate BAs. If the BAs cannot come to agreed values they should populate the actual interchange and schedule interchange they have at the time.

Differences

If~~ the~~ BAs cannot mutually agree to a common Actual Net Interchange or Scheduled Net Interchange with like values but opposite signs by the 15th calendar day of the following month they need to contact their RA and advise them of the situation. The BAs need to provide to the RA a description of the cause for the dispute and the plan for correcting the discrepancy including the timeline for the completion. This includes instances where the BAs need additional time for reconciliation. In circumstances where an RA does not exist, the involved BAs should resolve their differences to meet the NERC and North American Energy Standards Board (NAESB) standards~~, such as BAL-005. ~~.

Documentation should be saved for the parties' involved up to 24 months after the difference has been resolved.

Adjustments for Error

A BA may make after-the-fact corrections to the agreed-to monthly accounting data only as needed to reflect actual operating conditions (e.g. a meter being used for control was sending bad data). After-the-fact corrections to scheduled or actual values can only be made with agreement of the impacted Adjacent BAs, by making equal, but opposite, adjustments.

If changes need to occur after the data has been locked, email a request form (See Appendix A) to the RA including the following information:

- The month and year for which a change needs to be made.
- Whether the change is for NI_A or NI_S.

- Explanation for the change.
- Agreements to the change from all BAs involved.
- Whether the change is On-Peak or Off-Peak.

In circumstances where an RA does not exist, the involved BAs should resolve their differences to meet the NERC and NAESB standards~~, such as BAL-005~~.

Managing the Balancing Authorities’ Balance

Eastern Interconnection

Each BA’s accumulated Inadvertent Interchange for both the monthly On-Peak period and the monthly Off-Peak period, individually, should not exceed 150% of the previous calendar year’s average of integrated hourly ~~Peak~~peak Demand and integrated hourly peak generation (1.5*((average hourly peak for preceding calendar year + hourly peak generation)/2)). If the BA’s balance does exceed 150% of the previous calendar year’s average of integrated hourly Peak Demand and integrated hourly peak generation, it is expected that the BA should start a form of inadvertent payback method that includes a target of driving their balance ~~down~~ towards zero in accordance with the ~~North American Energy Standards Board (~~NAESB~~)~~ requirements.

Western Interconnection

Each BA Area’s accumulated Primary Inadvertent Interchange must be managed in accordance with BAL-004-WECCRequirement R1.

Dissolution of Balancing Authorities

When a BA deregisters, presumably to transfer its load and generation into another BA, its Inadvertent Interchange balance should be accurately accounted for to keep the Interconnection in balance. In the event the deregistering BA is being absorbed by more than one BA, the deregistering BA Inadvertent Interchange balance must be apportioned among the absorbing BAs.

The transfer of the inadvertent balance needs to occur the month *after* the dissolving BA is decommissioned.

The dissolving BA inadvertent balance will need to reflect *zero* in the ~~NERC Inadvertent Interchange reporting tool.~~IIRT. The new or acquiring BA would absorb the inadvertent balance of the dissolving BA.

The dissolving BA should contact the NERC RS, to discuss the necessary changes. This acts as a notification to the ~~vendor of the tool~~IIRTM so that an adjustment can be made to the ~~NERC inadvertent reporting tools~~IIRT.

The month after the dissolving BA’s balance has been transitioned to the new BA(s) the ~~vendor of the tool~~IIRTM should remove that BA from the list of BAs that must report into the ~~NERC inadvertent reporting tool.~~IIRT

Historical data will remain in the ~~NERC inadvertent reporting tool~~IIRT for the dissolving BA.

Below are examples for inadvertent accounting changes:

Example #1:

BA dissolving into a single BA
BA 1 last day of operation as a BA is June 30, 2012. They are being absorbed by BA 2 as of July 1, 2012 0000. BA 1 inadvertent balance will be taken to zero in the ~~NERC Inadvertent Interchange reporting tool~~IIRT once they are no longer a BA.

BA1 has finished their end of the month check out for the month of June 2012 they report their remaining inadvertent balance, ~~on~~On-Peak and ~~off peak~~Off-Peak, to ~~BA2~~BA 2.

For the month of July 2012 BA 1 and BA2 would report the accumulated inadvertent numbers between the two of them in the Actual columns, taking BA 1 inadvertent balance to zero and increasing (in magnitude) BA 2 inadvertent balance by the agreed to amount.

As of June
BA 1 On peak Inadvertent Interchange = -300
BA 1 Off Peak Inadvertent Interchange = 500

For July
BA 1 would report on peak actual of 300 with an off peak actual value of -500.

BA 2 would report on peak actual of -300 with an off peak actual value of 500.

This would take BA 1 inadvertent balance to zero for both ~~on~~On-Peak and ~~off peak~~Off-Peak and adjust BA 2 inadvertent balance by the amount absorbed from BA 1.

For BA 1 these should be the only numbers reported in July 2012. Going forward BA 1 would no longer report values in the ~~NERC Inadvertent Interchange reporting tool.~~IIRT.

Example #2:

One BA dissolving into two BAs
BA 1 last day of operation as a BA is June 30, 2012. They are being split between two BAs (BA 2 and BA 3) as of July 1, 2012 0000. The three BAs have agreed to split the inadvertent 50/50 between BA 2 and BA 3.

BA 1 inadvertent balance will be taken to zero in the ~~NERC Inadvertent Interchange reporting tool~~IIRT once they are no longer a BA.

BA1 has finished their end of the month check out for the month of June 2012 they report their remaining inadvertent balance, ~~on~~On-Peak and ~~off peak~~Off-Peak, to ~~BA2~~BA 2 and BA 3.

For the month of July 2012 BA 1, ~~BA2~~BA 2 and BA 3 would report the accumulated inadvertent numbers between the three of them in the Actual columns, taking BA 1 inadvertent balance to zero and increasing (in magnitude) BA 2 and BA 3 inadvertent balance by the agreed~~-~~ to amount.

Formatted: Font: Not Italic

As of June
BA 1 On peak Inadvertent Interchange = -1000
BA 1 Off Peak Inadvertent Interchange = 5000

For July
BA 2 would take the following
On peak = -500
Off peak = 2500

BA 3 would take the following:
On peak = -500
Off peak = 2500

In the NERC Tool BA 1 would report with BA 2 an on peak value of 500 and off peak value of -2500. ~~BA2~~BA 2 would report with BA 1 on peak of -500 and off peak value of 2500.

In the NERC Tool BA 1 would report with BA 3 an on peak value of 500 and off peak value of -2500. BA 3 would report with BA 1 on peak of -500 and off peak value of 2500.

This will take BA 1 inadvertent accounting balance to zero for both on and off peak and adjust BA 2 and BA 3 by the agreed to amount.

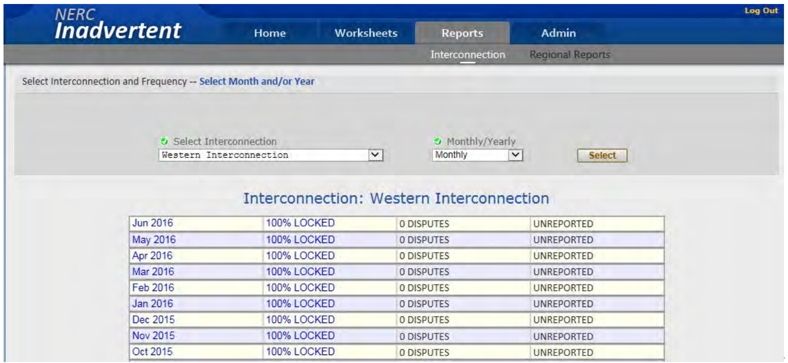
Creation of Balancing Authorities

Please refer to Housekeeping Task for New, Reconfigured or Retiring Balancing Authorities located on the NERC website.

Managing the Interconnection Balance

On a monthly basis, the summation of the Regions On-Peak and Off~~-~~ Peak balances sum to zero in the ~~NERC inadvertent reporting tool.~~IIRT. The ~~NERC Inadvertent Interchange reporting tool~~IIRT has the capability to provide inadvertent reports. The Inadvertent Interchange reports can be located by following the steps below:

1. Go to the Reports tab on the top of the screen/Select the correct Interconnection and select Monthly under Monthly/Yearly. Once the screen has loaded, select the desired month by clicking on the blue hyperlink.



Select Interconnection and Frequency -- Select Month and/or Year

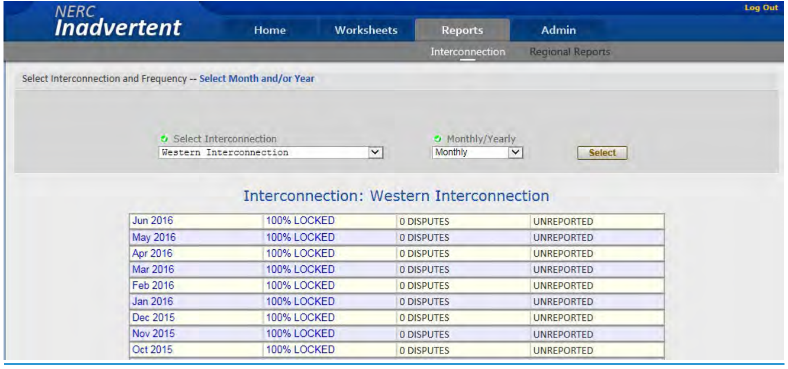
Select Interconnection: Western Interconnection

Monthly/Yearly: Monthly

Select

Interconnection: Western Interconnection

Jun 2016	100% LOCKED	0 DISPUTES	UNREPORTED
May 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Apr 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Mar 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Feb 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Jan 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Dec 2015	100% LOCKED	0 DISPUTES	UNREPORTED
Nov 2015	100% LOCKED	0 DISPUTES	UNREPORTED
Oct 2015	100% LOCKED	0 DISPUTES	UNREPORTED



Select Interconnection and Frequency -- Select Month and/or Year

Select Interconnection: Western Interconnection

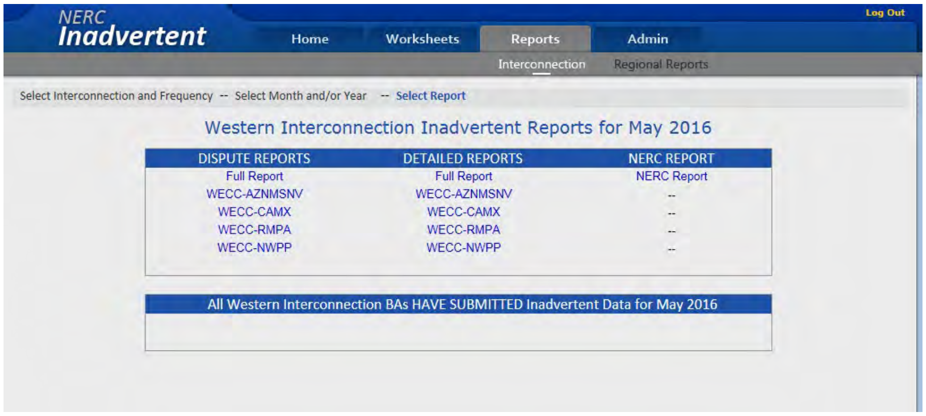
Monthly/Yearly: Monthly

Select

Interconnection: Western Interconnection

Jun 2016	100% LOCKED	0 DISPUTES	UNREPORTED
May 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Apr 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Mar 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Feb 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Jan 2016	100% LOCKED	0 DISPUTES	UNREPORTED
Dec 2015	100% LOCKED	0 DISPUTES	UNREPORTED
Nov 2015	100% LOCKED	0 DISPUTES	UNREPORTED
Oct 2015	100% LOCKED	0 DISPUTES	UNREPORTED

2. Click on the NERC Report link.

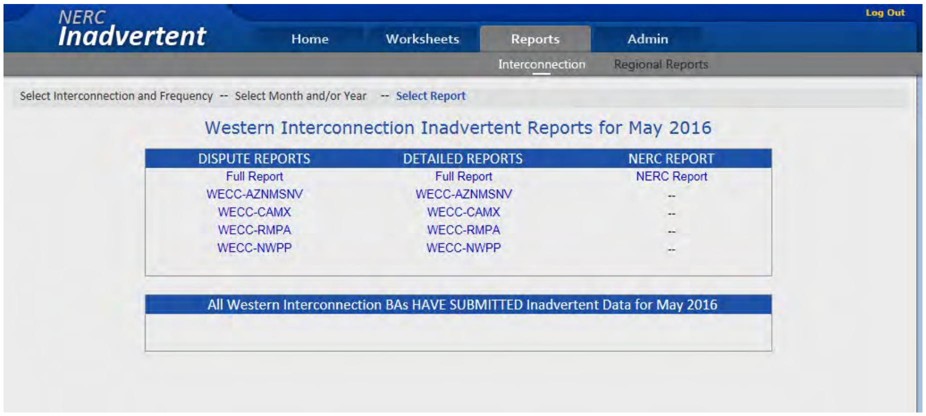


Select Interconnection and Frequency -- Select Month and/or Year -- Select Report

Western Interconnection Inadvertent Reports for May 2016

DISPUTE REPORTS	DETAILED REPORTS	NERC REPORT
Full Report	Full Report	NERC Report
WECC-AZNMSNV	WECC-AZNMSNV	--
WECC-CAMX	WECC-CAMX	--
WECC-RMPA	WECC-RMPA	--
WECC-NWPP	WECC-NWPP	--

All Western Interconnection BAs HAVE SUBMITTED Inadvertent Data for May 2016



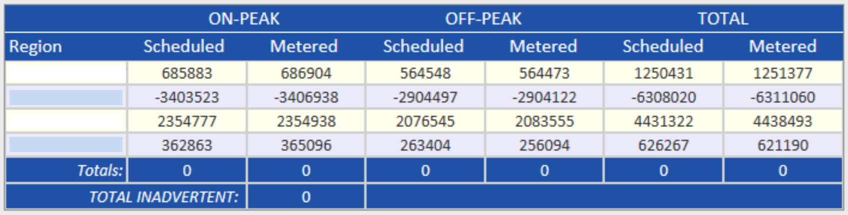
Select Interconnection and Frequency -- Select Month and/or Year -- Select Report

Western Interconnection Inadvertent Reports for May 2016

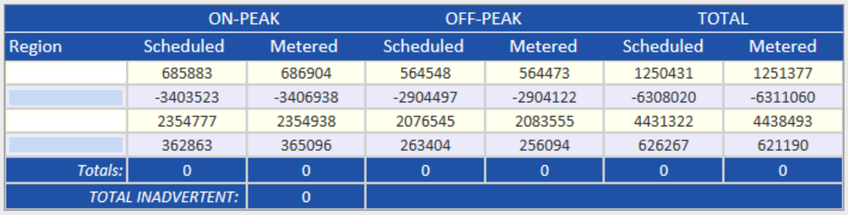
DISPUTE REPORTS	DETAILED REPORTS	NERC REPORT
Full Report	Full Report	NERC Report
WECC-AZNMSNV	WECC-AZNMSNV	--
WECC-CAMX	WECC-CAMX	--
WECC-RMPA	WECC-RMPA	--
WECC-NWPP	WECC-NWPP	--

All Western Interconnection BAs HAVE SUBMITTED Inadvertent Data for May 2016

3. Once the report is open, scroll to the bottom of the page and verify that the On Peak and Off Peak Totals net to zero between the Regions. Also verify the Total Inadvertent for the month is zero.



	ON-PEAK		OFF-PEAK		TOTAL	
Region	Scheduled	Metered	Scheduled	Metered	Scheduled	Metered
	685883	686904	564548	564473	1250431	1251377
	-3403523	-3406938	-2904497	-2904122	-6308020	-6311060
	2354777	2354938	2076545	2083555	4431322	4438493
	362863	365096	263404	256094	626267	621190
Totals:	0	0	0	0	0	0
TOTAL INADVERTENT:		0				



	ON-PEAK		OFF-PEAK		TOTAL	
Region	Scheduled	Metered	Scheduled	Metered	Scheduled	Metered
	685883	686904	564548	564473	1250431	1251377
	-3403523	-3406938	-2904497	-2904122	-6308020	-6311060
	2354777	2354938	2076545	2083555	4431322	4438493
	362863	365096	263404	256094	626267	621190
Totals:	0	0	0	0	0	0
TOTAL INADVERTENT:		0				

If the balance does not equal zero, the RA should investigate the root cause of the non-zero value and assist in resolving the imbalance. If the RA is unable to determine the cause of the discrepancy then the RA or the BA should contact the Chair of the NERC RS for assistance.

Inadvertent Interchange Payback Options

Eastern Interconnection

Please refer to the NAESB Wholesale Electric Quadrant (WEQ) Standard, Version 003, WEQ-007, entitled, Inadvertent Interchange Payback. The Federal Energy Regulatory Commission (FERC) approved Version 003 on September 18, 2014 in Order No. 676-H.[2]

Western Interconnection

Please refer to BAL-004-WECC. The only payback method allowed in the Western Interconnection is through automatic time error correction (ATEC); as described in the definition of Reportable ACE in the NERC Glossary of Terms.

Related Documents and Links:

NERC Operating Committee Charter

Revision History

Date	Version Number	Reason/Comments
7/27/2016	1.0	Initial Version – Inadvertent Interchange
12/13/2017	1.1	Addressed Industry Comments
12/14/2020	1.2	Triennial Review, add specificity around roles, account for dissolution of IIWG

[2] *Standards for Business Practices and Communication Protocols for Public Utilities*, 148 FERC ¶ 61,205 (2014).

Appendix A

Request to Unlock NERC Inadvertent Interchange Tool Form

*This form must be completed and sent to the RA if the NERC Tool needs to be unlocked

Company: ______________________________

Name: ______________________________

Date: ______________________________

1. State the Month and Year of the requested change

Month: ______________ Year: ______________

2. Changes affect

☐ Net Actual Interchange (NI_A)

☐ Net Schedule Interchange (NI_S)

☐ Both

3. Please explain the reason for the change request

____

____

____

____

4. List the names and contact information for each Balancing Authority (BA) representative who are in agreement with the change.

____

____

____

Reliability Guideline: Gas and Electrical Operational Coordination Considerations

Action

Approve

Background

In December 2017, NERC published the Reliability Guideline: Gas and Electrical Operational Coordination Considerations. This guideline began a triennial review, comment, and update in 2020. The work to finalize an updated version of the document is slated on the Real Time Operating Subcommittee (RTOS) work plan to be completed in Q2 of 2021.

Summary

In total, sixty comments were received on the document from seven different entities:

- 45 of the comments were incorporated in the updated version of the document, either exactly as requested or in a similar fashion.
- 14 comments were not incorporated, seven of which were not requesting change.
- Comments were submitted from a number of organizations, resulting in several duplicate comments which were addressed similarly among them.

The majority of the comments that were specifically not included when requesting changes fall into three major themes.

1. Comments that implied that the reliability guideline is new rather than a 2017 publication undergoing a review period, specifically recommending that the guideline should not be issued for a number of reasons.
2. Comments that implied that the reliability guideline be enforced like a reliability standard rather than a voluntary set of recommended considerations. If ever there is a conflict of information provided a reliability guideline with a NERC standard, local market rules, or local/state/provincial/federal laws, it must be understood that the former prevails.
3. Comments that implied that such recommendations are unachievable or unrelated to gas/electric coordination when there are examples of implementation in several regions throughout North America that was both successful and applicable.

Every recommendation of a reliability guideline may not apply to every organization, as there are many different roles at the various entities that work together to collectively run the power system. However, it must be understood that reliability guidelines offer suggestions that could be helpful but must be evaluated for implementation into any specific scenario.

Conversely, there are several comments that follow a theme of providing information that would be beneficial to the industry. A number of comments recommended including considerations for electric gas compression stations into the electric system restoration plans, in addition to the existing language that recommended evaluating the impact of load shed on those same facilities. Conceptually, these two are the same, but in implementation, the planning and process development may be done by different groups of people or even different organizations, making this distinction beneficial.

Other comments were added to make the document more inclusive. Expanding coordination, training, and communication to more groups and organizations may serve to expand the value of the reliability guideline. This additional information that was recommended for inclusion is shown in the redline version of the guideline and serves to improve the overall quality of the document.

Finally, the last comment that was neither addressed nor was it refuted requires engagement with NERC staff to determine the response. In a 2020 FERC order, the evaluation of the effectiveness of reliability guidelines was outlined. This would be addressed by NERC staff rather than the RTOS.

Draft Reliability Guideline

Gas and Electrical Operational Coordination Considerations

Applicability:

Reliability Coordinators (RCs), Balancing Authorities (BAs), Transmission Operators (TOPs)
Generator Owners (GOs), and Generator Operators (GOPs)

Preamble

It is in the public interest for the North American Electric Reliability Corporation (NERC) to develop guidelines that are useful for maintaining or enhancing the reliability of the Bulk Electric System (BES). The Reliability and Security Technical Committee (RSTC) are, per their charter authorized by the NERC Board of Trustees (Board) to develop Reliability and Security Guidelines. Guidelines establish voluntary codes of practice for consideration and use by BES users, owners, and operators. These guidelines are developed by the technical committees and include the collective experience, expertise and judgment of the industry. Reliability guidelines do not provide binding norms or create parameters by which compliance to standards is monitored or enforced. While the incorporation and use of guideline practices is strictly voluntary, the review, revision, and development of a program using these practices is strongly encouraged to promote and achieve the highest levels of reliability for the BES. Nothing in this guideline negates obligations or requirements under an entity's regulatory framework (local, state or federal) and all parties must take those requirements into consideration when implementing any of the guidance detailed herein.

Metrics

Pursuant to the Commission's Order on January 19, 2021, *North American Electric Reliability Corporation*, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review consistent with the RSTC Charter.

Baseline Metrics

- Performance of the BPS prior to and after a Reliability Guideline, as reflected in NERC's State of Reliability Report and Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments);
- Use and effectiveness of a Reliability Guideline as reported by industry via survey; and
- Industry assessment of the extent to which a Reliability Guideline is addressing risk as reported via survey.

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure and evaluate its effectiveness.

- No additional metrics

Background and Purpose

Coordination of operations between the gas and electric industries has become increasingly important over the course of the last decade. The electric power sector's use of gas, specifically natural gas-fired generation, has grown exponentially in many areas of North America due to increased availability of gas, potentially more competitive costs in relation to other fuels and a move throughout the industry to lower emissions to meet environmental goals. With increased growth in gas usage comes greater reliance and associated risk due to the dependency that each industry now has on the other. The operational impact of these dependencies requires gas and electric system operators to actively coordinate planning and operations. The goal of the coordination is to ensure that both the gas and electric systems remain secure and reliable during normal, and emergency conditions. This guideline attempts to provide a set of principles and strategies that may be adopted should the Region in which you operate require close coordination due to increased dependency. This guideline does not apply universally, and an evaluation of your area's unique needs is essential to determine which principles and strategies you apply. The guideline principles and strategies may be applied by RCs, BAs, TOPs, GOs and GOPs in order to ensure reliable coordination with the gas industry. Finally, the document focuses on the areas of preparation, coordination, communication and gathering and sharing information that may be applied in order to coordinate gas-electric utility operations and minimize reliability-related risk.

Guideline Content:

A. Establish Gas and Electric Industry Coordination Mechanisms

- Establish Contacts
  - An essential part of any coordination activity is the identification of participants. For gas and electric coordination, this could involve the identification of the natural gas interstate/intrastate pipelines, gas suppliers and Local Distribution Companies (LDC) as well as gas industry operations staff within the electric footprint boundaries and in some instances beyond those boundaries. Once contacts among these participants are established, additional coordination activities can begin. Gas industry trade organizations, such as the Interstate Natural Gas Association of America, Natural Gas Supply Association, American Gas Association or a regional entity such as the Northeast Gas Association may be able to aid in development of operational contacts and the establishment of coordination protocols. These contacts should be developed for long and short term planning/outage coordination as well as near term and real-time operations at a variety of organizations including, but not limited to, Reliability Coordinators, Balancing Authority Operators, Transmission Operators, Generator Operators, and Gas Control Operators.

The contacts should include both control room operating staff contacts as well as management. Establishing and maintaining these contacts is the most important aspect of gas and electric coordination. However, communications should be established during normal operations, so that the first call you make to a gas transmission pipeline or LDC should not be under emergency conditions.

- Communication Protocols
  - Once counterparts are identified in the gas industry, communications protocols will need to be established within the regulatory framework of both energy sectors looking to coordinate and share information. The Federal Energy Regulatory Commission issued a Final Rule under Order No. 787 allowing interstate natural gas pipelines and electric transmission operators to share non-public operational information to promote the reliability and integrity of their systems. Since the inception of this rule and the subsequent incorporation of those rules into the associated tariffs, followed by the appropriate confidentiality agreements, gas and electric entities have been able to freely share operational data. Data that could be shared to improve operational coordination may include but is not necessarily limited to the following:
    - Providing detailed operational reports to the gas pipeline operators by specific generating assets, operating on specific pipelines, which specify expected fuel burn by asset, by hour over the dispatch period under review. It is important to convert dispatch plans from electric power (MWh) to gas demand (in terms of gas units/time such as dekatherms/day or MMcf/hour) when conveying that information to gas system operators.
    - Combining the expected fuel to be used by asset on each pipeline in aggregate to provide an expected draw on the pipeline by generation connected to that pipeline on an hourly basis and on a gas and electric day basis.
  - Exchanging real-time operating information in both verbal and electronic forms (e.g., pipeline company informational postings) of actual operating conditions on specific assets on specific pipelines. Also consider the electronic communication of real-time system information between affected parties, such as real-time gas meter readings and generator dispatch instructions.
  - Outage planning for elements of significance to include sharing detailed electric and gas asset scheduling information on all time horizons and coordinating outages of those assets to ensure reliability on both the gas and electric systems. Examples include, but are not limited to, must-run requirements, inline inspection operations, risk of disruption to electric compression, and pipeline outages potentially causing the need for pressure reductions.
  - Scheduling coordination meetings, face-to-face whenever possible, on a periodic basis (e.g.annual, bi-annual, quarterly, etc…) to discuss a range of topics including but not limited to outage coordination, proposed electric/gas market rule changes, upcoming gas generator additions, pending electric retirements/repowers, enhancements/modifications to gas/electric coordination tools, gas pipeline infrastructure changes, near/long-term seasonal forecasts and load shape changes.

- Sharing normal and emergency conditions in real-time and ensuring each entity understands the implications to their respective systems. This should include gas and electric entities proactively reaching out to the operators of stressed gas systems to discuss the impacts, adverse or otherwise, of their expected or available actions. Understand the direct impacts to electric generation assets when gas pipelines are directed under more extreme gas system operating conditions and/or force majeure conditions.

- The sharing of non-public operating information between the electric operating entity and LDC, intrastate pipelines, and gathering pipelines is not covered under FERC Order 787. For this reason, individual communication and coordination protocols should be considered with each LDC and intrastate pipelines within the footprint of the operating entity. These protocols might be set up to specifically allow gas dispatchers or dispatch departments at intrastate, LDC, and gathering pipelines to communicate directly with generator operators.

    - Understanding the conditions under which an LDC or intrastate pipeline would interrupt gas-fired generation is of particular importance and incorporating this information into operational procedures and planning will assist in identification of potential at-risk generation.

    - Setting up electronic/email alerts from each LDC or intrastate pipeline as to the potential declaration of interruptions is one key means of real time identification of potential loss of generation behind the LDC city gate or meter station on an intrastate pipeline.

- Addressing the identification of electricity source for electric compression stations and protocols for protecting these sources during periods of high demand or system stress with plans to mitigate such risk, when possible.

- Coordinating Procurement Time Lines

    - Operating entities may want to consider changing next day operating plan scheduling practices to align more efficiently with gas day procurement cycles. The gas and electric industries operate on differing timelines for the Day Ahead planning processes and in real-time, with the electric day on a local midnight to midnight cycle. The gas industry process operates on a differing timeline with the operating day beginning at 9 a.m. Central Clock Time and uniform throughout North America. This difference in operating days can lead to inefficient scheduling of natural gas to meet the electric day demands. In many instances throughout North America, the electric industry has moved the development and publishing of unit commitments and next day operating plans in order to ensure that generation resources have the ability to procure and nominate natural gas more efficiently to better meet the scheduling timelines of the gas industry. In addition, the gas industry has adjusted some of its nomination and scheduling practices to allow for more efficient scheduling that meets the needs of the electric system.

    - Coordinating and modifying scheduling practices using more effective time periods may allow for a higher level of pipeline utilization, but more importantly, may provide the early identification of constraints that could require starting gas generation with alternate fuels if available, or using non-gas-fired facilities for fuel diversity to meet the energy and reserve needs of the electric system. Recently, the fast-ramping capability of gas-fired units has been used some places to bolster grid flexibility in areas trending toward more renewable energy, primarily with variable and intermittent supplies of fuel (e.g. sunshine, wind, and water). Maintaining a balanced power system will require a more flexible approach to energy and capacity adequacy in order to sustain operational awareness.

- Identification of Critical Gas System Components and Dual-fuel Supplier Components
  - It is essential gas and electric operating entities coordinate to ensure that critical natural gas pipelines, compressor stations, LNG, and other gas storage, natural gas processing plants, and other critical gas system components, identified by the owners and/or operators, should not be subject to electric utility load shedding in general but more specifically Under Frequency and or Manual Load shedding programs.
    - Electric transmission and distribution owners are capable of interrupting electrical load either automatically through under frequency load shedding relays installed in substations throughout North America or via manual load shedding ordered by RCs, BAs and or TOPs via SCADA. These manual and automatic load shedding protocols are part of every entity's emergency procedures. Entities should try to ensure critical gas sector infrastructure is not located on electrical circuits that are subject to the load shedding as described above. Electric operators should establish contact with the gas companies operating within its jurisdiction to compile a list of critical gas and other fuel facilities which are dependent upon electric service for operations. This list should also consider the availability of backup generation at critical gas facilities. Once the list is compiled, a comprehensive review of load shedding procedures/schemas/circuits should be done to verify that critical infrastructure is not connected to or located on any of those predefined circuits. This review should be considered for evaluation at least annually. The best practice in this area is to try and and ensure that these facilities are not included in the initial under frequency or manual load shedding protocols at the outset. In the event that critical gas system components are subject to load shedding, or even uncontrolled loss of load, consideration should be given to the priority or restoration in the restoration plan for that equipment. Fuel delivery infrastructure restoration may be necessary to fully utilize all aspects of a full restoration plan.
  - In a similar manner, it may be appropriate to coordinate with secondary fuel (e.g., diesel or fuel oil, onsite LNG) suppliers to ensure that any necessary critical terminals, pump stations, and other critical components, identified by the owners and/or operators, are not subject to electric utility load shedding programs in general and more specifically Under Frequency and or Manual Load shedding programs. This is especially appropriate if adequate on-site fuel reserves are not guaranteed and just-in-time fuel delivery practices are required.

- Operating Reserves
  - The electric industry may want to consider adjustments to operating reserve or capacity requirements to better reflect the increased reliance on natural gas for the generation fleet. For instance, if the loss of a fuel forwarding facility has the ability to result in an instantaneous or near instantaneous electric energy loss, that contingency should be reflected in the reserve or

capacity procurement for the operating day. In addition, some electric operators are considering the implementation of a risk-based operating reserve protocol that increases or decreases the amount of operating reserve procured based upon the risks identified to both the gas and electric system.

B. Preparation, Supply Rights, Training and Testing

- Assessments
- Preparing the gas and electric system for coordinated operations benefits from up front assessments and activities to ensure that when real-time events occur, the system operators are prepared for them and can effectively react. Preparation activities that may be considered include the following:
    - Developing a detailed understanding of where and how the gas infrastructure interfaces with the electric industry including:
        - Identifying each pipeline (interstate and intrastate) that operates within the electric footprint and mapping the associated electric resources that are dependent upon those pipelines.
        - Identifying the level and quantity of pipeline capacity service (firm or interruptible; primary/secondary) and any additional pipeline services (storage, no-notice, etc.) being utilized by each gas-fired generator.
        - Developing a model of and understanding the non-electric generation load that those pipelines and LDCs serve and will protect when gas curtailments are needed.
        - Identifying gas single element contingencies (i.e. single points of disruption) and how those contingencies will impact the electric infrastructure. For instance, although most gas side contingencies will not impact the electric grid instantaneously, they can be far more severe than electric side contingencies over time because gas side contingencies may impact several generation facilities. When identifying gas system contingencies, the electric entity should consider what the gas operator will do to secure its firm customers. This could include the potential that the gas system will invoke mutual aid agreements with other interconnected pipelines and this may involve curtailment of non-firm electrical generation from the non-impacted pipeline to aid the other.
        - Understanding how gas contingencies may interact with electric contingencies during a system restoration effort.
- Emergency Procedure Testing and Training
    - Consider the development of testing and training activities to recognize abnormal gas system operating conditions and to support extreme gas contingencies such as loss of compressor stations, pipelines, pipeline interconnections, large LNG facilities, which can result in multiple generator losses over time. When possible, training should include lessons learned from past events such as actual pipeline disruptions or compressor station lightning strikes. Particular

attention should be focused on any gas related contingency that may result in an instantaneous generation loss.

- Consider the addition of electric and natural gas coordination and interdependencies training to educate and exercise RCs, BAs, TOPs, GOs, and GOPs during potentially adverse natural gas supply disruptions.
- If voltage reduction capability exists within your area, practical testing and training should be considered as part of seasonal or annual work plans.
- The use of manual firm load shedding may be required for beyond criteria extreme gas and or electric contingencies. Consideration should be given to practicing the use of manual load-shedding in a simulated environment. These simulations should also be used as part of recurring system operator training at a minimum. The use of tabletop exercises can be a valuable training aid, but wherever possible, consideration should be given to using an advanced training simulator that employs the same tools the operators would use to accomplish the load shedding tasks.
- Consider conducting periodic operational drills and tabletop exercises between ISO/RTO's, RCs, BAs, TOPs, GOs, GOPs, local emergency management entities, and the applicable natural gas industry providers (interstate and intrastate pipelines as well as local distribution companies that serve gas generators) where possible.
- Consider the development of and drill on internal communication protocols specific to potential natural gas interruptions.
- Consider the development of training programs for generator personnel on the typical form (electronic or telephonic), message and circumstances that characterize information exchange between natural gas pipeline operators and the generator. This training should detail the relevant information for normal operations as well as emergency situations.

- Generator Testing
  - Consideration should be given to adopting generator testing requirements for dual fuel auditing. Some items to consider when establishing a dual fuel audit program are:
    - How often should the audits be conducted and under what weather and temperature conditions.
    - Verify sufficient alternate fuel (e.g., fuel oil) inventory to ensure required generation response and output with seasonal (i.e. winter vs summer) consideration. As part of this assessment, ensure that the stored fuel is fully burnable as well since the full volume of the tank may not be pumpable at very low inventories.
    - Capacity, ramping capability or other reductions related to alternate fuels.
    - Understanding metrics such as the capability and expected time it takes to startup, switch to alternate fuel, ramp to and operate at full capacity, ramp down and resource shut down. Additional consideration should be given for those assets which require a shutdown in order to swap to an alternate fuel source..

- The operating entity should consider any environmental constraints the generator that is being tested must meet in order to swap to and operate on the alternate fuel.

- Capacity and Energy Assessments

  - Consideration should be given to the development of forward looking capacity analyses with which the electric industry is familiar but applying the impacts of fuel restrictions that may occur due to pipeline constraints or other fuel delivery constraints such as LNG shipments or liquid fuel delivery considerations. In order to conduct these types of assessments, the analysis needs to consider the LDC loads within the Region, acknowledging the potential impact of LDC loads outside the Region. The weather component of the assessment should consider normal, and extreme conditions (i.e., Gas Design Day, which is the equivalent to the highest peak that the pipeline was designed for). This capacity assessment can be on several time horizons including; Real-time, Day Ahead, Month Ahead and Years into the future. These assessments should consider pipeline maintenance, known future outages, construction and expansion activities as well as all electric and gas industry considerations, such as potential or anticipated regulatory changes.

  - In addition to a capacity assessment that represents only a single point in time, consideration should be given to the development of a seasonal, annual or multiannual energy analysis that uses fuel delivery capability/limitations as a component. Such assessments can be scenario based, simulate varied weather conditions over the course of months, seasons and/or years, and consider the same elements as discussed in the capacity analysis. The output of the assessments should determine whether there is the potential for unserved energy and/or determine the ability to provide reserves over the period in question.

- Seasonal Readiness Reviews

  - Winter events, such as the 2014 Polar Vortex, have magnified the need to ensure that seasonal awareness and readiness training is completed within the electric industry including System Operators, Generator Operators and Transmission Operators. Seasonal readiness training for winter weather could include reviews and training associated with dual fuel testing, emergency capacity and energy plans, weather forecasts over the seasonal period, fuel survey protocols and fuel storage readiness. Other areas that require attention in winter readiness reviews include reviewing and setting specific operational expectations on communications protocols. Finallyany winter readiness seminars should include individual generator readiness, as outlined in the Reliability Guideline: Generating Unit Winter Weather Readiness Current Industry Practices – Version 3[1], such as ensuring adequate fuel arrangements are in place for unit availability, adequate freeze protection guidelines are in place, understanding access to primary and secondary fuels and testing to switch to alternate fuels, ensuring all environmental permitting is in place for the fuel options available to the asset, and making sure that the Balancing Authority and Transmission Operators are kept apprised of the unit availability. Many of the same benefits

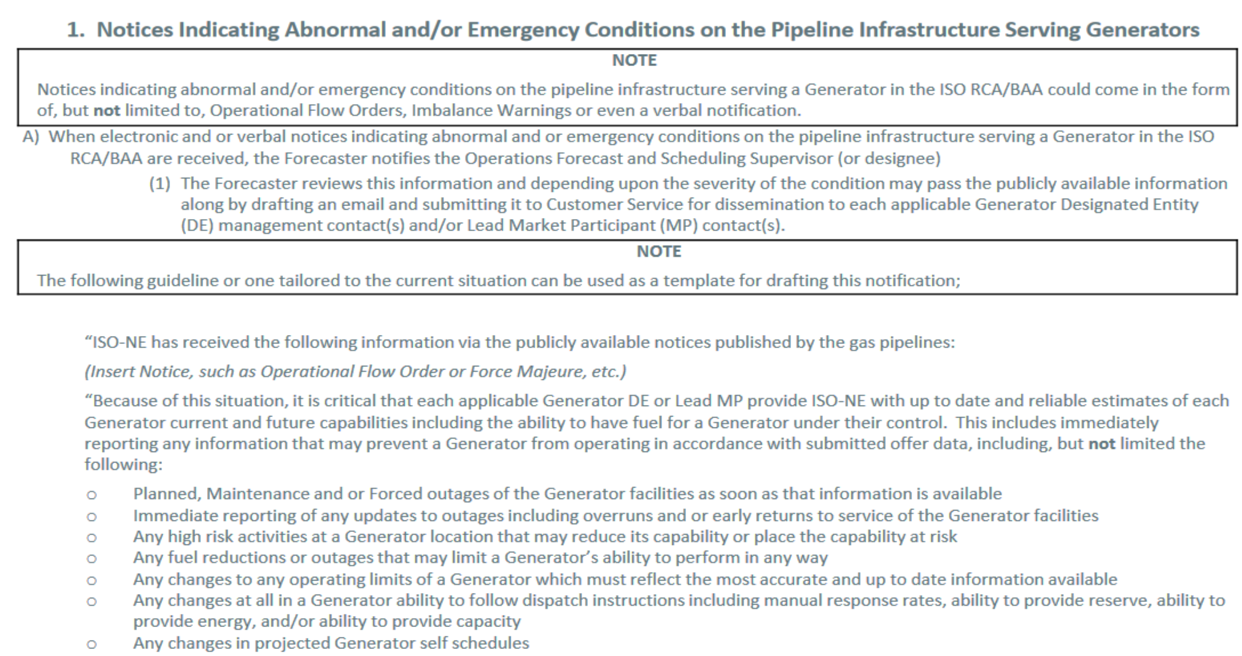
[1] https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Reliability_Guideline_Generating_Unit_Winter_Weather_Readiness_v3_Final.pdf

as winter readiness exercises can be realized with the added benefit of exercises under summer operating conditions when electric loads are higher than winter loads.

- Extreme Event Readiness Reviews
  - Seasonal readiness reviews for extreme events (e.g., hurricane, earthquakes, wildfires) could include response to potential natural gas supply limitations and corresponding decreases in natural gas deliveries that may impact electric generation.

C. Establish and Maintain Open Communication Channels

- Industry Coordination
  - In the long and short term planning horizons, regularly scheduled (e.g. monthly or quarterly, or at a frequency deemed effective as decided by the coordinating organizations) meetings between the gas and electric industries should be held to discuss upcoming operations including outage coordination, industry updates, project updates and exchange of contact information.
  - Operating entities should consider the development of a coordinated and annually updated set of operational and planning contact information for both the gas and electric industries. This information should include access to emergency phone numbers for management contacts as well as all control center real-time and forecaster desks for use in normal, and emergency conditions.
  - Gas and Electric emergency communication conference call capability should be considered between the industries such that operating personnel can be made available from both industries immediately, including off hours and within the confines of the individual confidentiality provisions of each entity. Electric sector personnel should periodically monitor pipeline posted information and notices.
  - In coordinating and modifying scheduling practices between gas and electric entities, the impact of the variability of intermittent resources should be considered in order to provide a more accurate assessment of available resources and to maintain bulk power system reliability.
- Emergency Notifications to Stakeholders
  - Operating Entities may want to consider proactive notifications to stakeholders of abnormal and or emergency conditions on gas infrastructure to ensure widespread situational awareness and obligations associated with dispatch relationships in the electric sector. An example of a notification used for generators in New England appears in Figure 1



1. **Notices Indicating Abnormal and/or Emergency Conditions on the Pipeline Infrastructure Serving Generators**

NOTE

Notices indicating abnormal and/or emergency conditions on the pipeline infrastructure serving a Generator in the ISO RCA/BAA could come in the form of, but **not** limited to, Operational Flow Orders, Imbalance Warnings or even a verbal notification.

A) When electronic and or verbal notices indicating abnormal and or emergency conditions on the pipeline infrastructure serving a Generator in the ISO RCA/BAA are received, the Forecaster notifies the Operations Forecast and Scheduling Supervisor (or designee)

(1) The Forecaster reviews this information and depending upon the severity of the condition may pass the publicly available information along by drafting an email and submitting it to Customer Service for dissemination to each applicable Generator Designated Entity (DE) management contact(s) and/or Lead Market Participant (MP) contact(s).

NOTE

The following guideline or one tailored to the current situation can be used as a template for drafting this notification;

"ISO-NE has received the following information via the publicly available notices published by the gas pipelines:

(Insert Notice, such as Operational Flow Order or Force Majeure, etc.)

"Because of this situation, it is critical that each applicable Generator DE or Lead MP provide ISO-NE with up to date and reliable estimates of each Generator current and future capabilities including the ability to have fuel for a Generator under their control. This includes immediately reporting any information that may prevent a Generator from operating in accordance with submitted offer data, including, but **not** limited the following:

- Planned, Maintenance and or Forced outages of the Generator facilities as soon as that information is available
- Immediate reporting of any updates to outages including overruns and or early returns to service of the Generator facilities
- Any high risk activities at a Generator location that may reduce its capability or place the capability at risk
- Any fuel reductions or outages that may limit a Generator's ability to perform in any way
- Any changes to any operating limits of a Generator which must reflect the most accurate and up to date information available
- Any changes at all in a Generator ability to follow dispatch instructions including manual response rates, ability to provide reserve, ability to provide energy, and/or ability to provide capacity
- Any changes in projected Generator self schedules

Figure 1: Example of New England Emergency Notifiction

Depending upon the level of severity and risk exposure, these written notifications and a means to communicate them may need to be followed up with direct verbal communications.

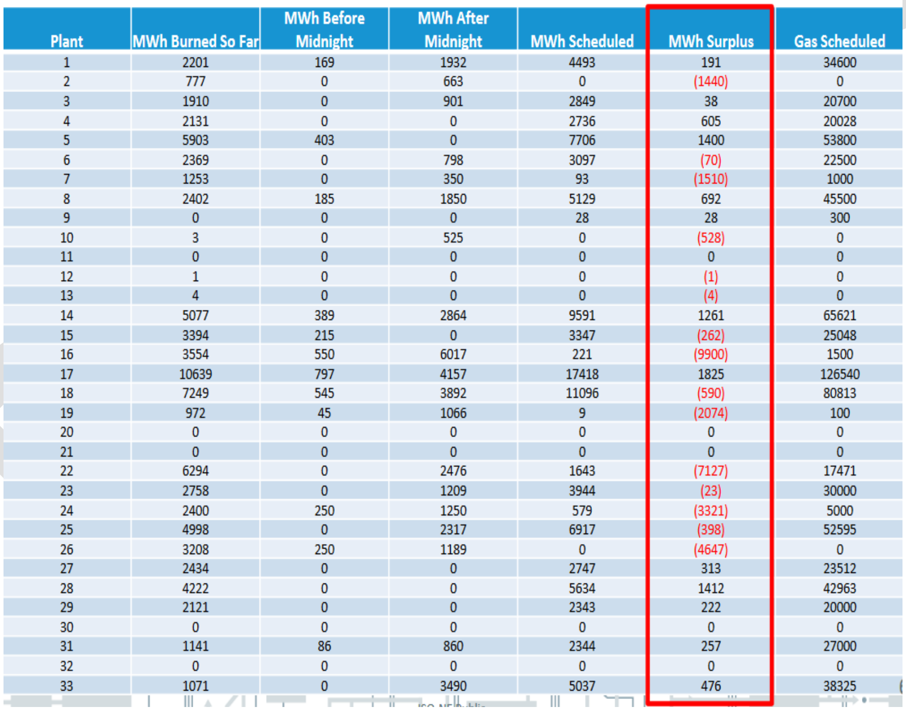
- Emergency Communication Protocols in the Public and Regulatory Community
  - Most every electric operating entity has long standing capacity and energy emergency plans in place that focus on public awareness, and emergency communications as well as appeals for conservation and load management. However, as the gas and electric industry become further dependent, considerations should be made for both industries to coordinate for extreme circumstances. Gas and electric operators in coordination with public officials, including relevant regulatory communities, may find situations where the energy of both the gas and electric sector is required to be reduced in order to preserve the reliability of both. While these types of efforts are still in their infancy they should be explored depending upon the particular circumstances of each entity's Region.

D. Gathering, Sharing Information, and Situational Awareness

- Fuel Surveys and Energy Emergency Protocols
  - Energy emergency procedures and fuel surveys are important tools in understanding the energy situation in a Region. The surveys can be used to determine energy adequacy for the region's electric power needs and for the communications and associated actions in anticipation or

declaration of an energy emergency[2]. The fuel surveys[3][4] should focus on the availability of other types of fuels if the gas infrastructure is the constrained resource.

- Fuel Procurement
  - Operating entities should consider evaluating each electric generator's natural gas procurement and commitment to determine fuel security for the operating day.
    - The electric operating entity can collect publicly available interstate pipeline bulletin board data and compare the gas schedules for individual generators against the expected electric operations of the same facility in the current or next day's operating plan. An example of this type of data collection appears in Figure 2 with the data helping to determine if enough fuel is available to meet an individual plant or in aggregate an entire gas fleet's expected operation for the current or future day. The report can indicate whether a fuel surplus or deficit exists by asset or for an entire pipeline. If sufficient gas has not been nominated and scheduled to the generator meter, assessments can be done to determine the impact on system operations and the operating staff may call the generator to inquire as to whether the intention is to secure the requisite gas supply to match its expected dispatch plus operating reserve designations.



Plant	MWh Burned So Far	MWh Before Midnight	MWh After Midnight	MWh Scheduled	MWh Surplus	Gas Scheduled
1	2201	169	1932	4493	191	34600
2	777	0	663	0	(1440)	0
3	1910	0	901	2849	38	20700
4	2131	0	0	2736	605	20028
5	5903	403	0	7706	1400	53800
6	2369	0	798	3097	(70)	22500
7	1253	0	350	93	(1510)	1000
8	2402	185	1850	5129	692	45500
9	0	0	0	28	28	300
10	3	0	525	0	(528)	0
11	0	0	0	0	0	0
12	1	0	0	0	(1)	0
13	4	0	0	0	(4)	0
14	5077	389	2864	9591	1261	65621
15	3394	215	0	3347	(262)	25048
16	3554	550	6017	221	(9900)	1500
17	10639	797	4157	17418	1825	126540
18	7249	545	3892	11096	(590)	80813
19	972	45	1066	9	(2074)	100
20	0	0	0	0	0	0
21	0	0	0	0	0	0
22	6294	0	2476	1643	(7127)	17471
23	2758	0	1209	3944	(23)	30000
24	2400	250	1250	579	(3321)	5000
25	4998	0	2317	6917	(398)	52595
26	3208	250	1189	0	(4647)	0
27	2434	0	0	2747	313	23512
28	4222	0	0	5634	1412	42963
29	2121	0	0	2343	222	20000
30	0	0	0	0	0	0
31	1141	86	860	2344	257	27000
32	0	0	0	0	0	0
33	1071	0	3490	5037	476	38325

Figure 2: Interstate Pipeline Bulletin Board Data Collection

[2] Energy emergency example: https://www.iso-ne.com/static-assets/documents/rules_proceds/operating/isone/op21/op21_rto_final.pdf

[3] Seasonal survey example – See section 7.3.5 in Manual 14 http://www.pjm.com/~/media/documents/manuals/m14d.ashx

[4] Real-time survey example – See section 6.4 of Manual 13 http://www.pjm.com/~/media/documents/manuals/m13.ashx

Varying configurations of generator gas supplies can quickly complicate reports. Efforts should be made prior to the development of such reporting tools to ensure that all facets of gas scheduling can be displayed. Not all scheduled gas data will be publically available, especially when dealing with LDC and intrastate-connected generators. Generators are occasionally supplied by multiple interstate pipelines simultaneously and may change supply sources based on daily natural gas prices. If possible, the electric operating entity should list its range of contractual arrangements with the natural gas sector such as firm capacity and supply, no-notice storage, etc.

- Gas System Visualization
  - Several Reliability Coordinators have developed visualization tools to provide scheduling and real-time operations staff with situational awareness that ties the gas and electric infrastructure together at their common point of operation. What follows in **Figure 3** is an example of one such tool that has been made generic for the purposes of the illustration. The bubbles in the tool indicate the functionality available to the user with notes that follow.

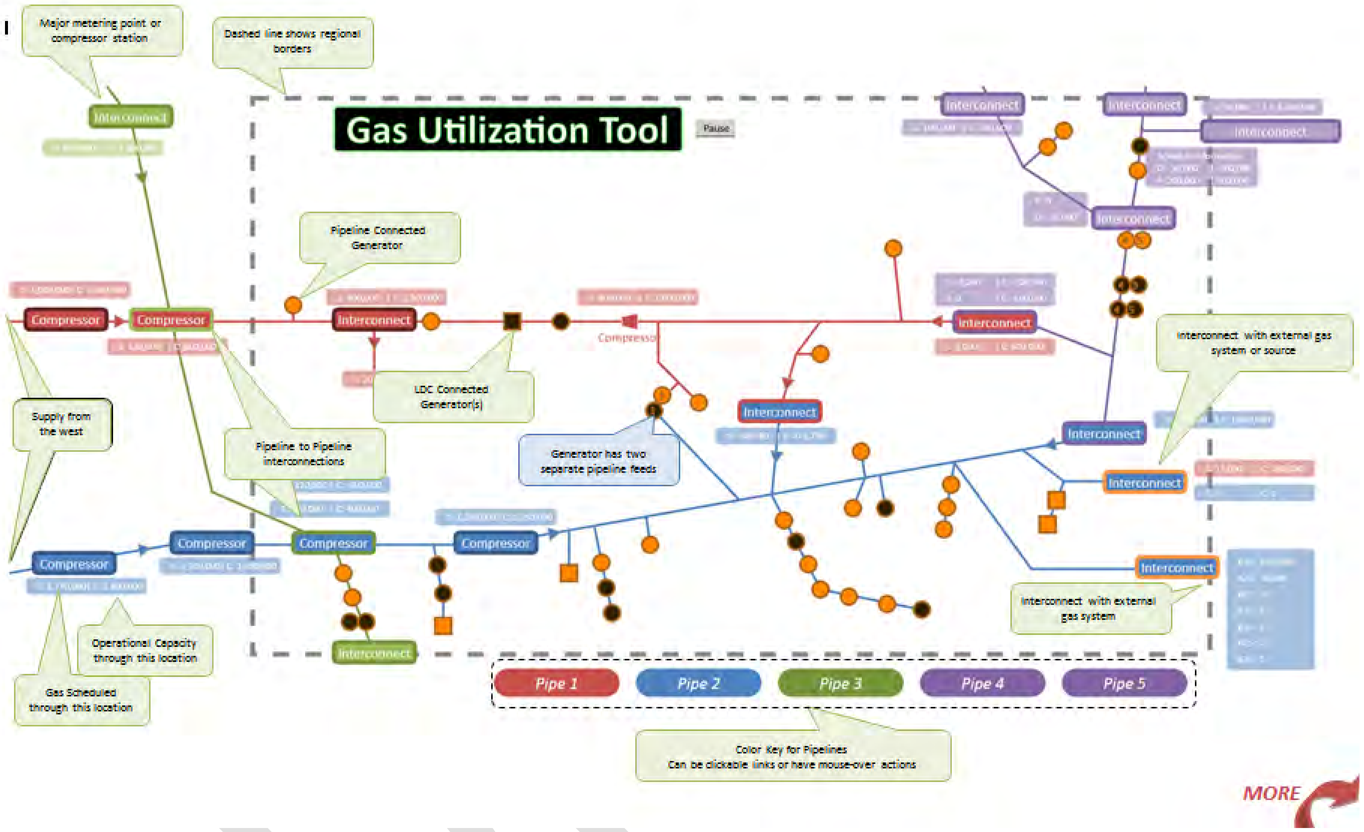
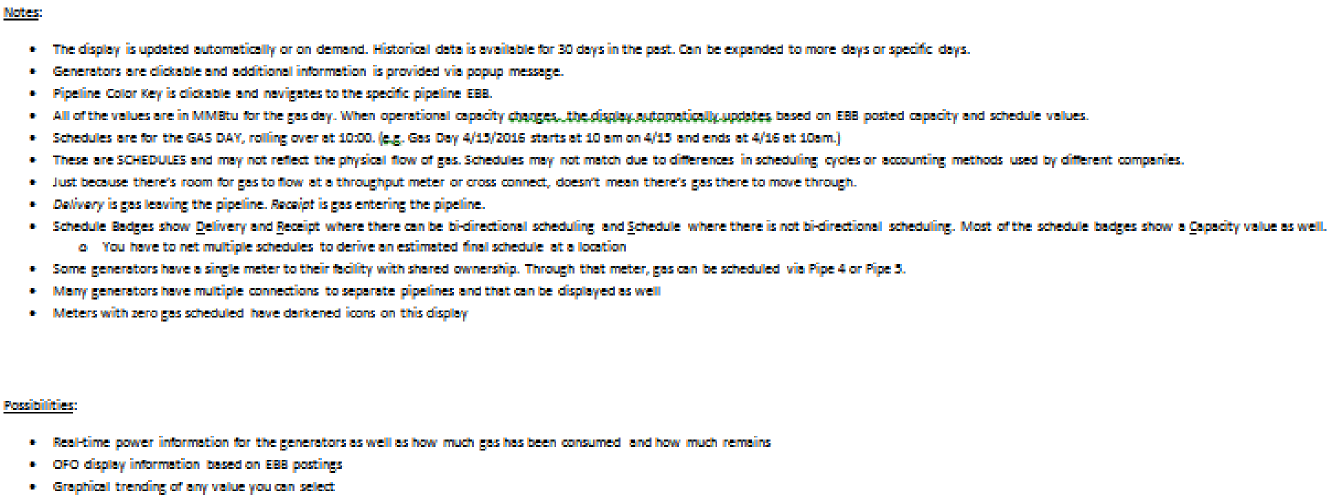

Major metering point or compressor station
Dashed line shows regional borders
Gas Utilization Tool
Pause
Interconnect
Compressor
Pipeline Connected Generator
LDC Connected Generator(s)
Generator has two separate pipeline feeds
Supply from the west
Pipeline to Pipeline interconnections
Interconnect with external gas system or source
Interconnect with external gas system
Operational Capacity through this location
Gas Scheduled through this location
Pipe 1
Pipe 2
Pipe 3
Pipe 4
Pipe 5
Color Key for Pipelines Can be clickable links or have mouse-over actions
MORE

Figure 3: Gas System Visualization



Notes:

- The display is updated automatically or on demand. Historical data is available for 30 days in the past. Can be expanded to more days or specific days.
- Generators are clickable and additional information is provided via popup message.
- Pipeline Color Key is clickable and navigates to the specific pipeline EBB.
- All of the values are in MMBtu for the gas day. When operational capacity changes, the display automatically updates based on EBB posted capacity and schedule values.
- Schedules are for the GAS DAY, rolling over at 10:00. (e.g. Gas Day 4/13/2016 starts at 10 am on 4/15 and ends at 4/16 at 10am.)
- These are SCHEDULES and may not reflect the physical flow of gas. Schedules may not match due to differences in scheduling cycles or accounting methods used by different companies.
- Just because there's room for gas to flow at a throughput meter or cross connect, doesn't mean there's gas there to move through.
- *Delivery* is gas leaving the pipeline. *Receipt* is gas entering the pipeline.
- Schedule Badges show Delivery and Receipt where there can be bi-directional scheduling and Schedule where there is not bi-directional scheduling. Most of the schedule badges show a Capacity value as well.
  - You have to net multiple schedules to derive an estimated final schedule at a location
- Some generators have a single meter to their facility with shared ownership. Through that meter, gas can be scheduled via Pipe 4 or Pipe 5.
- Many generators have multiple connections to seperate pipelines and that can be displayed as well
- Meters with zero gas scheduled have darkened icons on this display

Possibilities:

- Real-time power information for the generators as well as how much gas has been consumed and how much remains
- OFO display information based on EBB postings
- Graphical trending of any value you can select

E. Summary

The transformation in the mix of fuel sources used to power electric generation throughout North America and in particular, the increased penetration of renewable resources, as well as the continued increase in the use of natural gas highlights the continued need for the coordination processes discussed in this guideline. This guideline should serve as a reference document that NERC functional entities may use as needed to improve and ensure BES reliability and is based upon actual lessons learned over the last several years as natural gas has developed into the fuel of choice due to its availability and economic competitiveness. The document focuses on the areas of preparation, coordination, communication, and intelligence that may be applied to improve gas and electric coordinated operations and minimize interdependent risks. Each entity should assess the risks associated with this transformation and apply a set of appropriate processes and practices across its system to mitigate those risks. The guidance is not a "one size fits all" set of measures but rather a list of principles and strategies that can be applied according to the circumstances encountered in a particular system, Balancing Authority, generator fleet or even an individual Generator Operator.

F. Contributors

This Reliability Guideline was originally published in December, 2017. The final revised product, from a full review of industry feedback, was completed in 2021 as planned by the RSTC. This work was a collaboration by the members of the NERC Electric Gas Working Group and the NERC Real Time Operating Subcommittee.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Draft Reliability Guideline

Gas and Electrical Operational Coordination Considerations

Applicability:

Reliability Coordinators (RCs), Balancing Authorities (BAs), Transmission Operators (TOPs) Generator Owners (GOs), and Generator Operators (GOPs)

Preamble

It is in the public interest for the North American Electric Reliability Corporation (NERC) to develop guidelines that are useful for maintaining or enhancing the reliability of the Bulk Electric System (BES). The ~~Technical Committees of NERC- the~~ Reliability and Security Technical Committee (RSTC)~~Operating Committee (OC), the Planning Committee (PC) and the Critical Infrastructure Protection Committee (CIPC) –~~ are, per their charter~~s~~ authorized by the NERC Board of Trustees to develop Reliability ~~(OC and PC)~~ and Security ~~(CIPC)~~ Guidelines. Guidelines establish voluntary codes of practice for consideration and use by BES users, owners, and operators. These guidelines are developed by the technical committees and include the collective experience, expertise and judgment of the industry. Reliability guidelines do not provide binding norms or create parameters by which compliance to standards is monitored or enforced. While the incorporation and use of guideline practices is strictly voluntary, the review, revision, and development of a program using these practices is strongly encouraged to promote and achieve the highest levels of reliability for the BES. Nothing in this guideline negates obligations or requirements under an entity's regulatory framework (local, state or federal) and all parties must take those requirements into consideration when implementing any of the guidance detailed herein.

Metrics

Formatted: Heading 1, Left

Pursuant to the Commission's Order on January 19, 2021, *North American Electric Reliability Corporation*, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review consistent with the RSTC Charter.

Formatted: Justified

Baseline Metrics

- Performance of the BPS prior to and after a Reliability Guideline, as reflected in NERC's State of Reliability Report and Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments);
- Use and effectiveness of a Reliability Guideline as reported by industry via survey; and
- Industry assessment of the extent to which a Reliability Guideline is addressing risk as reported via survey.

Formatted: Justified

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure and evaluate its effectiveness.

- No additional metrics

Formatted: Normal

Background and Purpose

Coordination of operations between the gas and electric industries has become increasingly important over the course of the last decade. The electric power sector's use of gas, specifically natural gas-fired generation, has grown exponentially in many areas of North America due to increased availability of gas, potentially more competitive costs in relation to other fuels and a move throughout the industry to lower emissions to meet environmental goals. With increased growth in gas usage comes greater reliance and associated risk due to the dependency that each industry now has on the other. The operational impact of these dependencies requires gas and electric system operators to actively coordinate planning and operations. The goal of the coordination is to ensure that both the gas and electric systems remain secure and reliable during normal, and emergency conditions. This guideline attempts to provide a set of principles and strategies that may be adopted should the ~~region~~ Region in which you operate require close coordination due to increased dependency. This guideline does not apply universally, and an evaluation of your area's unique needs is essential to determine which principles and strategies you apply. The guideline principles and strategies may be applied by RCs, BAs, TOPs, GOs and GOPs in order to ensure reliable coordination with the gas industry. Finally, the document focuses on the areas of preparation, coordination, communication and gathering ~~&~~ and sharing information that may be applied in order to coordinate gas-electric utility operations and minimize reliability-related risk.

Guideline Content:

A. Establish Gas and Electric Industry Coordination Mechanisms

B. Preparation, Supply Rights, Training and Testing

C. Establish and Maintain Open Communication Channels

D. Gathering, Sharing Information and Situational Awareness

E. Summary

A. Establish Gas and Electric Industry Coordination Mechanisms

- Establish Contacts
  - An essential part of any coordination activity is the identification of participants. For gas and electric coordination, this could involve the identification of the natural gas interstate/intrastate pipelines, gas suppliers and Local Distribution Companies (LDC) as well as gas industry operations staff within the electric footprint boundaries and in some instances beyond those boundaries. Once contacts among these participants are established, additional coordination activities can begin. Gas industry trade organizations, such as the Interstate Natural Gas Association of America, Natural Gas Supply Association, American Gas Association or a regional entity such as the Northeast Gas Association may be able to aid in development of operational contacts and the establishment of coordination protocols. These contacts should be developed for long and short term planning/outage coordination as well as near term and real-time operations at a

variety of organizations including, but not limited to, Reliability Coordinators, Balancing Authority Operators, Transmission Operators, Generator Operators, and Gas Control Operators. The contacts should include both control room operating staff contacts as well as management. Establishing and maintaining these contacts is the most important aspect of gas and electric coordination. However, communications should be established during normal operations, so that the first call you make to a gas transmission pipeline or LDC should not be under emergency conditions.~~Past lessons learned have taught the industry that the first call you make to a gas transmission pipeline or LDC should not be during emergency conditions.~~

- Communication Protocols
  - Once counterparts are identified in the gas industry, communications protocols will need to be established within the regulatory framework of both energy sectors looking to coordinate and share information. The Federal Energy Regulatory Commission issued a Final Rule under Order No. 787 allowing interstate natural gas pipelines and electric transmission operators to share non-public operational information to promote the reliability and integrity of their systems. Since the inception of this rule and the subsequent incorporation of those rules into the associated tariffs, followed by the appropriate confidentiality agreements, gas and electric entities have been able to freely share operational data. Data that could be shared to improve operational coordination may include but is not necessarily limited to the following:
    - Providing detailed operational reports to the gas pipeline operators by specific generating assets, operating on specific pipelines, which specify expected fuel burn by asset, by hour over the dispatch period under review. It is important to convert dispatch plans from electric power (MWh) to gas demand (in terms of gas units/time such as dekatherms/day or MMcf/hour) when conveying that information to gas system operators.
    - Combining the expected fuel to be used by asset on each pipeline in aggregate to provide an expected draw on the pipeline by generation connected to that pipeline on an hourly basis and on a gas and electric day basis.
  - Exchanging real-time operating information in both verbal and electronic forms (e.g., pipeline company informational postings) of actual operating conditions on specific assets on specific pipelines. Also consider the electronic communication of real-time system information between affected parties, such as real-time gas meter readings and generator dispatch instructions.
  - Outage planning for elements of significance to include sharing detailed electric and gas asset scheduling information on all time horizons and coordinating outages of those assets to ensure reliability on both the gas and electric systems. Examples include, but are not limited to, must-run requirements, inline inspection operations, risk of disruption to electric compression, and pipeline outages potentially causing the need for pressure reductions.
  - Scheduling ~~face-to-face~~ coordination meetings, face-to-face whenever possible, on a periodic basis (e.g.annual, bi-annual, quarterly, etc…) to discuss a range of topics including but not limited to outage coordination, proposed electric/gas market rule changes, upcoming gas generator additions, pending electric retirements/repowers, enhancements/modifications to gas/electric

coordination tools, gas pipeline infrastructure changes, near/long-term seasonal forecasts and load shape changes.

- Sharing normal~~,~~ and emergency conditions in real-time and ensuring each entity understands the implications to their respective systems. This should include gas and electric entities proactively reaching out to the operators of stressed gas systems to discuss the impacts, adverse or otherwise, of their expected or available actions. Under~~ extreme gas system operating conditions, under~~stand the direct impacts to electric generation assets when gas pipelines are directed under more extreme gas system operating conditions and/or force majeure conditions.

- The sharing of non-public operating information between the electric operating entity and LDC, intrastate pipelines, and gathering pipelines is not covered under FERC Order 787. For this reason, individual communication and coordination protocols should be considered with each LDC and intrastate pipelines within the footprint of the operating entity. These protocols might be set up to specifically allow gas dispatchers or dispatch departments at intrastate, LDC, and gathering pipelines to communicate directly with generator operators.

  - ~~-~~Understanding the conditions under which an LDC or intrastate pipeline would interrupt gas-fired generation is of particular importance and incorporating this information into operational procedures and planning will assist in identification of potential at-risk generation.

Formatted: List Bullet 3

  - Setting up electronic/email alerts from each LDC or intrastate pipeline as to the potential declaration of interruptions is one key means of real time identification of potential loss of generation behind the LDC city gate or meter station on an intrastate pipeline.

- Addressing the identification of electricity source for electric compression stations and protocols for protecting these sources during periods of high demand or system stress with plans to mitigate such risk, when possible.

- Coordinating Procurement Time Lines

  - Operating entities may want to consider changing next day operating plan scheduling practices to align more efficiently with gas day procurement cycles. The gas and electric industries operate on differing timelines for the Day Ahead planning processes and in real-time, with the electric day on a local midnight to midnight cycle. The gas industry process operates on a differing timeline with the operating day beginning at 9 a.m. Central Clock Time and uniform throughout North America. This difference in operating days can lead to inefficient scheduling of natural gas to meet the electric day demands. In many instances throughout North America, the electric industry has moved the development and publishing of unit commitments and next day operating plans in order to ensure that generation resources have the ability to procure and nominate natural gas more efficiently to better meet the scheduling timelines of the gas industry. In addition, the gas industry has adjusted some of its nomination and scheduling practices to allow for more efficient scheduling that meets the needs of the electric system.

  - Coordinating and modifying scheduling practices using more effective time periods may allow for a higher level of pipeline utilization, but more importantly, may provide the early identification of constraints that could require starting gas generation with alternate fuels if available, or using non-gas-fired facilities for fuel diversity to meet the energy and reserve needs of the electric system. Recently, the fast-ramping capability of gas-fired units has been used some places to bolster grid flexibility in areas trending toward more renewable energy, primarily with variable and intermittent supplies of fuel (e.g. sunshine, wind, and water). Maintaining a balanced power system will require a more flexible approach to energy and capacity adequacy in order to sustain operational awareness.~~As the mix of resources trends toward more renewable energy, primarily with variable and intermittent supplies of fuel (e.g. sunshine, wind, and water), maintaining a balanced power system will require a more flexible approach to energy and capacity adequacy in order to maintain operational awareness.~~

- Identification of Critical Gas System Components and Dual-fuel Supplier Components
  - It is essential gas and electric operating entities coordinate to ensure that critical natural gas pipelines, compressor stations, LNG, and other gas storage, natural gas processing plants, and other critical gas system components, identified by the owners and/or operators, should not be subject to electric utility load shedding in general but more specifically Under Frequency and or Manual Load shedding programs.
    - Electric transmission and distribution owners are capable of interrupting electrical load either automatically through under frequency load shedding relays installed in substations throughout North America or via manual load shedding ordered by RCs, BAs and or TOPs via SCADA. These manual and automatic load shedding protocols are part of every entity's emergency procedures. Entities should try to ensure critical gas sector infrastructure is not located on electrical circuits that are subject to the load shedding as described above. Electric operators should establish contact with the gas companies operating within its jurisdiction to compile a list of critical gas and other fuel facilities which are dependent upon electric service for operations. This list should also consider the availability of backup generation at critical gas facilities. Once the list is compiled, a comprehensive review of load shedding procedures/schemas/circuits should be done to verify that critical infrastructure is not connected to or located on any of those predefined circuits. This review should be considered for evaluation at least annually. The best practice in this area is to try and ensure that these facilities are not included in the initial under frequency or manual load shedding protocols at the outset. In the event that critical gas system components are subject to load shedding, or even uncontrolled loss of load, consideration should be given to the priority or restoration in the restoration plan for that equipment. Fuel delivery infrastructure restoration may be necessary to fully utilize all aspects of a full restoration plan.
  - In a similar manner, it may be appropriate to coordinate with secondary fuel (e.g., diesel or fuel oil, onsite LNG) suppliers to ensure that any necessary critical terminals, pump stations, and other critical components, identified by the owners and/or operators, are not subject to electric utility load shedding programs in general and more specifically Under Frequency and or Manual Load shedding programs. This is especially appropriate if adequate on-site fuel reserves are not guaranteed and just-in-time fuel delivery practices are required.

- Operating Reserves
  - The electric industry may want to consider adjustments to operating reserve or capacity requirements to better reflect the increased reliance on natural gas for the generation fleet. For instance, if the loss of a fuel forwarding facility has the ability to result in an instantaneous or near instantaneous electric energy loss, that contingency should be reflected in the reserve or capacity procurement for the operating day. In addition, some electric operators are considering the implementation of a risk-based operating reserve protocol that increases or decreases the amount of operating reserve procured based upon the risks identified to both the gas and electric system.

B. Preparation, Supply Rights, Training and Testing

- Assessments
- Preparing the gas and electric system for coordinated operations benefits from up front assessments and activities to ensure that when real-time events occur, the system operators are prepared for them and can effectively react. ~~Preparing the gas and electric system for coordinated operations benefits from up front assessments and activities to ensure that when real-time events occur, the system operators are prepared for and can effectively react.~~ Preparation activities that may be considered include the following:
  - Developing a detailed understanding of where and how the gas infrastructure interfaces with the electric industry including:
    - Identifying each pipeline (interstate and intrastate) that operates within the electric footprint and mapping the associated electric resources that are dependent upon those pipelines.
    - Identifying the level and quantity of pipeline capacity service (firm or interruptible; primary/secondary) and any additional pipeline services (storage, no-notice, etc.) being utilized by each gas-fired generator.
    - Developing a model of and understanding the non-electric generation load that those pipelines and LDCs serve and will protect when gas curtailments are needed.
    - Identifying gas single element contingencies (i.e. single points of disruption) and how those contingencies will impact the electric infrastructure. For instance, although most gas side contingencies will not impact the electric grid instantaneously, they can be far more severe than electric side contingencies over time because gas side contingencies may impact several generation facilities. When identifying gas system contingencies, the electric entity should consider what the gas operator will do to secure its firm customers. This could include the potential that the gas system will invoke mutual aid agreements with other interconnected pipelines and this may involve curtailment of non-firm electrical generation from the non-impacted pipeline to aid the other.
    - Understanding how gas contingencies may interact with electric contingencies during a system restoration effort.

        - ~~An additional example of appropriate actions to consider as part of the assessment phase of preparation is provided as a Natural Gas Risk Matrix[1].~~

- Emergency Procedure Testing and Training
    - Consider the development of testing and training activities to recognize abnormal gas system operating conditions and to support extreme gas contingencies such as loss of compressor stations, pipelines, pipeline interconnections, large LNG facilities, which can result in multiple generator losses over time. When possible, training should include lessons learned from past events such as actual pipeline disruptions or compressor station lightning strikes. Particular attention should be focused on any gas related contingency that may result in an instantaneous generation loss.
    - Consider the addition of electric and natural gas coordination and interdependencies training to educate and exercise RCs, BAs, TOPs, GOs, and GOPs during potentially adverse natural gas supply disruptions.
    - If voltage reduction capability exists within your area, practical testing and training should be considered as part of seasonal or annual work plans.
    - The use of manual firm load shedding may be required for beyond criteria extreme gas and or electric contingencies. Consideration should be given to practicing the use of manual load-shedding in a simulated environment. These simulations should also be used as part of recurring system operator training at a minimum. The use of tabletop exercises can be a valuable training aid, but wherever possible, consideration should be given to using an advanced training simulator that employs the same tools the operators would use to accomplish the load shedding tasks.
    - Consider conducting periodic operational drills and tabletop exercises between ISO/RTO's, RCs, BAs, TOPs, GOs, GOPs, local emergency management entities, and the applicable natural gas industry providers (interstate and intrastate pipelines as well as local distribution companies that serve gas generators) where possible.
    - Consider the development of and drill on internal communication protocols specific to potential natural gas interruptions.
    - Consider the development of training programs for generator personnel on the typical form (electronic or telephonic), message and circumstances that characterize information exchange between natural gas pipeline operators and the generator. This training should detail the relevant information for normal operations as well as emergency situations.
- Generator Testing
    - Consideration should be given to adopting generator testing requirements for dual fuel auditing. Some items to consider when establishing a dual fuel audit program are:

[1] ~~https://www.misoenergy.org/StakeholderCenter/CommitteesWorkGroupsTaskForces/ENGCTF/Pages/home.aspx~~

  - How often should the audits be conducted and under what weather and temperature conditions.
  - Verify sufficient alternate fuel (e.g., fuel oil) inventory to ensure required generation response and output with seasonal (i.e. winter vs summer) consideration. As part of this assessment, ensure that the stored fuel is fully burnable as well since the full volume of the tank may not be pumpable at very low inventories.
  - Capacity, ramping capability or other reductions related to alternate fuels.
  - Understanding metrics such as the capability and expected time it takes to startup, switch to alternate fuel, ramp to and operate at full capacity, ramp down and resource shut down. Additional consideration should be given for those assets which require a shutdown in order to swap to an alternate fuel source.~~Understanding the exact time it takes to startup, switch to alternate fuel, ramp to and operate at full capacity, ramp down and resource shut down. Additional consideration should be given for those assets which require a shutdown in order to swap to an alternate fuel source~~.
  - The operating entity should consider any environmental constraints the generator ~~under test~~that is being tested must meet in order to swap to and operate on the alternate fuel.

- Capacity and Energy Assessments
  - Consideration should be given to the development of forward looking capacity analyses with which the electric industry is familiar but applying the impacts of fuel restrictions that may occur due to pipeline constraints or other fuel delivery constraints such as LNG shipments or liquid fuel delivery considerations. In order to conduct these types of assessments, the analysis needs to consider the LDC loads within the R~~r~~egion, acknowledging the potential impact of LDC loads outside the Region. The weather component of the assessment should consider normal, and extreme conditions (i.e., Gas Design Day, which is the equivalent to the highest peak that the pipeline was designed for). This capacity assessment can be on several time horizons including; Real-time, Day Ahead, Month Ahead and Years into the future. These assessments should consider pipeline maintenance, known future outages, construction and expansion activities as well as all electric and gas industry considerations, such as potential or anticipated regulatory changes.
  - In addition to a capacity assessment that represents only a single point in time, consideration should be given to the development of a seasonal, annual or multiannual energy analysis that uses fuel delivery capability/limitations as a component. Such assessments can be scenario based, simulate varied weather conditions over the course of months, seasons and/or years, and consider the same elements as discussed in the capacity analysis. The output of the assessments should determine whether there is the potential for unserved energy and/or determine the ability to provide reserves over the period in question.
- Seasonal Readiness Reviews

  Winter events, such as the 2014 Polar Vortex, have magnified the need to ensure that seasonal awareness and readiness training is completed within the electric industry including System

Operators, Generator Operators and Transmission Operators. Seasonal readiness training for winter weather could include reviews and training associated with dual fuel testing, emergency capacity and energy plans, weather forecasts over the seasonal period, fuel survey protocols and fuel storage readiness. Other areas that require attention in winter readiness reviews include reviewing and setting specific operational expectations on communications protocols. Finally~~,~~ any winter readiness seminars should include individual generator readiness, as outlined in the Reliability Guideline: Generating Unit Winter Weather Readiness Current Industry Practices – Version 3[2], such as ensuring adequate fuel arrangements are in place for unit availability, adequate freeze protection guidelines are in place, understanding access to primary and secondary fuels and testing to switch to alternate fuels, ensuring all environmental permitting is in place for the fuel options available to the asset, and making sure that the Balancing Authority and Transmission Operators are kept apprised of the unit availability. Many of the same benefits as winter readiness exercises can be realized with the added benefit of exercises under summer operating conditions when electric loads are higher than winter loads.

Formatted: Outline numbered + Level: 2 + Numbering Style: Bullet + Aligned at: 0.5" + Indent at: 0.75"

- Extreme Event Readiness Reviews
  - Seasonal readiness reviews for extreme events (e.g., hurricane, earthquakes, wildfires) could include response to potential natural gas supply limitations and corresponding decreases in natural gas deliveries that may impact electric generation.

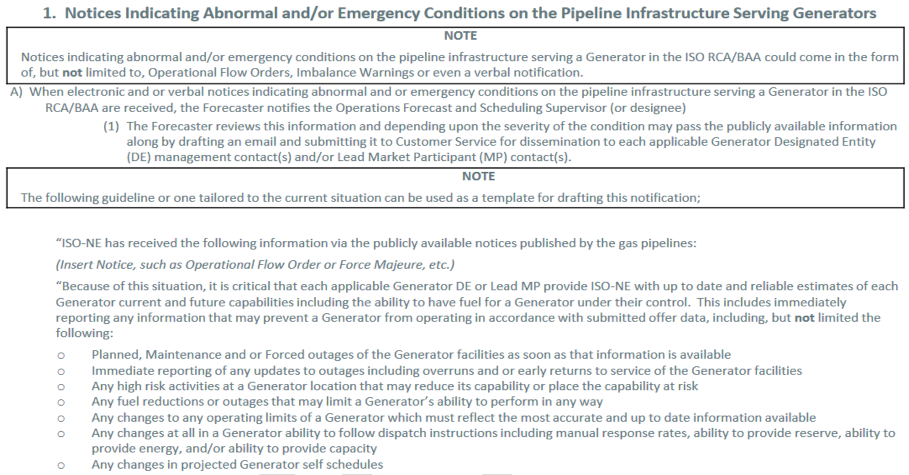
C. Establish and Maintain Open Communication Channels

- Industry Coordination
  - In the long and short term planning horizons, regularly scheduled (e.g. monthly or quarterly, or at a frequency deemed effective as decided by the coordinating organizations) meetings between the gas and electric industries should be held to discuss upcoming operations including outage coordination, industry updates, project updates and exchange of contact information.
  - Operating entities should consider the development of a coordinated and annually updated set of operational and planning contact information for both the gas and electric industries. This information should include access to emergency phone numbers for management contacts as well as all control center real-time and forecaster desks for use in normal, and emergency conditions.
  - Gas and Electric emergency communication conference call capability should be considered between the industries such that operating personnel can be made available from both industries immediately, including off hours and within the confines of the individual confidentiality provisions of each entity. Electric sector personnel should periodically monitor pipeline posted information and notices.

[2] https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Reliability_Guideline_Generating_Unit_Winter_Weather_Readiness_v3_Final.pdf

  - In coordinating and modifying scheduling practices between gas and electric entities, the impact of the variability of intermittent resources should be considered in order to provide a more accurate assessment of available resources and to maintain bulk power system reliability.

- Emergency Notifications to Stakeholders
  - Operating Entities may want to consider proactive notifications to stakeholders of abnormal and or emergency conditions on gas infrastructure to ensure widespread situational awareness and obligations associated with dispatch relationships in the electric sector. An example of a notification used for generators in New England appears in **Figure 1**



1. Notices Indicating Abnormal and/or Emergency Conditions on the Pipeline Infrastructure Serving Generators

NOTE

Notices indicating abnormal and/or emergency conditions on the pipeline infrastructure serving a Generator in the ISO RCA/BAA could come in the form of, but **not** limited to, Operational Flow Orders, Imbalance Warnings or even a verbal notification.

A) When electronic and or verbal notices indicating abnormal and or emergency conditions on the pipeline infrastructure serving a Generator in the ISO RCA/BAA are received, the Forecaster notifies the Operations Forecast and Scheduling Supervisor (or designee)

(1) The Forecaster reviews this information and depending upon the severity of the condition may pass the publicly available information along by drafting an email and submitting it to Customer Service for dissemination to each applicable Generator Designated Entity (DE) management contact(s) and/or Lead Market Participant (MP) contact(s).

NOTE

The following guideline or one tailored to the current situation can be used as a template for drafting this notification;

"ISO-NE has received the following information via the publicly available notices published by the gas pipelines:

(Insert Notice, such as Operational Flow Order or Force Majeure, etc.)

"Because of this situation, it is critical that each applicable Generator DE or Lead MP provide ISO-NE with up to date and reliable estimates of each Generator current and future capabilities including the ability to have fuel for a Generator under their control. This includes immediately reporting any information that may prevent a Generator from operating in accordance with submitted offer data, including, but **not** limited the following:

- Planned, Maintenance and or Forced outages of the Generator facilities as soon as that information is available
- Immediate reporting of any updates to outages including overruns and or early returns to service of the Generator facilities
- Any high risk activities at a Generator location that may reduce its capability or place the capability at risk
- Any fuel reductions or outages that may limit a Generator's ability to perform in any way
- Any changes to any operating limits of a Generator which must reflect the most accurate and up to date information available
- Any changes at all in a Generator ability to follow dispatch instructions including manual response rates, ability to provide reserve, ability to provide energy, and/or ability to provide capacity
- Any changes in projected Generator self schedules

Figure 1: Example of New England Emergency Notifiction

Depending upon the level of severity and risk exposure, these written notifications and a means to communicate them may need to be followed up with direct verbal communications.

  - Emergency Communication Protocols in the Public and Regulatory Community
    - Most every electric operating entity has long standing capacity and energy emergency plans in place that focus on public awareness, and emergency communications as well as appeals for conservation and load management. However, as the gas and electric industry become further dependent, considerations should be made for both industries to coordinate for extreme circumstances. Gas and electric operators in coordination with public officials, including relevant regulatory communities, may find situations where the energy of both the gas and electric sector is required to be reduced in order to preserve the reliability of both. While these types of efforts are still in their infancy they should be explored depending upon the particular circumstances of each entity's ~~region~~Region.

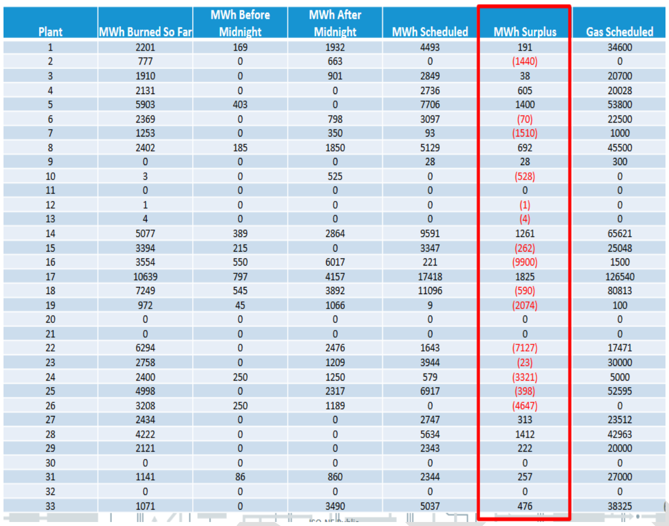
D. Gathering, Sharing Information, and Situational Awareness

Formatted: Font color: Blue

- Fuel Surveys and Energy Emergency Protocols
  - Energy emergency procedures and fuel surveys are important tools in understanding the energy situation in a ~~region~~Region. The surveys can be used to determine energy adequacy for the region's electric power needs and for the communications and associated actions in anticipation or declaration of an energy emergency[3]. The fuel surveys[4][5] should focus on the availability of other types of fuels if the gas infrastructure is the constrained resource.
- Fuel Procurement
  - Operating entities should consider evaluating each electric generator's natural gas procurement and commitment to determine fuel security for the operating day.
    - The electric operating entity can collect publicly available interstate pipeline bulletin board data and compare the gas schedules for individual generators against the expected electric operations of the same facility in the current or next day's operating plan. An example of this type of data collection appears in **Figure 2** with the data helping to determine if enough fuel is available to meet an individual plant or in aggregate an entire gas fleet's expected operation for the current or future day. The report can indicate whether a fuel surplus or deficit exists by asset or for an entire pipeline. If sufficient gas has not been nominated and scheduled to the generator meter, assessments can be done to determine the impact on system operations and the operating staff may call the generator to inquire as to whether the intention is to secure the requisite gas supply to match its expected dispatch plus operating reserve designations.

Formatted: Font color: Blue

[3] Energy emergency example: https://www.iso-ne.com/static-assets/documents/rules_proceds/operating/isone/op21/op21_rto_final.pdf
[4] Seasonal survey example – See section 7.3.5 in Manual 14 http://www.pjm.com/~/media/documents/manuals/m14d.ashx
[5] Real-time survey example – See section 6.4 of Manual 13 http://www.pjm.com/~/media/documents/manuals/m13.ashx



Plant	MWh Burned So Far	MWh Before Midnight	MWh After Midnight	MWh Scheduled	MWh Surplus	Gas Scheduled
1	2201	169	1932	4493	191	34600
2	777	0	663	0	(1440)	0
3	1910	0	901	2849	38	20700
4	2131	0	0	2736	605	20028
5	5903	403	0	7706	1400	53800
6	2369	0	798	3097	(70)	22500
7	1253	0	350	93	(1510)	1000
8	2402	185	1850	5129	692	45500
9	0	0	0	28	28	300
10	3	0	525	0	(528)	0
11	0	0	0	0	0	0
12	1	0	0	0	(1)	0
13	4	0	0	0	(4)	0
14	5077	389	2864	9591	1261	65621
15	3394	215	0	3347	(262)	25048
16	3554	550	6017	221	(9900)	1500
17	10639	797	4157	17418	1825	126540
18	7249	545	3892	11096	(590)	80813
19	972	45	1066	9	(2074)	100
20	0	0	0	0	0	0
21	0	0	0	0	0	0
22	6294	0	2476	1643	(7127)	17471
23	2758	0	1209	3944	(23)	30000
24	2400	250	1250	579	(3321)	5000
25	4998	0	2317	6917	(398)	52595
26	3208	250	1189	0	(4647)	0
27	2434	0	0	2747	313	23512
28	4222	0	0	5634	1412	42963
29	2121	0	0	2343	222	20000
30	0	0	0	0	0	0
31	1141	86	860	2344	257	27000
32	0	0	0	0	0	0
33	1071	0	3490	5037	476	38325

Figure 2: Interstate Pipeline Bulletin Board Data Collection

Varying configurations of generator gas supplies can quickly complicate reports. Efforts should be made prior to the development of such reporting tools to ensure that all facets of gas scheduling can be displayed. Not all scheduled gas data will be publically available, especially when dealing with LDC and intrastate-connected generators. Generators are occasionally supplied by multiple interstate pipelines simultaneously and may change supply sources based on daily natural gas prices. If possible, the electric operating entity should list its range of contractual arrangements with the natural gas sector such as firm capacity and supply, no-notice storage, etc.

- Gas System Visualization
  - Several Reliability Coordinators have developed visualization tools to provide scheduling and real-time operations staff with situational awareness that ties the gas and electric infrastructure together at their common point of operation. What follows in **Figure 3** is an example of one such tool that has been made generic for the purposes of the illustration. The bubbles in the tool indicate the functionality available to the user with notes that follow.

Formatted: Font color: Blue

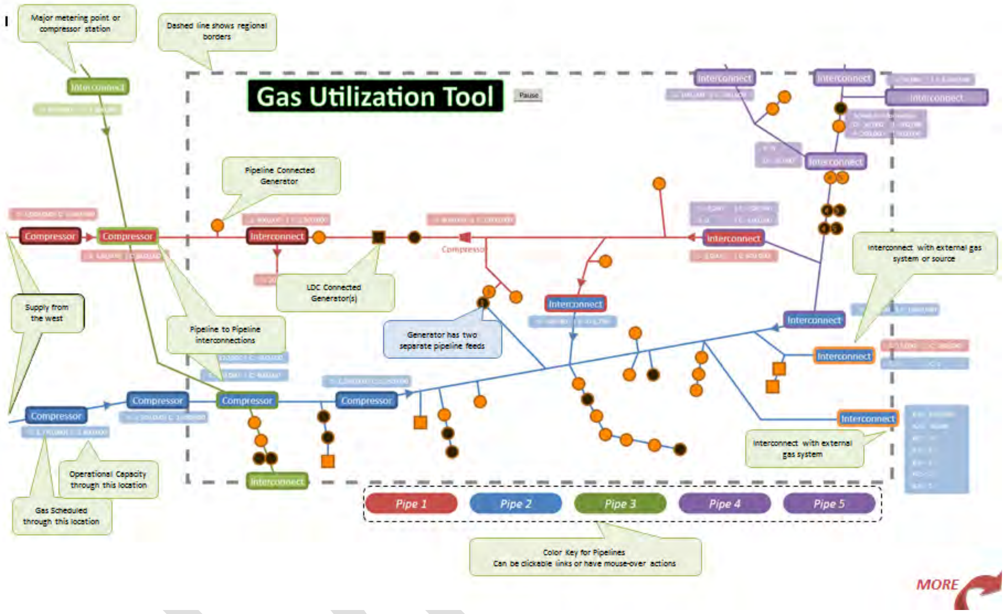
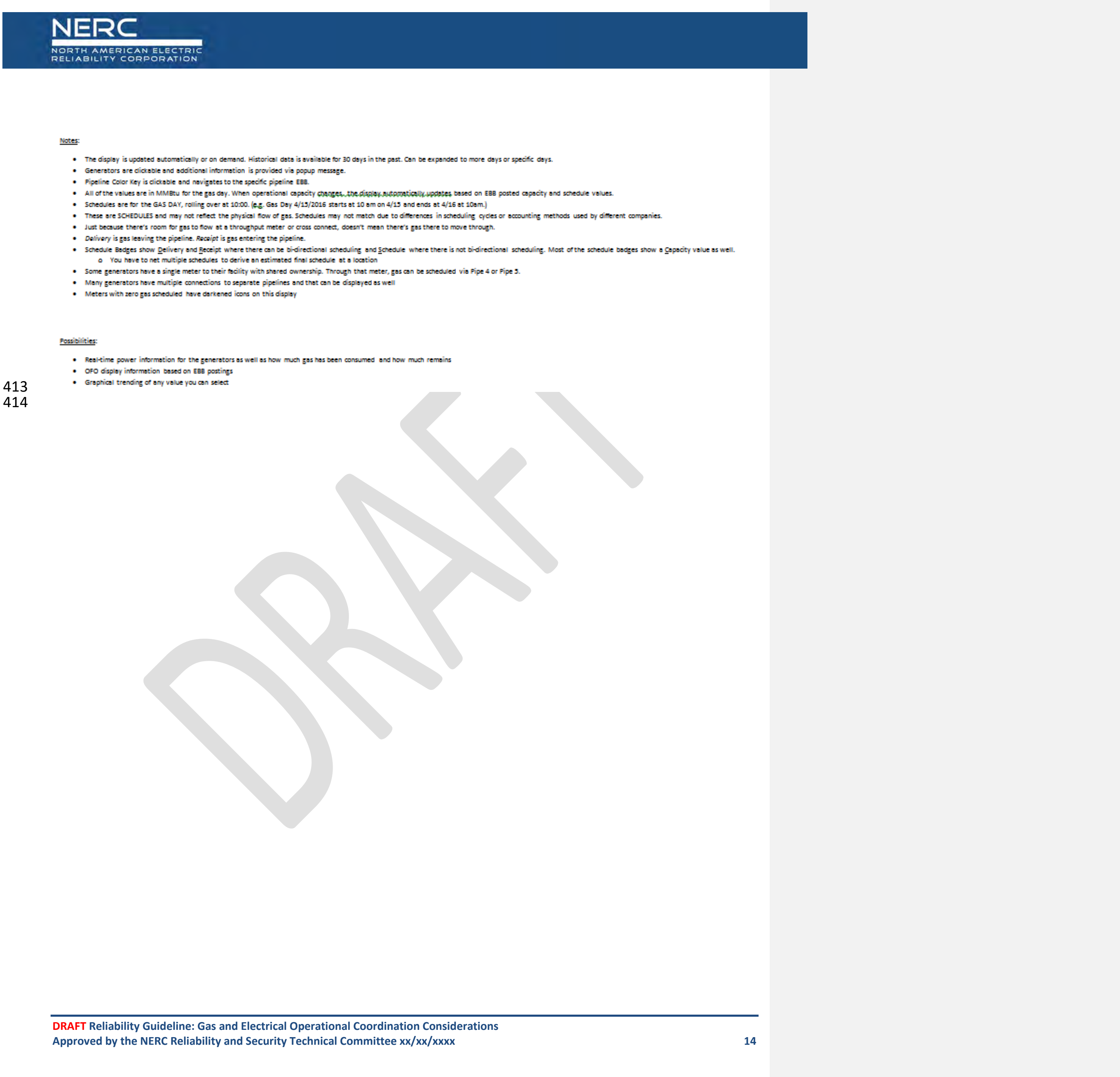

Major metering point or compressor station
Dashed line shows regional borders
Gas Utilization Tool
Pause
Interconnect
Pipeline Connected Generator
Compressor
Compressor
Interconnect
Compressor
LDC Connected Generator(s)
Supply from the west
Pipeline to Pipeline interconnections
Generator has two separate pipeline feeds
Interconnect
Interconnect
Interconnect
Interconnect
Interconnect
Interconnect
Interconnect with external gas system or source
Interconnect
Interconnect
Compressor
Compressor
Compressor
Compressor
Interconnect with external gas system
Interconnect
Operational Capacity through this location
Gas Scheduled through this location
Pipe 1
Pipe 2
Pipe 3
Pipe 4
Pipe 5
Color Key for Pipelines
Can be clickable links or have mouse-over actions
MORE

Figure 3: Gas System Visualization



Notes:

- The display is updated automatically or on demand. Historical data is available for 30 days in the past. Can be expanded to more days or specific days.
- Generators are clickable and additional information is provided via popup message.
- Pipeline Color Key is clickable and navigates to the specific pipeline EBB.
- All of the values are in MMBtu for the gas day. When operational capacity changes, the display automatically updates based on EBB posted capacity and schedule values.
- Schedules are for the GAS DAY, rolling over at 10:00. (e.g. Gas Day 4/15/2016 starts at 10 am on 4/15 and ends at 4/16 at 10am.)
- These are SCHEDULES and may not reflect the physical flow of gas. Schedules may not match due to differences in scheduling cycles or accounting methods used by different companies.
- Just because there's room for gas to flow at a throughput meter or cross connect, doesn't mean there's gas there to move through.
- *Delivery* is gas leaving the pipeline. *Receipt* is gas entering the pipeline.
- Schedule Badges show Delivery and Receipt where there can be bi-directional scheduling and Schedule where there is not bi-directional scheduling. Most of the schedule badges show a Capacity value as well.
    - You have to net multiple schedules to derive an estimated final schedule at a location
- Some generators have a single meter to their facility with shared ownership. Through that meter, gas can be scheduled via Pipe 4 or Pipe 5.
- Many generators have multiple connections to separate pipelines and that can be displayed as well
- Meters with zero gas scheduled have darkened icons on this display

Possibilities:

- Real-time power information for the generators as well as how much gas has been consumed and how much remains
- OFO display information based on EBB postings
- Graphical trending of any value you can select

~~A.~~E. Summary

Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 5 + Alignment: Left + Aligned at: 0" + Indent at: 0.25"

The transformation in the mix of fuel sources used to power electric generation throughout North America and in particular, the increased penetration of renewable resources, as well as the continued increase in the use of natural gas highlights the continued need for the coordination processes discussed in this guideline. This guideline should serve as a reference document that NERC functional entities may use as needed to improve and ensure BES reliability and is based upon actual lessons learned over the last several years as natural gas has developed into the fuel of choice due to its availability and economic competitiveness. The document focuses on the areas of preparation, coordination, communication, and intelligence that may be applied to improve gas and electric coordinated operations and minimize interdependent risks. Each entity should assess the risks associated with this transformation and apply a set of appropriate processes and practices across its system to mitigate those risks. The guidance is not a "one size fits all" set of measures but rather a list of principles and strategies that can be applied according to the circumstances encountered in a particular system, Balancing Authority, generator fleet or even an individual Generator Operator.

Formatted: Left

F. Contributors

Formatted: Heading 1, Left, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 5 + Alignment: Left + Aligned at: 0" + Indent at: 0.25"

This Reliability Guideline was originally published in December, 2017. The final revised product, from a full review of industry feedback, was completed in 2021 as planned by the RSTC. This work was a collaboration by the members of the NERC Electric Gas Working Group and the NERC Real Time Operating Subcommittee.

Formatted: Left

Agenda Item 8
Reliability and Security
Technical Committee Meeting
June 8, 2021

Security Guideline for the Electricity Sector: Assessing and Reducing Risk

Action

Approve

Summary

The purpose of this Guideline is to help organizations determine their current security and compliance posture and develop an improvement plan for addressing any gaps that are identified. The tool for that analysis maps requirements of the CIP Reliability Standards to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (hereafter referred to as “the framework”), and it can help a responsible entity identify areas that may require further action. This document was posted for a 45-day comment period and conforming revisions made to it based on comments received. A clean and redline version were included in the agenda package along with a response to comments.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Guideline for the Electricity Sector: Assessing and Reducing Risk

The North American Electric Reliability Corporation (NERC) Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups, develops and triennially reviews reliability guidelines in accordance with the procedures set forth in the RSTC Charter[1]. Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that impact bulk power system (BPS) operations, safety, planning, security, and resiliency. Reliability guidelines provide key practices, guidance, and information on specific issues critical to promote and maintain a highly reliable and secure BPS.

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory Reliability Standards. Reliability guidelines are not binding norms or parameters; however, NERC encourages entities to review, validate, adjust, and/or develop a program with the practices set forth in this guideline in coordination with the Reliability Guidelines. Entities should review this guideline in detail and in conjunction with evaluations of their internal processes and procedures; these reviews could highlight that appropriate changes are needed, and these changes should be done with consideration of system design, configuration, and business practices.

The objective of the Security Guideline is to distribute key practices and information on specific issues critical to promote and maintain a highly reliable and secure bulk power system (BPS). Security Guidelines are not binding norms or parameters to the level that compliance to NERC's Reliability Standards is monitored or enforced. Rather, their incorporation into industry practices is strictly voluntary.

Executive Summary

The purpose of this Guideline is to help organizations determine their current security and compliance posture and develop an improvement plan for addressing any gaps that are identified. The tool for that analysis maps requirements of the CIP Reliability Standards to the National Institute of Standards and Technology (NIST) Cybersecurity Framework[2] (hereafter referred to as "the framework"), and it can help a responsible entity identify areas that may require further action.

The tool and associated instructions were the result of a collaborative effort by industry volunteers from the RSTC, Security Working Group (SWG), and representatives from NERC and NIST. The deliverables associated with the guideline underwent a pilot study with SWG members; their recommendations were incorporated into the final version.

Background

[1] https://www.nerc.com/comm/RSTC/RelatedFiles/RSTC_Charter_approved20191105.pdf
[2] https://www.nist.gov/cyberframework

NIST's mission is to promote United States innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. As a part of its mission, NIST has developed standards, special publications, and guidelines on various topics, including cybersecurity. In February 2014, NIST published the original Cybersecurity Framework based on existing standards, guidelines, and practices for reducing cybersecurity risks. The framework provides a prioritized, flexible, repeatable, and cost-effective approach, including information security measures and controls to help owners and operators of critical infrastructure and other interested entities to identify, assess, and manage cybersecurity-related risk while protecting business confidentiality, individual privacy, and civil liberties.

In January 2020, NERC and NIST representatives approached the SWG to review the framework 1.1 mapping[3] and update it to align with the current version of the CIP Reliability Standards.

The SWG team that produced this Guideline had the following objectives:

- **Vision**

  Provide responsible entity subject matter experts or practitioners with the capability to assess current compliance and security posture and develop a roadmap and/or business justification to reach risk levels per their organization's acceptable risk appetite.

- **Deliverables**

  Documentation

  Guideline that provides a methodology for performing a self-assessment, directions for using the self-assessment tool, potential use cases for identifying gaps in compliance or programs, and assistance in developing risk based business justifications for improvement.

  Tool

  Spreadsheet to self-assess compliance with CIP requirements and security practices and prioritize risk management strategies based on the self-assessment results.

Methodology

The methodology used to develop this Guideline leverages the external sources that are indicated below to highlight the relationships between the CIP Reliability Standard requirements and cybersecurity outcomes. "Outcomes" provide a common language for assessing, understanding, and communicating the results for managing cybersecurity-related risk to internal and external stakeholders without limiting the focus to compliance.

- **Authoritative documents[4]**

  NERC CIP Reliability Standards

  The cybersecurity requirements for reliable operation of the North American BPS

[3] Mapping of CIP Standards to NIST Cybersecurity Framework (CSF) v1.1

[4] Note: mechanisms and processes being implemented to update the self-assessment tool to reflect authoritative document changes

NIST Framework V1.1:

A set of activities to achieve specific cybersecurity outcomes and informative reference examples of guidance how to achieve them

- **Informative references**

  Standards, guidelines, and practices that illustrate a method to achieve the cybersecurity outcomes, as cited in the framework

- **Relationships**

  The association of framework outcomes to CIP requirements to inform overall cybersecurity posture, program, and risk management practice maturity:

  Compliance

  Outcomes that directly relate to and support compliance and cybersecurity requirements

  Cybersecurity

  Although not directly applicable to compliance with the CIP Reliability Standards, associated framework outcomes provide cybersecurity program assurance

Self-Assessment Tool Usage Instructions

These are the instructions for using the companion self-assessment tool of this Guideline. See the **Appendix - Self-Assessment tool design and logic** of this document for an explanation of the design, logic, and screen shots of the self-assessment tool.

1. **Required:** read the "Instructions" tab of the self-assessment tool that mirror these instructions.

2. **Optional:** familiarize yourself with the "Implementation Tier" short descriptions on the Data Validation Values tab of the self-assessment tool. You may wish to print those and have them on hand when performing the self-assessment.
    a. Implementation tiers are a direct copy of the tiers as described in the NIST framework.
    b. Implementation tiers provide context on how an organization views cybersecurity risk and the processes in place to manage risk.
    c. The tool provides the capabilities for changing the implementation tier short descriptors to suit your Organization's terms if so desired in cells B2:B5.

3. **Optional:** if no substantive knowledge of the CIP requirements, review the "CIP Standards" tab and/or the link included in the instructions to NERC's CIP Reliability Standards for the detailed requirements associated with each CIP Reliability Standard.

4. **Optional:** for a list of security standards, guidelines, and practices that map to each framework sub-category, see the "Cyber Security Framework" tab. The associated standards can be used to compare your company's internal controls or cybersecurity program against the Cyber Security Framework to identify potential gaps.

5. **Required:** on the "Self-Assessment" tab, perform a risk self-assessment of your company's CIP compliance and cybersecurity practices by selecting from Column I the tier that best represents your implementation level/status of associated outcome.

    Note: the self-assessment tool is intended for CIP requirement owners or practitioners responsible for the creation and implementation of the security controls

6. **Optional:** included with the tool is the capability to modify the provided relationships for each framework sub-category to the associated CIP requirements if so desired.
    a. Select an alternate relationship from the available drop-down list of Column H.
    b. If different and/or a set of alternative relationships are desired, provisions have been built into the tool to do so on the "data validation values" tab in cells B16:B20.

7. **Required:** review the self-assessment results on the "Implementation Dashboard" tab. This tab is automatically updated based on the information entered on the "Self-Assessment" tab. Results displayed are as follows:
    a. Column E (Average Implementation Score) shows the average implementation of the associated framework sub-categories. Conditional color formatting is used to show levels

of risk based on the level of implemented cybersecurity-related risk management practices (larger numbers = higher implementation levels, with lower risk):

   i. Green for > 3.5 – low risk
   ii. Yellow for between 2.5–3.5 – minimal risk
   iii. Orange for between 1.5–2.5 – moderate risk
   iv. Red for between 1.0–1.5 – high risk

b. Column H (CSF-ID to CIP relationship) is provided to identify compliance or cybersecurity-related categories related to an associated CIP requirement that could be used to prioritize risk treatment activities based on the risk focus of your organization.

c. Column I (Cybersecurity Risk Management Tier) represents the implementation tier of the framework sub-category outcomes associated with a given CIP requirement.

   i. Level 1 represents low or immature capabilities and Level 4 represents high or very mature capabilities.

   Note: Column J contains the descriptor with the associated Implementation Tier from the "data validation values" tab in cells B2:B5.

Self-Assessment Results Use Cases

The following are potential suggested use cases of the self-assessment results on the "Implementation Dashboard" of the self-assessment tool:

1. **CIP Violation Risk Factor focus:** filter on Column D (VRF) to identify High VRF ranked CIP requirements with a low average implementation scores in Column E. This sorting identifies potential CIP Violation Risk Factor compliance improvement opportunities

2. **CIP Compliance focus:** filter on Column H (CSF-IT to CIP Relationship) for "compliance related" relationships (or your equivalent alternative you may have added), to identify potential CIP compliance improvement opportunities based on the associated risk implementation tier noted in columns I and J

3. **Cybersecurity focus:** filter on Column H (CSF-IT to CIP Relationship) for "cybersecurity related" relationships (or your equivalent alternative you may have added), to identify potential cybersecurity compliance improvement opportunities based on the associated risk implementation tier noted in columns I and J

Regardless of focus, results can be used to develop business justification for annual budget and resource planning purposes focused on security and compliance risk reduction. Results could also be used to develop a long-term improvement roadmap.

In all cases, responsible entities are encouraged to leverage the framework informative references that may be used in the following manners:

- Center for Internet Security (CIS) Top 20 Critical Security Controls[5]: technology teams leverage the CIS top 20 security controls to review IT internal controls
- **Security Programs:** cybersecurity teams utilize NIST 800-53 or ISO27001/ISO27002 comprehensive security controls to compare implemented security programs
- **Governance:** governance and oversight teams utilize COBIT security controls to review IT governance and management practices
- **Industrial Control/OT:** control system operations leverage the ISA 62443 security controls to review implemented security protection measures

Metrics

Pursuant to the Commission's Order on January 19, 2021, North American Electric Reliability Corporation, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review, consistent with the RSTC Charter.

Baseline Metrics

- Performance of the BPS prior to and after a reliability guideline, as reflected in NERC's State of Reliability Report and Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments);
- Use and effectiveness of a reliability guideline as reported by industry via survey; and
- Industry assessment of the extent to which a reliability guideline is addressing risk as reported via survey.

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure and evaluate its effectiveness.

[5] https://www.cisecurity.org/controls/cis-controls-list/

SWG Task Force Members

The following is the list of SWG task force members who volunteered to develop this Guideline document, associated self-assessment tool and overview PowerPoint.

Keith St. Amand (project lead)
Midcontinent Independent System Operator

Dan Wagner / Aldo Nevárez
Western Electricity Coordinating Council

Monica Jain
Southern California Edison

Brenda Davis
CPS Energy

Mike Johnson
Pacific Gas & Electric

Karl Perman
Department of Water Resources California

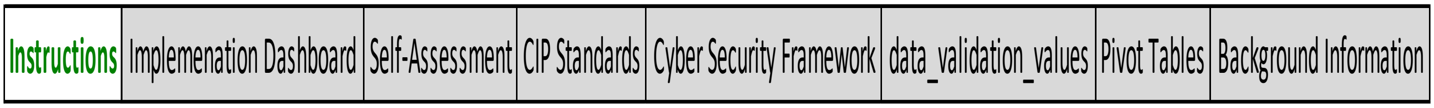
Jeff Marron
National Institute of Standards and Technology

Matthew Light
Western Area Power Administration

Appendix: Self-Assessment Tool Design and Logic

A companion self-assessment tool to this Guideline document has also been developed. The self-assessment tool is based on Microsoft Excel (see **Figure 1**) and provides a mechanism for CIP standard and requirement owners to perform a simple rating of their current risk implementation levels and obtain a "dashboard" that provides actionable criteria to focus on and communicate to stakeholders.

Note: this self-assessment tool was tested within a volunteer set of SWG member companies—their feedback and update suggestions were incorporated into this Guideline and the self-assessment tool.



Instructions	Implemenation Dashboard	Self-Assessment	CIP Standards	Cyber Security Framework	data_validation_values	Pivot Tables	Background Information

Figure 1: Excel workbook tabs

Tabs: The Excel workbook contains the following tabs and associated descriptions:

- **Instructions:** contains general guidance and suggested order of usage information
- **Implementation Dashboard:** presents the results of the Self-Assessment tab; results depicting summary score of each framework sub-category associated with a CIP requirement
- **Self-Assessment:** mapping of CIP requirements aligned to the framework categories (Objectives) and sub-categories (outcomes) with a cybersecurity risk management tier selection item for CIP requirement owner to choose.
- **CIP Standards:** containing unique ID, purpose + requirements, and violation risk factor (VRF) Rating associated with each requirement (Columns B and C are direct copies from the standards. Column A is provided to facilitate Excel pivot table and formula functionality).

  Note: this tab is for reference purposes only and is used in the first two tabs to minimize future maintenance and update efforts of the tool.
- **Cyber Security Framework**: contain information downloadable and available directly from the NIST Cybersecurity Framework.

  Note: this tab is for reference purposes only and is used in the first two tabs to minimize maintenance and update efforts.
- **Data Validation Values:**
  - Contains Excel "named references" used throughout the workbook.
  - Provides the capability of changing the implementation tier descriptions if the native framework risk implementation tiers are not preferred.
  - Contains a description for the framework risk tiers

    - Contains a description of the CIP to the framework relationships used in the tool

- **Pivot Tables:** contains Excel pivot tables that depict the cross-references of CIP requirement ID to the Framework Sub-Category ID and the Framework Sub-Category to CIP to CIP requirement IT.

  Note: The purpose of these cross-references is to facilitate independent analysis if needed/desired.

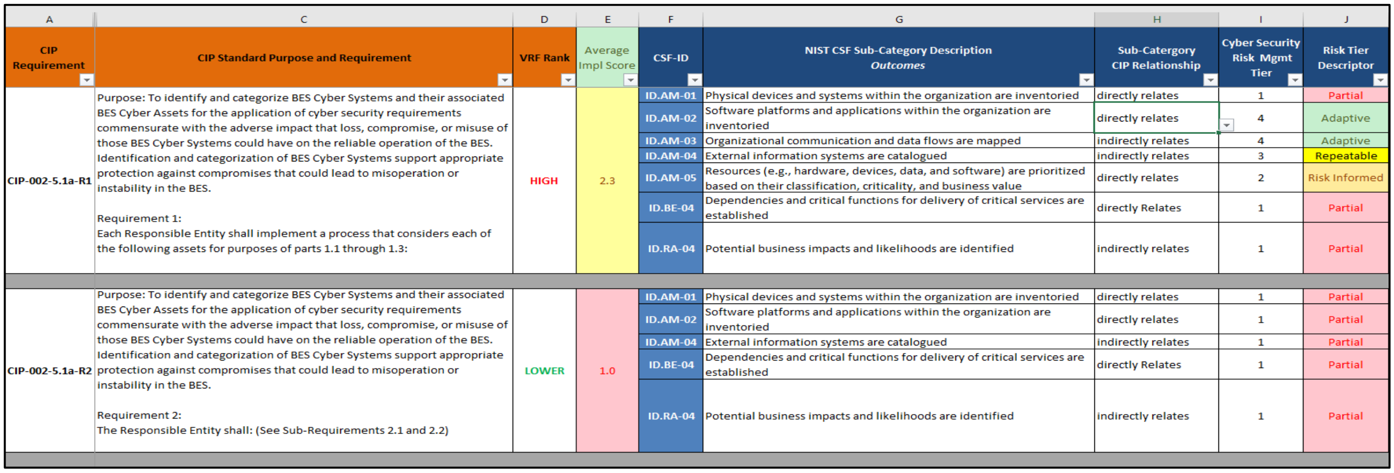
- **Background Information:** contains additional detail information, benefits, tab descriptions, and assumptions – with the goal of providing sufficient information to make this a standalone tool and requiring a separate document to fully understand the tool.

Logic: The following provides the highlights of the logic applied in the Excel self-assessment tool:

- All tabs are password protected and cells are locked in order to preserve the dynamic and automated features built into the tool.

  Note: The SWG task force team has designed the tool to minimize future update and maintenance efforts. Plans are to provide updates periodically, as either the CIP requirements or the framework updates are released.

- **Implementation Dashboard Tab (see Figure 2)**
    - Contains cell formula in all but Column A and F to automatically update cell contents
        - Column C and D contents updated based on matching row in the CIP Standards tab
        - Column E is the average calculated from the corresponding Risk Management Tier values in Column I
        - Column G contents updated based on matching row in the Cyber Security Framework tab
        - Column H was filled in based on the analysis for the SWG task force team and feedback from testing volunteers
        - Column J contents based on the corresponding value from the data validation values tab
        - Color Conditional formatting:
            - Column D: red for high, brown for medium, green for Lower
            - Column E: green for > 3.5, yellow for 2.5–3.5, orange for 1.5–2.5, red for 1.0–1.5 (in order to avoid applying color formatting to blank rows)
            - Colum J: dynamic formula based on the matching tier on the data validation values tab

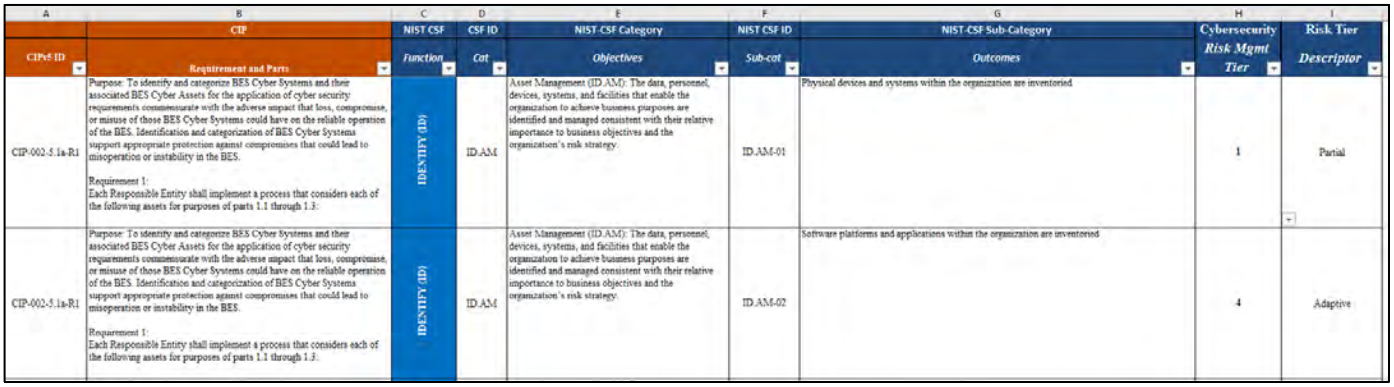


CIP Requirement	CIP Standard Purpose and Requirement	VRF Rank	Average Impl Score	CSF-ID	NIST CSF Sub-Category Description *Outcomes*	Sub-Catergory CIP Relationship	Cyber Security Risk Mgmt Tier	Risk Tier Descriptor
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	HIGH	2.3	ID.AM-01	Physical devices and systems within the organization are inventoried	directly relates	1	Partial
				ID.AM-02	Software platforms and applications within the organization are inventoried	directly relates	4	Adaptive
				ID.AM-03	Organizational communication and data flows are mapped	indirectly relates	4	Adaptive
				ID.AM-04	External information systems are catalogued	indirectly relates	3	Repeatable
				ID.AM-05	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	directly relates	2	Risk Informed
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	directly Relates	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	indirectly relates	1	Partial
CIP-002-5.1a-R2	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 2: The Responsible Entity shall: (See Sub-Requirements 2.1 and 2.2)	LOWER	1.0	ID.AM-01	Physical devices and systems within the organization are inventoried	directly relates	1	Partial
				ID.AM-02	Software platforms and applications within the organization are inventoried	directly relates	1	Partial
				ID.AM-04	External information systems are catalogued	indirectly relates	1	Partial
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	directly Relates	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	indirectly relates	1	Partial

Figure 2: Implementation Dashboard Tab

- **Self-Assessment Tab (see Figure 3)**
  - All cell contents are populated based on formula reading from either the CIP standards, cyber security framework, or data validation values tabs—intent is to simplify future maintenance update efforts

  Note – the outcomes in Column G are not requirements or may not necessarily equate with the NERC CIP requirement, but they can be helpful for Responsible Entities to improve their security posture while helping demonstrate compliance with associated NERC CIP requirements

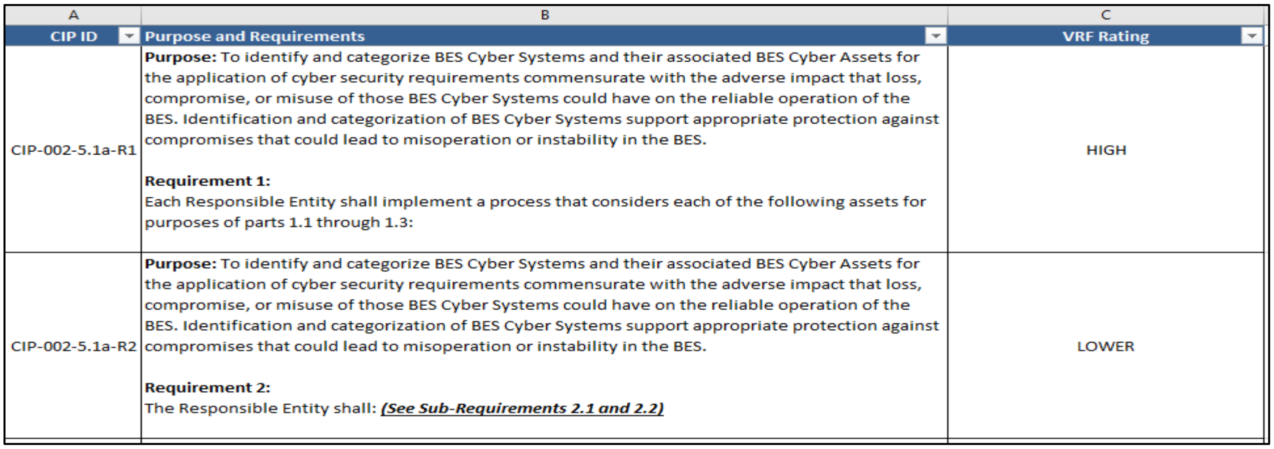


	CIP	NIST CSF	CSF ID	NIST-CSF Category	NIST CSF ID	NIST-CSF Sub-Category	Cybersecurity	Risk Tier
CIPv5 ID	Requirement and Parts	*Function*	*Cat*	*Objectives*	*Sub-cat*	*Outcomes*	*Risk Mgmt Tier*	*Descriptor*
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-01	Physical devices and systems within the organization are inventoried	1	Partial
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-02	Software platforms and applications within the organization are inventoried	4	Adaptive

Figure 3: Self-Assessment Tab

- **CIP Standards Tab** (see **Figure 4**)**:** is a compilation of the current effective CIP standards subject to enforcement, as posted on the NERC CIP Standards site.

  Note: normalized/standardized IDs were created in order to facilitate linkage between the various tabs, filtering, and Pivot Table capabilities

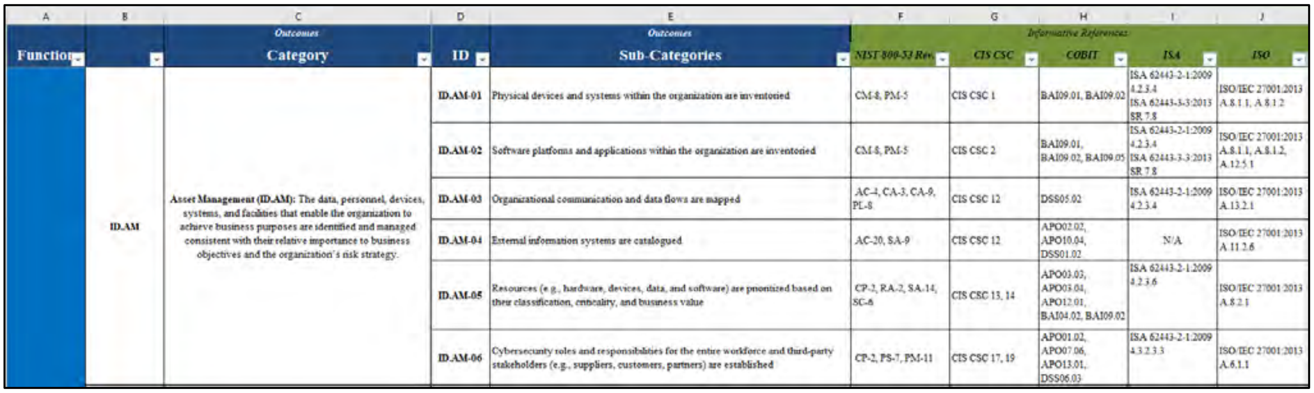


A	B	C
CIP ID	Purpose and Requirements	VRF Rating
CIP-002-5.1a-R1	**Purpose:** To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. **Requirement 1:** Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	HIGH
CIP-002-5.1a-R2	**Purpose:** To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. **Requirement 2:** The Responsible Entity shall: ***(See Sub-Requirements 2.1 and 2.2)***	LOWER

Figure 4: CIP Standards Tab

- **Cyber Security Framework Tab (see Figure 5):** contains a modified download of the Excel file available from the framework site[6]. The only modification was to place the informative references into individual columns as opposed to including them all in a single cell for each sub-category.

  Note: normalized/standardized IDs were created in order to facilitate linkage between the various tabs, filtering, and Pivot Table capabilities



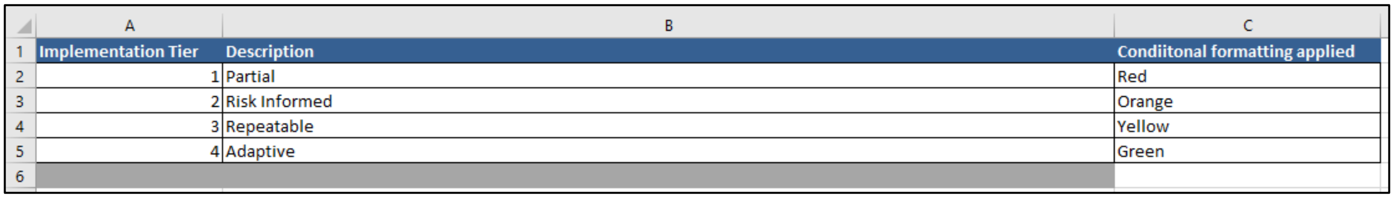
A	B	C	D	E	F	G	H	I	J
		Outcomes		*Outcomes*	*Informative References*				
Function		Category	ID	Sub-Categories	*NIST 800-53 Rev.*	*CIS CSC*	*COBIT*	*ISA*	*ISO*
	ID.AM	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-01	Physical devices and systems within the organization are inventoried	CM-8, PM-5	CIS CSC 1	BAI09.01, BAI09.02	ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8	ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
			ID.AM-02	Software platforms and applications within the organization are inventoried	CM-8, PM-5	CIS CSC 2	BAI09.01, BAI09.02, BAI09.05	ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8	ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1
			ID.AM-03	Organizational communication and data flows are mapped	AC-4, CA-3, CA-9, PL-8	CIS CSC 12	DSS05.02	ISA 62443-2-1:2009 4.2.3.4	ISO/IEC 27001:2013 A.13.2.1
			ID.AM-04	External information systems are catalogued	AC-20, SA-9	CIS CSC 12	APO02.02, APO10.04, DSS01.02	N/A	ISO/IEC 27001:2013 A.11.2.6
			ID.AM-05	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, SA-14, SC-6	CIS CSC 13, 14	APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02	ISA 62443-2-1:2009 4.2.3.6	ISO/IEC 27001:2013 A.8.2.1
			ID.AM-06	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CP-2, PS-7, PM-11	CIS CSC 17, 19	APO01.02, APO07.06, APO13.01, DSS06.03	ISA 62443-2-1:2009 4.3.2.3.3	ISO/IEC 27001:2013 A.6.1.1

Figure 5: Cyber Security Framework Tab

- **Data validation Values (see Figure 6):** primarily for lookup and Excel "named references" purposes used throughout the workbook:
  - **Customization:** cells B2–B5 are unlocked, if a responsible entity does not like the Risk Implementation Tiers as provided by the framework. Changing those to whatever an entity prefers, will automatically update the corresponding values on the other sheets.

[6] https://www.nist.gov/cyberframework/framework

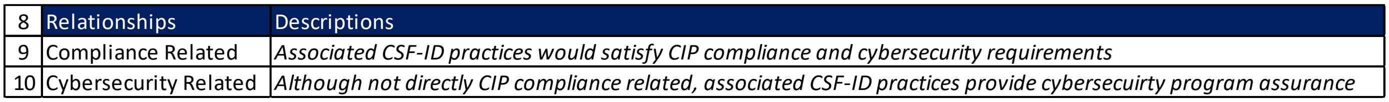
Note: Cells C2–C5 are for reference purposes only, describing the conditional formatting colors used on the Implementation Dashboard corresponding to the associated Implementation Tier #.



	A	B	C
1	Implementation Tier	Description	Condiitonal formatting applied
2	1	Partial	Red
3	2	Risk Informed	Orange
4	3	Repeatable	Yellow
5	4	Adaptive	Green
6			

Figure 6: Data Validation Values tab: Customization #1

- **Customization (see Figure 7)**: cells A9 and A13 are unlocked if a responsible entity wishes to use different text to describe.



8	Relationships	Descriptions
9	Compliance Related	*Associated CSF-ID practices would satisfy CIP compliance and cybersecurity requirements*
10	Cybersecurity Related	*Although not directly CIP compliance related, associated CSF-ID practices provide cybersecuirty program assurance*

Figure 7: Data Validation Values tab: Customization #2

Design Assumptions

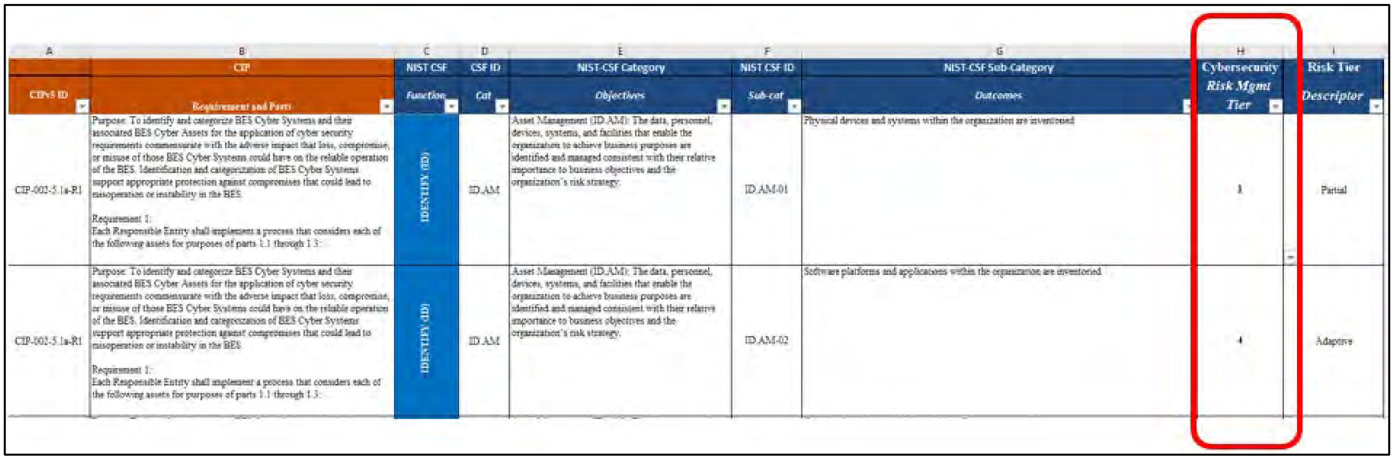
- Each responsible entity will have implemented their own security controls that are often based on the same security guidance identified in the framework informative references.
- Generally, there are separate CIP requirement owners assigned within responsible entity companies and usually develop associated policies, controls, and/or practices.
- By providing a cross-mapping of the CIP standards to the framework sub-categories, requirement owners can view the associated informative reference practices to compare their implemented security controls against.
- The Implementation Dashboard tab summary results will help identify gaps and/or improvement opportunities.

Self-Assessment Tab Instructions (see Figure 8)

1. Either distribute the self-assessment tool spreadsheet to individual CIP requirement owners or gather all CIP requirement owners together to collectively review and assess their associated requirement implementation level.

2. CIP requirement owners review each of their associated CIP requirements and select the risk implementation level from the available drop-down number in Column H (Cybersecurity Risk Management Tier) that best represents their current practice implementation level.

3. Once completed, move on to review summary results in the Implementation Dashboard tab.



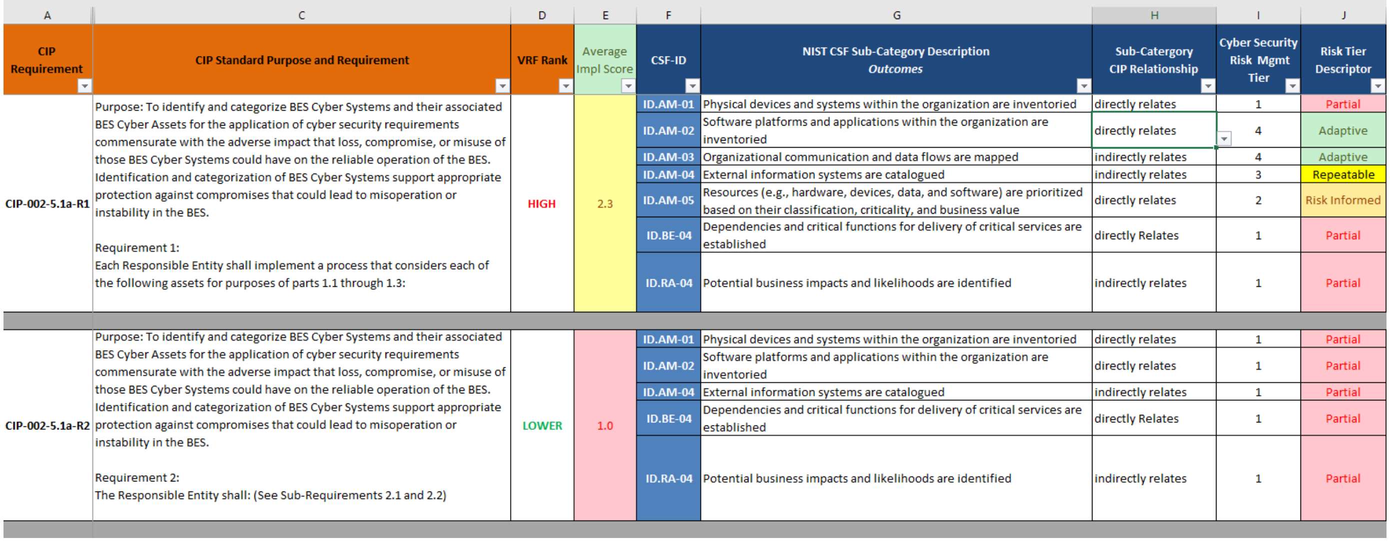
A	B	C	D	E	F	G	H	I
	CIP	NIST CSF	CSF ID	NIST-CSF Category	NIST CSF ID	NIST-CSF Sub-Category	Cybersecurity	Risk Tier
CIPv5 ID	Requirement and Parts	*Function*	*Cat*	*Objectives*	*Sub-cat*	*Outcomes*	*Risk Mgmt Tier*	*Descriptor*
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-01	Physical devices and systems within the organization are inventoried	1	Partial
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-02	Software platforms and applications within the organization are inventoried	4	Adaptive

Figure 8: Completing Self-Assessment tab

Implementation Dashboard potential Use Cases:

After all rows in the Self-Assessment tab (see Figure 9) have been completed, the implementation dashboard will represent the summary risk results by CIP requirement to highlight the following:

- Identify where there may be **CIP Violation** risks based on the VRF rank value in Column D and the corresponding "Average Impl Score" in Column E
- Identify where there may be **Compliance** risks, based on the "Directly Relates" relationship in Column H and a corresponding low implementation level in Column J
- Identify where there may be **Security** risks, based on the "Indirectly Relates" relationship in Column H and a corresponding low implementation level in Column J



A	C	D	E	F	G	H	I	J
CIP Requirement	CIP Standard Purpose and Requirement	VRF Rank	Average Impl Score	CSF-ID	NIST CSF Sub-Category Description *Outcomes*	Sub-Catergory CIP Relationship	Cyber Security Risk Mgmt Tier	Risk Tier Descriptor
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	HIGH	2.3	ID.AM-01	Physical devices and systems within the organization are inventoried	directly relates	1	Partial
				ID.AM-02	Software platforms and applications within the organization are inventoried	directly relates	4	Adaptive
				ID.AM-03	Organizational communication and data flows are mapped	indirectly relates	4	Adaptive
				ID.AM-04	External information systems are catalogued	indirectly relates	3	Repeatable
				ID.AM-05	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	directly relates	2	Risk Informed
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	directly Relates	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	indirectly relates	1	Partial
CIP-002-5.1a-R2	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 2: The Responsible Entity shall: (See Sub-Requirements 2.1 and 2.2)	LOWER	1.0	ID.AM-01	Physical devices and systems within the organization are inventoried	directly relates	1	Partial
				ID.AM-02	Software platforms and applications within the organization are inventoried	directly relates	1	Partial
				ID.AM-04	External information systems are catalogued	indirectly relates	1	Partial
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	directly Relates	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	indirectly relates	1	Partial

Figure 9: Review Self-Assessment Results

References

- NIST Cybersecurity Framework 1.1: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NERC CIP Enforceable Standards: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- Mapping of NIST Cybersecurity Framework to NERC CIP v3/v5 November 2014 - https://www.nerc.com/comm/CIPC_Security_Guidelines_DL/CSSWG-Mapping_of_NIST_Cybersecurity_Framework_to_NERC_CIP.pdf
- Mapping of CIP Standards to NIST Cybersecurity Framework v1.1 Updated: https://www.nerc.com/pa/comp/Pages/CAOneStopShop.aspx (under Compliance | NIST)
- FERC NOPR 12-17-2020 Incentives Effort - E-2-RM21-3-000 | Federal Energy Regulatory Commission (ferc.gov)

Version History

SWG Security and Compliant Guidance Version History					
Version No.	Date	Chapter	Page	Description	Version
1	October 2020	All	All	Original Document	.1
2	November 12, 2020	All	All	Publications and Admin review complete	.2
3	June 2021	All	All	Approved by the RSTC	1.0

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Security Guideline for the Electricity Sector: Assessing and Reducing Risk

The North American Electric Reliability Corporation (NERC) Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups, develops and triennially reviews reliability guidelines in accordance with the procedures set forth in the RSTC Charter[1]. Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that impact bulk power system (BPS) operations, safety, planning, ~~and~~ security, and resiliency. Reliability guidelines provide key practices, guidance, and information on specific issues critical to promote and maintain a highly reliable and secure BPS.

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory Reliability Standards. Reliability guidelines are not binding norms or parameters; however, NERC encourages entities to review, validate, adjust, and/or develop a program with the practices set forth in this guideline in coordination with the Reliability Guidelines. Entities should review this guideline in detail and in conjunction with evaluations of their internal processes and procedures; these reviews could highlight that appropriate changes are needed, and these changes should be done with consideration of system design, configuration, and business practices.

The objective of the Security Guideline is to distribute key practices and information on specific issues critical to promote and maintain a highly reliable and secure bulk power system (BPS). Security Guidelines are not binding norms or parameters to the level that compliance to NERC's Reliability Standards is monitored or enforced. Rather, their incorporation into industry practices is strictly voluntary.

Executive Summary

The purpose of this Guideline is to help organizations determine their current security and compliance posture and develop an improvement plan for addressing any gaps that are identified. The tool for that analysis maps requirements of the CIP Reliability Standards to the National Institute of Standards and Technology (NIST) Cybersecurity Framework[2] (hereafter referred to as "the framework"), and it can help a responsible entity identify areas that may require further action.

The tool and associated instructions were the result of a collaborative effort by industry volunteers from the RSTC, Security Working Group (SWG), and representatives from NERC and NIST. The deliverables associated with the guideline underwent a pilot study with SWG members; their recommendations were incorporated into the final version.

Background

[1] https://www.nerc.com/comm/RSTC/RelatedFiles/RSTC_Charter_approved20191105.pdf
[2] https://www.nist.gov/cyberframework

NIST's mission is to promote United States innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. As a part of its mission, NIST has developed standards, special publications, and guidelines on various topics, including cybersecurity. In February 2014, NIST published the original Cybersecurity Framework based on existing standards, guidelines, and practices for reducing cybersecurity risks. The framework provides a prioritized, flexible, repeatable, and cost-effective approach, including information security measures and controls to help owners and operators of critical infrastructure and other interested entities to identify, assess, and manage cybersecurity-related risk while protecting business confidentiality, individual privacy, and civil liberties.

In January 2020, NERC and NIST representatives approached the SWG to review the framework 1.1 mapping[3] and update it to align with the current version of the CIP Reliability Standards.

The SWG team that produced this Guideline had the following objectives:

- **Vision**

  Provide responsible entity subject matter experts or practitioners with the capability to assess current compliance and security posture and develop a roadmap and/or business justification to reach risk levels per their organization's acceptable risk appetite.

- **Deliverables**

  Documentation

  Guideline that provides a methodology for performing a self-assessment, directions for using the self-assessment tool, potential use cases for identifying gaps in compliance or programs, and assistance in developing risk ~~basked~~ based business justifications for improvement.

  Tool

  Spreadsheet to self-assess compliance with CIP requirements and security practices and prioritize risk management strategies based on the self-assessment results.

Methodology

The methodology used to develop this Guideline leverages the external sources that are indicated below to highlight the relationships between the CIP Reliability Standard requirements and cybersecurity outcomes. "Outcomes" provide a common language for assessing, understanding, and communicating the results for managing cybersecurity-related risk to internal and external stakeholders without limiting the focus to compliance.

- **Authoritative documents[4]**

  NERC CIP Reliability Standards

  The cybersecurity requirements for reliable operation of the North American BPS

[3] Mapping of CIP Standards to NIST Cybersecurity Framework (CSF) v1.1

[4] Note: mechanisms and processes being implemented to update the self-assessment tool to reflect authoritative document changes

NIST Framework V1.1:

A set of activities to achieve specific cybersecurity outcomes and informative reference examples of guidance how to achieve them

- **Informative references**

  Standards, guidelines, and practices that illustrate a method to achieve the cybersecurity outcomes, as cited in the framework

- **Relationships**

  The association of framework outcomes to CIP requirements to inform overall cybersecurity posture, program, and risk management practice maturity:

  Compliance

  Outcomes that directly relate to and support compliance and cybersecurity requirements

  Cybersecurity

  Although not directly applicable to compliance with the CIP Reliability Standards, associated framework outcomes provide cybersecurity program assurance

Self-Assessment Tool Usage Instructions

These are the instructions for using the companion self-assessment tool of this Guideline. See the **Appendix - Self-Assessment tool design and logic** of this document for an explanation of the design, logic, and screen shots of the self-assessment tool.

1. **Required:** read the “Instructions” tab of the self-assessment tool that mirror these instructions.

2. **Optional:** familiarize yourself with the “Implementation Tier” short descriptions on the Data Validation Values tab of the self-assessment ~~also~~tool. You may wish to print those and have them on hand when performing the self-assessment.
    a. Implementation tiers are a direct copy of the tiers as described in the NIST framework.
    b. Implementation tiers provide context on how an organization views cybersecurity risk and the processes in place to manage risk.
    c. The tool provides the capabilities for changing the implementation tier short descriptors to suit your O~~o~~rganization’s terms if so desired in cells B2:B5.

3. **Optional:** if no~~t~~ substantive knowledge ~~ofintimately familiar with the~~of the CIP requirements, review the “CIP Standards” tab and/or the link included in the instructions to NERC’s CIP Reliability Standards for the detailed requirements associated with each CIP Reliability Standard.

4. **Optional:** for a list of security standards, guidelines, and practices that map to each framework sub-category, see the “Cyber Security Framework” tab. The associated standards can be used to compare your company’s internal controls or cybersecurity program against the Cyber Security Framework to identify potential gaps.

5. **Required:** on the “Self-Assessment” tab, perform a risk self-assessment of your company’s CIP compliance and cybersecurity practices by selecting from Column I the tier that best represents your implementation level/status of associated outcome.

    Note: the self-assessment tool is intended for CIP requirement owners or practitioners responsible for the creation and implementation of the security controls

6. **Optional:** included with the tool is the capability to modify the provided relationships for each framework sub-category to the associated CIP requirements if so desired.
    a. Select an alternate relationship from the available drop-down list of Column H.
    b. If different and/or a set of alternative relationships are desired, provisions have been built into the tool to do so on the “data validation values” tab in cells B16:B20.

7. **Required:** review the self-assessment results on the “Implementation Dashboard” tab. This tab is automatically updated based on the information entered on the “Self-Assessment” tab. Results displayed are as follows:
    a. Column E (Average Implementation Score) shows the average implementation of the associated framework sub-categories. Conditional color formatting is used to show levels

of risk based on the level of implemented cybersecurity-related risk management practices (larger numbers = higher implementation levels, with lower risk):

i. Green for > 3.5 – low risk
ii. Yellow for between 2.5–3.5 – minimal risk
iii. Orange for between 1~~3~~.5–2~~4~~.5 – moderate risk
iv. Red for between 1.0–1.5 – high risk

b. Column H (CSF-ID to CIP relationship) is provided to identify compliance or cybersecurity-related categories related to an associated CIP requirement that could be used to prioritize risk treatment activities based on the risk focus of your organization.

c. Column I (Cybersecurity Risk Management Tier) represents the implementation tier of the framework sub-category outcomes associated with a given CIP requirement.

i. Level 1 represents low or immature capabilities and Level ~~5~~ 4 represents high or very mature capabilities.

Note: Column J contains the descriptor with the associated Implementation Tier from the "data validation values" tab in cells B2:B5.

Self-Assessment Results Use Cases

The following are potential suggested use cases of the self-assessment results on the "Implementation Dashboard" of the self-assessment tool:

1. **CIP Violation Risk Factor focus:** filter on Column D (VRF) to identify High VRF ranked CIP requirements with a low average implementation scores in Column E~~,~~. ~~to identify~~This sorting identifies potential CIP Violation Risk Factor compliance improvement opportunities

2. **CIP Compliance focus:** filter on Column H (CSF-IT to CIP Relationship) for "compliance related" relationships (or your equivalent alternative you may have added), to identify potential CIP compliance improvement opportunities based on the associated risk implementation tier noted in columns I and J

3. **Cybersecurity focus:** filter on Column H (CSF-IT to CIP Relationship) for "cybersecurity related" relationships (or your equivalent alternative you may have added), to identify potential cybersecurity compliance improvement opportunities based on the associated risk implementation tier noted in columns I and J

Regardless of focus, results can be used to develop business justification for ~~annul~~ annual budget and resource planning purposes focused on security and compliance risk reduction. Results could also be used to develop a long-term improvement roadmap.

In all cases, responsible entities are encouraged to leverage the framework informative references that may be used in the following manners:

- Center for Internet Security (CIS) Top 20 Critical Security Controls[5]: technology teams leverage the CIS top 20 security controls to review IT internal controls
- **Security Programs:** cybersecurity teams utilize NIST 800-53 or ISO27001/ISO27002 comprehensive security controls to compare implemented security programs
- **Governance:** governance and oversight teams utilize COBIT security controls to review IT governance and management practices
- **Industrial Control/OT:** control system operations leverage the ISA 62443 security controls to review implemented security protection measures

Metrics

Pursuant to the Commission's Order on January 19, 2021, North American Electric Reliability Corporation, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review, consistent with the RSTC Charter.

Baseline Metrics

- Performance of the BPS prior to and after a reliability guideline, as reflected in NERC's State of Reliability Report and Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments);
- Use and effectiveness of a reliability guideline as reported by industry via survey; and
- Industry assessment of the extent to which a reliability guideline is addressing risk as reported via survey.

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure and evaluate its effectiveness.

~~• *Suvey Monkey link will be added*~~

[5] https://www.cisecurity.org/controls/cis-controls-list/

SWG Task Force Members

The following is the list of SWG task force members who volunteered to develop this Guideline document, associated self-assessment tool and overview PowerPoint.

Keith St. Amand (project lead)
Midcontinent Independent System Operator

Dan Wagner / Aldo Nevárez
Western Electricity Coordinating Council

Monica Jain
Southern California Edison

Brenda Davis
CPS Energy

Mike Johnson
Pacific Gas & Electric

Karl Perman
Department of Water Resources California

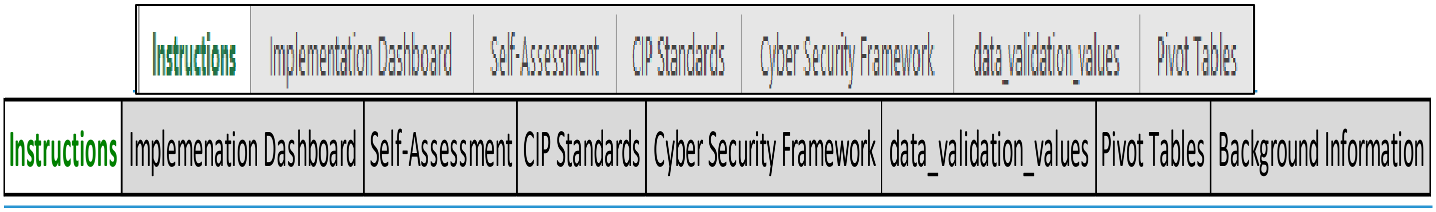
Jeff Marron
National Institute of Standards and Technology

Matthew Light
Western Area Power Administration

Appendix: Self-Assessment Tool Design and Logic

A companion self-assessment tool to this Guideline document has also been developed. The self-assessment tool is based on Microsoft Excel (see **Figure 1**) and provides a mechanism for CIP standard and requirement owners to perform a simple rating of their current risk implementation levels and obtain a “dashboard” that provides actionable criteria to focus on and communicate to stakeholders.

Note: this self-assessment tool was tested within a volunteer set of SWG member companies—their feedback and update suggestions were incorporated into this Guideline and the self-assessment tool.



Instructions	Implementation Dashboard	Self-Assessment	CIP Standards	Cyber Security Framework	data_validation_values	Pivot Tables	
Instructions	Implemenation Dashboard	Self-Assessment	CIP Standards	Cyber Security Framework	data_validation_values	Pivot Tables	Background Information

Figure 1: Excel workbook tabs

Tabs: The Excel workbook contains the following tabs and associated descriptions:

- **Instructions:** contains general guidance and suggested order of usage information
- **Implementation Dashboard:** presents the results of the Self-Assessment tab; results depicting summary score of each framework sub-category associated with a CIP requirement
- **Self-Assessment:** mapping of CIP requirements aligned to the framework categories (Objectives) and sub-categories (outcomes) with a cybersecurity risk management tier selection item for CIP requirement owner to choose.
- **CIP Standards:** containing unique ID, purpose + requirements, and violation risk factor (VRF) Rating associated with each requirement (Columns B and C are direct copies from the standards. Column A is provided to facilitate Excel pivot table and formula functionality).

  Note: this tab is for reference purposes only and is used in the first two tabs to minimize future maintenance and update efforts of the tool.
- **Cyber Security Framework**: contain information downloadable and available directly from the NIST Cybersecurity Framework.

  Note: this tab is for reference purposes only and is used in the first two tabs to minimize maintenance and update efforts.
- **Data Validation Values:**
  - Contains Excel “named references” used throughout the workbook.
  - Provides the capability of changing the implementation tier descriptions if the native framework risk implementation tiers are not preferred.

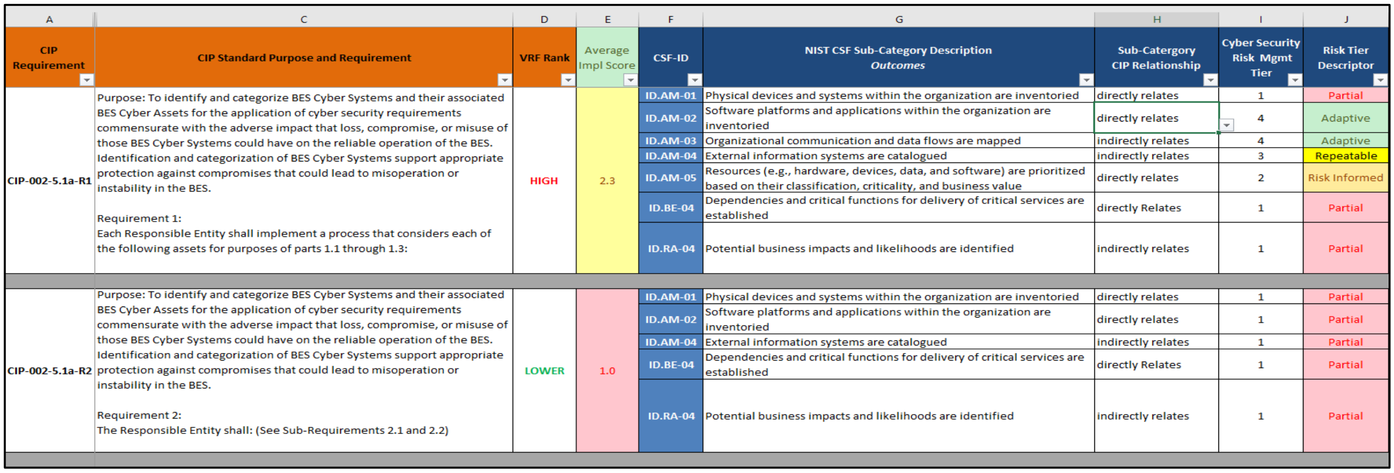
    - Contains a description for the framework risk tiers
    - Contains a description of the CIP to the framework relationships used in the tool
- **Pivot Tables:** contains Excel pivot tables that depict the cross-references of CIP requirement ID to the Framework Sub-Category ID and the Framework Sub-Category to CIP to CIP requirement IT.

  Note: The purpose of these cross-references is to facilitate independent analysis if needed/desired.
- **Background Information:** contains additional detail information, benefits, tab descriptions, and assumptions – with the goal of providing sufficient information to make this a standalone tool and requiring a separate document to fully understand the tool.

Logic: The following provides the highlights of the logic applied in the Excel self-assessment tool:

- All tabs are password protected and cells are locked in order to preserve the dynamic and automated features built into the tool.

  Note: The SWG task force team has designed the tool to minimize future update and maintenance efforts. Plans are to provide updates periodically, as either the CIP requirements or the framework updates are released.
- **Implementation Dashboard Tab (see Figure 2)**
    - Contains cell formula in all but Column A and F to automatically update cell contents
        - Column C and D contents updated based on matching row in the CIP Standards tab
        - Column E is the average calculated from the corresponding Risk Management Tier values in Column I
        - Column G contents updated based on matching row in the Cyber Security Framework tab
        - Column H was filled in based on the analysis for the SWG task force team and feedback from testing volunteers
        - Column J contents based on the corresponding value from the data validation values tab
        - Color Conditional formatting:
            - Column D: red for high, brown for medium, green for Lower
            - Column E: green for > 3.5, yellow for 2.5–3.5, orange for 1.5–2.5, red for 1.0–1.5 (in order to avoid applying color formatting to blank rows)
            - Colum J: dynamic formula based on the matching tier on the data validation values tab

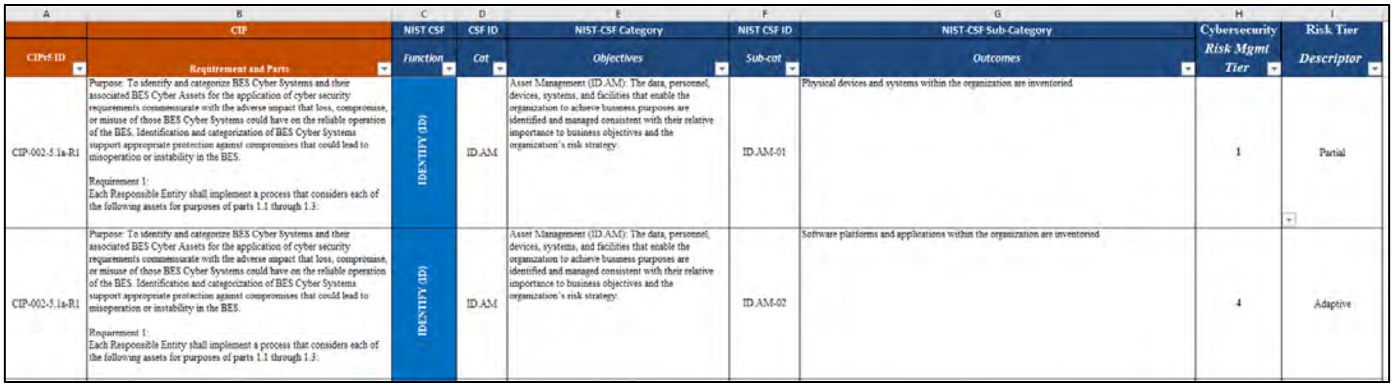


A	C	D	E	F	G	H	I	J
CIP Requirement	CIP Standard Purpose and Requirement	VRF Rank	Average Impl Score	CSF-ID	NIST CSF Sub-Category Description *Outcomes*	Sub-Catergory CIP Relationship	Cyber Security Risk Mgmt Tier	Risk Tier Descriptor
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	HIGH	2.3	ID.AM-01	Physical devices and systems within the organization are inventoried	directly relates	1	Partial
				ID.AM-02	Software platforms and applications within the organization are inventoried	directly relates	4	Adaptive
				ID.AM-03	Organizational communication and data flows are mapped	indirectly relates	4	Adaptive
				ID.AM-04	External information systems are catalogued	indirectly relates	3	Repeatable
				ID.AM-05	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	directly relates	2	Risk Informed
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	directly Relates	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	indirectly relates	1	Partial
CIP-002-5.1a-R2	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 2: The Responsible Entity shall: (See Sub-Requirements 2.1 and 2.2)	LOWER	1.0	ID.AM-01	Physical devices and systems within the organization are inventoried	directly relates	1	Partial
				ID.AM-02	Software platforms and applications within the organization are inventoried	directly relates	1	Partial
				ID.AM-04	External information systems are catalogued	indirectly relates	1	Partial
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	directly Relates	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	indirectly relates	1	Partial

Figure 2: Implementation Dashboard Tab

- **Self-Assessment Tab (see Figure 3)**
  - All cell contents are populated based on formula reading from either the CIP standards, cyber security framework, or data validation values tabs—intent is to simplify future maintenance update efforts

Note – the outcomes in Column G are not requirements or may not necessarily equate with the NERC CIP requirement, but they can be helpful for Responsible Entities~~esource~~ to improve their security posture while helping demonstrate compliance with associated NERC CIP requirements

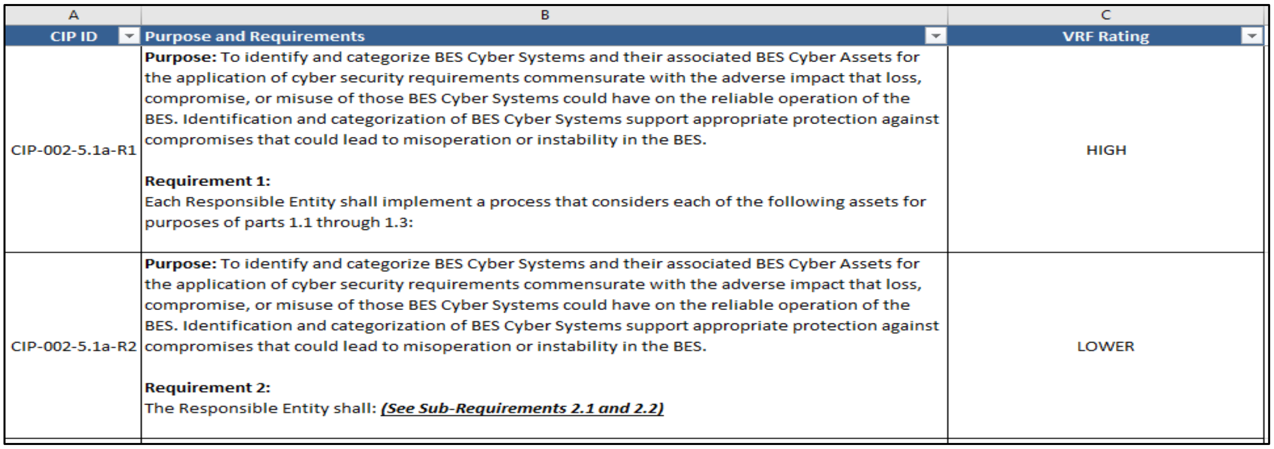


A	B	C	D	E	F	G	H	I
	CIP	NIST CSF	CSF ID	NIST-CSF Category	NIST CSF ID	NIST-CSF Sub-Category	Cybersecurity	Risk Tier
CIPv5 ID	Requirement and Parts	*Function*	*Cat*	*Objectives*	*Sub-cat*	*Outcomes*	*Risk Mgmt Tier*	*Descriptor*
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-01	Physical devices and systems within the organization are inventoried	1	Partial
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-02	Software platforms and applications within the organization are inventoried	4	Adaptive

Figure 3: Self-Assessment Tab

- **CIP Standards Tab** (see **Figure 4**)**:** is a compilation of the current effective CIP standards subject to enforcement, as posted on the NERC CIP Standards site.

Note: normalized/standardized IDs ~~in Column A~~ were created in order to facilitate linkage between the various tabs, filtering, and ~~pivot table~~Pivot Table capabilities

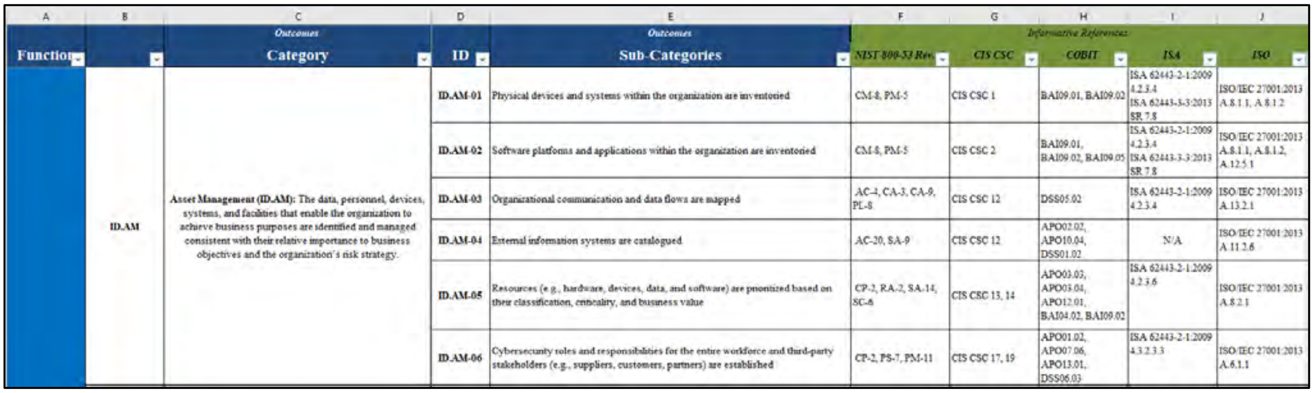


A	B	C
CIP ID	Purpose and Requirements	VRF Rating
CIP-002-5.1a-R1	**Purpose:** To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. **Requirement 1:** Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	HIGH
CIP-002-5.1a-R2	**Purpose:** To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. **Requirement 2:** The Responsible Entity shall: ***(See Sub-Requirements 2.1 and 2.2)***	LOWER

Figure 4: CIP Standards Tab

- **Cyber Security Framework Tab (see Figure 5):** contains a modified download of the Excel file available from the framework site[6]. The only modification was to place the informative references into individual columns as opposed to including them all in a single cell for each sub-category.

  Note: normalized/standardized IDs were created in order to facilitate linkage between the various tabs, filtering, and Pivot Table capabilities



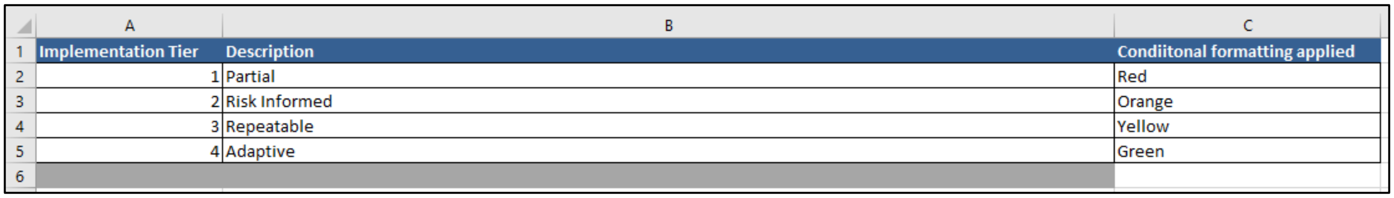
A	B	C	D	E	F	G	H	I	J
		Outcomes		*Outcomes*	*Informative References*				
Function		Category	ID	Sub-Categories	*NIST 800-53 Rev.*	*CIS CSC*	*COBIT*	*ISA*	*ISO*
	ID.AM	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-01	Physical devices and systems within the organization are inventoried	CM-8, PM-5	CIS CSC 1	BAI09.01, BAI09.02	ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8	ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
			ID.AM-02	Software platforms and applications within the organization are inventoried	CM-8, PM-5	CIS CSC 2	BAI09.01, BAI09.02, BAI09.05	ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8	ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1
			ID.AM-03	Organizational communication and data flows are mapped	AC-4, CA-3, CA-9, PL-8	CIS CSC 12	DSS05.02	ISA 62443-2-1:2009 4.2.3.4	ISO/IEC 27001:2013 A.13.2.1
			ID.AM-04	External information systems are catalogued	AC-20, SA-9	CIS CSC 12	APO02.02, APO10.04, DSS01.02	N/A	ISO/IEC 27001:2013 A.11.2.6
			ID.AM-05	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, SA-14, SC-6	CIS CSC 13, 14	APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02	ISA 62443-2-1:2009 4.2.3.6	ISO/IEC 27001:2013 A.8.2.1
			ID.AM-06	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CP-2, PS-7, PM-11	CIS CSC 17, 19	APO01.02, APO07.06, APO13.01, DSS06.03	ISA 62443-2-1:2009 4.3.2.3.3	ISO/IEC 27001:2013 A.6.1.1

Figure 5: Cyber Security Framework Tab

- **Data validation Values (see Figure 6):** primarily for lookup and Excel "named references" purposes used throughout the workbook:
  - **Customization:** cells B2–B5 are unlocked, if a responsible entity does not like the Risk Implementation Tiers as provided by the framework. Changing those to whatever an entity prefers, will automatically update the corresponding values on the other sheets.

[6] https://www.nist.gov/cyberframework/framework

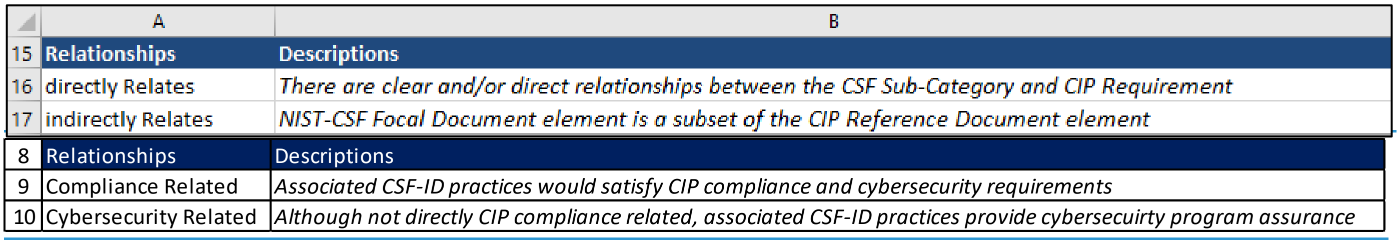
Note: Cells C2–C5 are for reference purposes only, describing the conditional formatting colors used on the Implementation Dashboard corresponding to the associated Implementation Tier #.



	A	B	C
1	Implementation Tier	Description	Condiitonal formatting applied
2	1	Partial	Red
3	2	Risk Informed	Orange
4	3	Repeatable	Yellow
5	4	Adaptive	Green
6			

Figure 6: Data Validation Values tab: Customization #1

- **Customization (see Figure 7)**: cells A9~~16~~ and A13~~7~~ are unlocked if a responsible entity wishes to use different text to describe.



	A	B
15	Relationships	Descriptions
16	directly Relates	*There are clear and/or direct relationships between the CSF Sub-Category and CIP Requirement*
17	indirectly Relates	*NIST-CSF Focal Document element is a subset of the CIP Reference Document element*

8	Relationships	Descriptions
9	Compliance Related	*Associated CSF-ID practices would satisfy CIP compliance and cybersecurity requirements*
10	Cybersecurity Related	*Although not directly CIP compliance related, associated CSF-ID practices provide cybersecuirty program assurance*

Figure 7: Data Validation Values tab: Customization #2

Design Assumptions

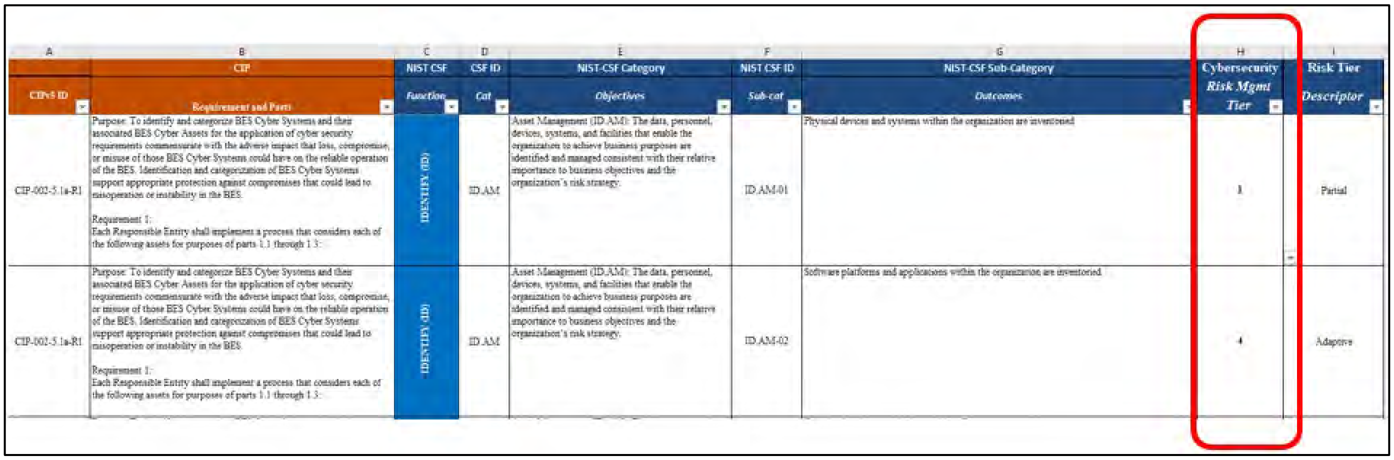
- Each responsible entity will have implemented their own security controls that are often based on the same security guidance identified in the framework informative references.
- Generally, there are separate CIP requirement~~s~~ owners assigned within responsible entity companies and usually develop associated policies, controls, and/or practices.
- By providing a cross-mapping of the CIP standards to the framework sub-categories, requirement owners can view the associated informative reference practices to compare their implemented security controls against.
- The Implementation Dashboard tab summary results will help identify gaps and/or improvement opportunities.

Self-Assessment Tab Instructions (see Figure 8)

1. Either distribute the self-assessment tool spreadsheet to individual CIP requirement owners or gather all CIP requirement owners together to collectively review and assess their associated requirement implementation level.

2. CIP requirement owners review each of their associated CIP requirements and select the risk implementation level from the available drop-down number in Column H (Cybersecurity Risk Management Tier) that best represents their current practice implementation level.

3. Once completed, move on to review summary results in the Implementation Dashboard tab.



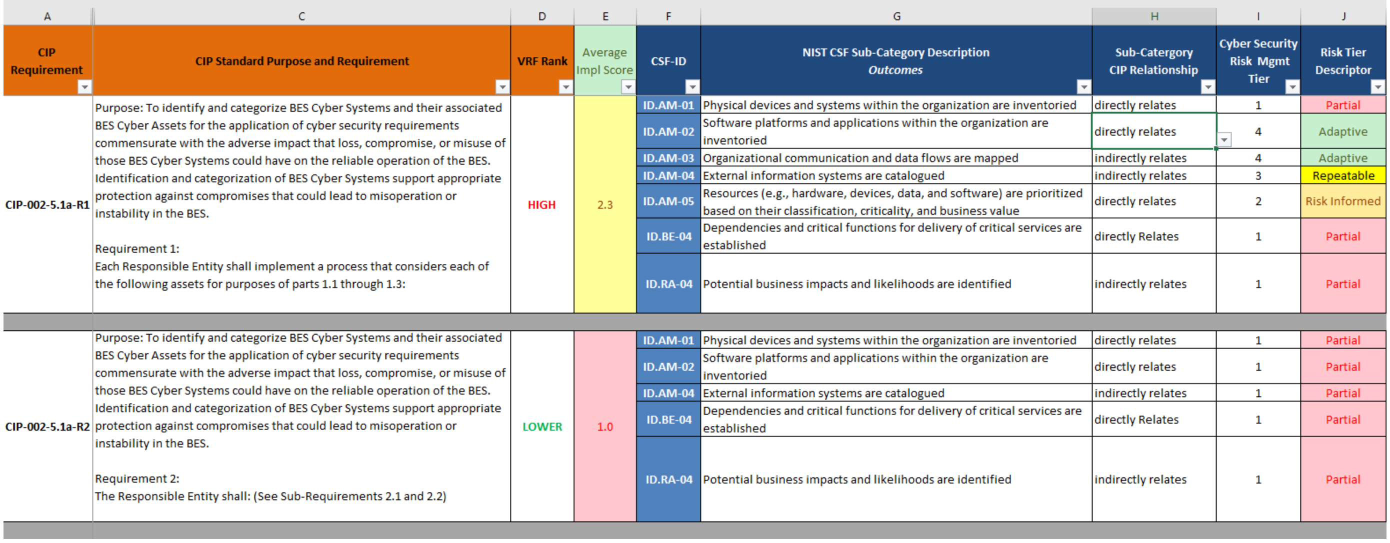
A	B	C	D	E	F	G	H	I
	CIP	NIST CSF	CSF ID	NIST-CSF Category	NIST CSF ID	NIST-CSF Sub-Category	Cybersecurity	Risk Tier
CIPv5 ID	Requirement and Parts	*Function*	*Cat*	*Objectives*	*Sub-cat*	*Outcomes*	*Risk Mgmt Tier*	*Descriptor*
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-01	Physical devices and systems within the organization are inventoried	1	Partial
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-02	Software platforms and applications within the organization are inventoried	4	Adaptive

Figure 8: Completing Self-Assessment tab

Implementation Dashboard potential Use Cases:

After all rows in the Self-Assessment tab (see **Figure 9**) have been completed, the implementation dashboard will represent the summary risk results by CIP requirement to highlight the following:

- Identify where there may be **CIP Violation** risks based on the VRF rank value in Column D and the corresponding “A~~a~~verage I~~i~~mpl~~y~~ S~~s~~core” in Column E
- Identify where there may be **Compliance** risks, based on the “Directly Relates” relationship in Column H and a corresponding low implementation level in Column J
- Identify where there may be **Security** risks, based on the “Indirectly Relates” relationship in Column H and a corresponding low implementation level in Column J



A	C	D	E	F	G	H	I	J
CIP Requirement	CIP Standard Purpose and Requirement	VRF Rank	Average Impl Score	CSF-ID	NIST CSF Sub-Category Description *Outcomes*	Sub-Catergory CIP Relationship	Cyber Security Risk Mgmt Tier	Risk Tier Descriptor
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	HIGH	2.3	ID.AM-01	Physical devices and systems within the organization are inventoried	directly relates	1	Partial
				ID.AM-02	Software platforms and applications within the organization are inventoried	directly relates	4	Adaptive
				ID.AM-03	Organizational communication and data flows are mapped	indirectly relates	4	Adaptive
				ID.AM-04	External information systems are catalogued	indirectly relates	3	Repeatable
				ID.AM-05	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	directly relates	2	Risk Informed
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	directly Relates	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	indirectly relates	1	Partial
CIP-002-5.1a-R2	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 2: The Responsible Entity shall: (See Sub-Requirements 2.1 and 2.2)	LOWER	1.0	ID.AM-01	Physical devices and systems within the organization are inventoried	directly relates	1	Partial
				ID.AM-02	Software platforms and applications within the organization are inventoried	directly relates	1	Partial
				ID.AM-04	External information systems are catalogued	indirectly relates	1	Partial
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	directly Relates	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	indirectly relates	1	Partial

Figure 9: Review Self-Assessment Results

References

- NIST Cybersecurity Framework 1.1: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NERC CIP Enforceable Standards: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- Mapping of NIST Cybersecurity Framework to NERC CIP v3/v5 November 2014 - https://www.nerc.com/comm/CIPC_Security_Guidelines_DL/CSSWG-Mapping_of_NIST_Cybersecurity_Framework_to_NERC_CIP.pdf
- Mapping of CIP Standards to NIST Cybersecurity Framework v1.1 Updated: https://www.nerc.com/pa/comp/Pages/CAOneStopShop.aspx (under Compliance | NIST)
- FERC NOPR 12-17-2020 Incentives Effort - E-2-RM21-3-000 | Federal Energy Regulatory Commission (ferc.gov)

Version History

SWG Security and Compliant Guidance Version History					
Version No.	Date	Chapter	Page	Description	Version
1	October 2020	All	All	Original Document	.1
2	November 12, 2020	All	All	Publications and Admin review complete	.2
3	June 2021	All	All	Approved by the RSTC	1.0

The NERC Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups, develops and triennially reviews reliability guidelines in accordance with the procedures set forth in the RSTC Charter. Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that impact bulk power system (BPS) operations, planning, and security. Reliability guidelines provide key practices, guidance, and information on specific issues critical to promote and maintain a highly reliable and secure BPS.

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining

Disclaimer - The objective of this tool is to distribute key practices and information on specific issues critical to promote and maintain a highly reliable and secure bulk power system (BPS). Security Guidelines are not binding norms or parameters to the level that compliance to NERC's Reliability

Intended Use

This spreadsheet is meant to be a "**Security and Compliance**" Self-Assessment tool for CIP Requirement Owners within Responsible Entity companies

Self-Assessment Results will be displayed on the "Implementation Dashboard" tab

Results are intended to help guide two use cases:

- Annual Budget and Prioritization improvement justification
- Develop a multiyear improvement roadmap

Suggest proceeding in this order

1. Required - Read all the Information on this tab

2. Optional - Familiarize yourself with the Implementation Tier Short Descriptions on the data_validation_values tab (you may want to have them printed out); customize descriptors in B2:B5 if desired.

3. Optional - If you are not intimately familiar with the CIP Requirements, spend some time on the CIP Standards tab and/or reviewing the NERC Standards at the link below

4. Optional - If you would like to see how Industry security standards map into this effort, use the Cyber Security Framework tab for a number of Informative References

5. Required - Perform the self-assessment, by selecting the value in Column I on the Self-Assessment tab that best describe your current Cybersecurity and Compliance Implementation Levels

6. Optional - If you would like to change the provided CSF-ID to CIP relationships on the Self-Assessment tab, select the available option from the associated drop down list

>> you also have the option to change and/or add additional relationships that best reflect your organizational requirements on the data_validation_values tab in cells B16:B20

6. Required - Review your results on the Implementation Dashboard tab

>> Low implementation level scores in column E or I = higher risk

7. Optional - Potential use cases of completed results on the Information Dashboard tab

>> CIP Violation Risk Factor focus – filter on Column D (VRF) to identify VRF with a Low average implementation scores in Column E, to identify potential CIP Violation Risk Factor compliance improvement opportunities

>> CIP Compliance focus – filter on Column H (CSF-IT to CIP Relationship) for “Compliance related” relationships (or your equivalent alternative you may have added), to identify potential CIP compliance improvement opportunities based on associated Risk Implementation Tier noted in columns I & J

>> Cybersecurity focus - filter on Column H (CSF-IT to CIP Relationship) for “Cyberseucrity related” relationships (or your equivalent alternative you may have added), to identify

See Companion Guideline document for fuller, more detailed Instructions and background (link will be included once a final document is approved)

See Background Information tab for additional information such as - Intended Benefits, Tab Descriptions, Assumptions, Allowable Customizations, Dashboard Use Cases

NERC CIP Standards - https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (under the "Critical Information Protection" | "Subject to enforcement" sections)

NIST Cyber Security Framework - https://www.nist.gov/cyberframework (under the "Framework" section)

CIP Requirement	CIP Standard Purpose and Requirement	VRF Rank	Average Impl Score	CSF-ID	NIST CSF Sub-Category Description *Outcomes*	CSF-ID to CIP Relationship	Cyber Security Risk Mgmt Tier	Risk Tier Descriptor
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	**HIGH**	2.1	**ID.AM-01**	Physical devices and systems within the organization are inventoried	Compliance Related	2	Risk Informed
				ID.AM-02	Software platforms and applications within the organization are inventoried	Compliance Related	3	Repeatable
				ID.AM-03	Organizational communication and data flows are mapped	Compliance Related	4	Adaptive
				ID.AM-04	External information systems are catalogued	Cybersecurity Related	2	Risk Informed
				ID.AM-05	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Compliance Related	2	Risk Informed
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	Compliance Related	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	Cybersecurity Related	1	Partial
CIP-002-5.1a-R2	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 2: The Responsible Entity shall: (See Sub-Requirements 2.1 and 2.2)	**LOWER**	1.0	**ID.AM-01**	Physical devices and systems within the organization are inventoried	Compliance Related	1	Partial
				ID.AM-02	Software platforms and applications within the organization are inventoried	Compliance Related	1	Partial
				ID.AM-04	External information systems are catalogued	Cybersecurity Related	1	Partial
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	Compliance Related	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	Cybersecurity Related	1	Partial
CIP-003-8-R1	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: (See Sub-Requirements 1.1 and 1.2)	**MEDIUM**	2.5	**ID.GV-01**	Organizational information security policy is established and communicated	Compliance Related	4	Adaptive
				PR.IP-05	Policy and regulations regarding the physical operating environment for organizational assets are met	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low	**LOWER**	1.0	**DE.AE-02**	Detected events are analyzed to understand attack targets and methods	Compliance Related	1	Partial
				DE.AE-04	Impact of events is determined	Compliance Related	1	Partial
				DE.CM-02	The physical environment is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
				DE.CM-04	Malicious code is detected	Compliance Related	1	Partial
				DE.CM-05	Unauthorized mobile code is detected	Cybersecurity Related	1	Partial
				DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Compliance Related	1	Partial
				DE.DP-01	Roles and responsibilities for detection are well defined to ensure accountability	Cybersecurity Related	1	Partial
				DE.DP-02	Detection activities comply with all applicable requirements	Compliance Related	1	Partial
				DE.DP-03	Detection processes are tested	Compliance Related	1	Partial
				DE.DP-04	Event detection information is communicated	Compliance Related	1	Partial
				DE.DP-05	Detection processes are continuously improved	Compliance Related	1	Partial
				ID.GV-01	Organizational information security policy is established and communicated	Compliance Related	1	Partial
				PR.AC-01	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	Cybersecurity Related	1	Partial
				PR.AC-02	Physical access to assets is managed and protected	Compliance Related	1	Partial
				PR.AC-03	Remote access is managed	Cybersecurity Related	1	Partial
				PR.AT-01	All users are informed and trained	Cybersecurity Related	1	Partial
				PR.AT-02	Privileged users understand roles & responsibilities	Cybersecurity Related	1	Partial

	impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.			**PR.AT-03**	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Cybersecurity Related	1	Partial
				PR.AT-04	Senior executives understand their roles & responsibilities	Cybersecurity Related	1	Partial
				PR.AT-05	Physical and cybersecurity personnel understand their roles and responsibilities	Cybersecurity Related	1	Partial
				PR.DS-02	Data-in-transit is protected	Cybersecurity Related	1	Partial
				PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Compliance Related	1	Partial
				PR.PT-02	Removable media is protected and its use restricted according to policy	Compliance Related	1	Partial
				RS.AN-01	Notifications from detection systems are investigated	Compliance Related	1	Partial
				RS.AN-03	Forensics are performed	Cybersecurity Related	1	Partial
				RS.AN-04	Incidents are categorized consistent with response plans	Compliance Related	1	Partial
				RS.CO-02	Incidents are reported consistent with established criteria	Compliance Related	1	Partial
				RS.CO-03	Information is shared consistent with response plans	Compliance Related	1	Partial
				RS.CO-04	Coordination with stakeholders occurs consistent with response plans	Compliance Related	1	Partial
				RS.IM-01	Response plans incorporate lessons learned	Compliance Related	1	Partial
				RS.IM-02	Response strategies are updated	Compliance Related	1	Partial
				RS.MI-01	Incidents are contained	Compliance Related	1	Partial
				RS.MI-02	Incidents are mitigated	Compliance Related	1	Partial
CIP-003-8-R3	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.	**MEDIUM**	1.0	**DE.DP-01**	Roles and responsibilities for detection are well defined to ensure accountability	Cybersecurity Related	1	Partial
				ID.AM-06	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Cybersecurity Related	1	Partial
				ID.GV-02	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	Cybersecurity Related	1	Partial
				PR.AT-04	Senior executives understand their roles & responsibilities	Cybersecurity Related	1	Partial
CIP-003-8-R4	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	**LOWER**	1.0	**DE.DP-01**	Roles and responsibilities for detection are well defined to ensure accountability	Cybersecurity Related	1	Partial
				ID.AM-06	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Cybersecurity Related	1	Partial
				ID.GV-02	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	Cybersecurity Related	1	Partial
				PR.AT-04	Senior executives understand their roles & responsibilities	Cybersecurity Related	1	Partial
CIP-004-6-R1	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-6 Table R1 – Security Awareness Program.	**LOWER**	1.0	**PR.AT-01**	All users are informed and trained	Cybersecurity Related	1	Partial
				PR.AT-02	Privileged users understand roles & responsibilities	Cybersecurity Related	1	Partial
				PR.AT-03	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Cybersecurity Related	1	Partial
				PR.AT-04	Senior executives understand their roles & responsibilities	Cybersecurity Related	1	Partial
				PR.AT-05	Physical and cybersecurity personnel understand their roles and responsibilities	Cybersecurity Related	1	Partial

CIP-004-6-R2	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.	**LOWER**	1.0	**ID.AM-06**	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Compliance Related	1	Partial
				ID.BE-03	Priorities for organizational mission, objectives, and activities are established and communicated	Compliance Related	1	Partial
				ID.GV-01	Organizational information security policy is established and communicated	Compliance Related	1	Partial
				PR.AT-01	All users are informed and trained	Compliance Related	1	Partial
				PR.AT-02	Privileged users understand roles & responsibilities	Compliance Related	1	Partial
				PR.AT-03	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Compliance Related	1	Partial
				PR.AT-04	Senior executives understand their roles & responsibilities	Compliance Related	1	Partial
				PR.AT-05	Physical and cybersecurity personnel understand their roles and responsibilities	Compliance Related	1	Partial
				PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Cybersecurity Related	1	Partial
CIP-004-6-R3	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 3: Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-6 Table R3 – Personnel Risk Assessment Program.	**MEDIUM**	1.0	**PR.AC-06**	Identities are proofed and bound to credentials and asserted in interactions	Compliance Related	1	Partial
				PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Cybersecurity Related	1	Partial
CIP-004-6-R4	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 4: Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.	**MEDIUM**	1.0	**ID.AM-06**	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Cybersecurity Related	1	Partial
				PR.AC-01	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	Compliance Related	1	Partial
				PR.AC-02	Physical access to assets is managed and protected	Compliance Related	1	Partial
				PR.AC-03	Remote access is managed	Cybersecurity Related	1	Partial
				PR.AC-04	Access permissions are managed, incorporating the principles of least privilege and separation of duties	Compliance Related	1	Partial
				PR.DS-01	Data-at-rest is protected	Cybersecurity Related	1	Partial
				PR.DS-02	Data-in-transit is protected	Cybersecurity Related	1	Partial
				PR.DS-05	Protections against data leaks are implemented	Cybersecurity Related	1	Partial
				PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Cybersecurity Related	1	Partial
CIP-004-6-R5	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 5: Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.	**MEDIUM**	1.0	**PR.AC-01**	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	Compliance Related	1	Partial
				PR.AC-02	Physical access to assets is managed and protected	Compliance Related	1	Partial
				PR.AC-03	Remote access is managed	Compliance Related	1	Partial
				PR.AC-04	Access permissions are managed, incorporating the principles of least privilege and separation of duties	Compliance Related	1	Partial
				PR.DS-01	Data-at-rest is protected	Cybersecurity Related	1	Partial
				PR.DS-02	Data-in-transit is protected	Cybersecurity Related	1	Partial
				PR.DS-05	Protections against data leaks are implemented	Cybersecurity Related	1	Partial
				PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Cybersecurity Related	1	Partial
				DE.AE-02	Detected events are analyzed to understand attack targets and methods	Cybersecurity Related	1	Partial

CIP-005-5-R1	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	**MEDIUM**	1.0	**DE.CM-01**	The network is monitored to detect potential cybersecurity events	Cybersecurity Related	1	Partial
				DE.CM-06	External service provider activity is monitored to detect potential cybersecurity events	Cybersecurity Related	1	Partial
				DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Compliance Related	1	Partial
				ID.AM-04	External information systems are catalogued	Compliance Related	1	Partial
				PR.AC-03	Remote access is managed	Compliance Related	1	Partial
				PR.AC-05	Network integrity is protected, incorporating network segregation where appropriate	Compliance Related	1	Partial
				PR.AC-07	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Cybersecurity Related	1	Partial
				PR.DS-02	Data-in-transit is protected	Cybersecurity Related	1	Partial
				PR.DS-05	Protections against data leaks are implemented	Cybersecurity Related	1	Partial
				PR.DS-07	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Compliance Related	1	Partial
				PR.PT-04	Communications and control networks are protected	Cybersecurity Related	1	Partial
CIP-005-5-R2	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.	**MEDIUM**	1.0	**DE.CM-06**	External service provider activity is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
				ID.AM-03	Organizational communication and data flows are mapped	Compliance Related	1	Partial
				PR.AC-03	Remote access is managed	Cybersecurity Related	1	Partial
				PR.AC-04	Access permissions are managed, incorporating the principles of least privilege and separation of duties	Compliance Related	1	Partial
				PR.AC-07	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Cybersecurity Related	1	Partial
				PR.DS-02	Data-in-transit is protected	Cybersecurity Related	1	Partial
				PR.DS-05	Protections against data leaks are implemented	Cybersecurity Related	1	Partial
				PR.MA-02	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Cybersecurity Related	1	Partial
				PR.PT-04	Communications and control networks are protected	Compliance Related	1	Partial
CIP-006-6-R1	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.	**MEDIUM**	1.0	**DE.CM-02**	The physical environment is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
				DE.CM-03	Personnel activity is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
				DE.CM-06	External service provider activity is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
				DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Compliance Related	1	Partial
				PR.AC-02	Physical access to assets is managed and protected	Compliance Related	1	Partial
				PR.PT-01	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Compliance Related	1	Partial
				PR.PT-04	Communications and control networks are protected	Cybersecurity Related	1	Partial
CIP-006-6-R2	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program.	**MEDIUM**	1.0	**DE.CM-02**	The physical environment is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
				PR.AC-02	Physical access to assets is managed and protected	Compliance Related	1	Partial
				PR.AT-05	Physical and cybersecurity personnel understand their roles and responsibilities	Compliance Related	1	Partial
				PR.PT-01	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Cybersecurity Related	1	Partial
	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems			**DE.DP-03**	Detection processes are tested	Cybersecurity Related	1	Partial

CIP-006-6-R3	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 3: Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in CIP-006-6 Table R3 – Maintenance and Testing Program.	**MEDIUM**	1.0	**PR.MA-01**	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	Compliance Related	1	Partial
				PR.MA-02	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Compliance Related	1	Partial
CIP-007-6-R1	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services.	**MEDIUM**	1.0	**PR.AC-02**	Physical access to assets is managed and protected	Compliance Related	1	Partial
				PR.PT-02	Removable media is protected and its use restricted according to policy	Compliance Related	1	Partial
				PR.PT-03	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Compliance Related	1	Partial
CIP-007-6-R2	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.	**MEDIUM**	1.0	**ID.RA-01**	Asset vulnerabilities are identified and documented	Compliance Related	1	Partial
				ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	Compliance Related	1	Partial
				ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Compliance Related	1	Partial
				ID.RA-06	Risk responses are identified and prioritized	Compliance Related	1	Partial
				PR.IP-03	Configuration change control processes are in place	Cybersecurity Related	1	Partial
				PR.IP-12	A vulnerability management plan is developed and implemented	Cybersecurity Related	1	Partial
				RS.AN-05	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	Compliance Related	1	Partial
				RS.MI-03	Newly identified vulnerabilities are mitigated or documented as accepted risks	Compliance Related	1	Partial
CIP-007-6-R3	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that	**MEDIUM**	1.0	**DE.CM-04**	Malicious code is detected	Cybersecurity Related	1	Partial
				DE.CM-05	Unauthorized mobile code is detected	Compliance Related	1	Partial
				DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Cybersecurity Related	1	Partial
				DE.DP-02	Detection activities comply with all applicable requirements	Compliance Related	1	Partial
				PR.DS-05	Protections against data leaks are implemented	Compliance Related	1	Partial
				PR.IP-12	A vulnerability management plan is developed and implemented	Cybersecurity Related	1	Partial
CIP-007-6-R4	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	**MEDIUM**	1.0	**DE.AE-02**	Detected events are analyzed to understand attack targets and methods	Compliance Related	1	Partial
				DE.AE-03	Event data are collected and correlated from multiple sources and sensors	Compliance Related	1	Partial
				DE.AE-05	Incident alert thresholds are established	Compliance Related	1	Partial
				DE.CM-03	Personnel activity is monitored to detect potential cybersecurity events	Cybersecurity Related	1	Partial
				DE.CM-04	Malicious code is detected	Compliance Related	1	Partial
				DE.CM-06	External service provider activity is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
				DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Cybersecurity Related	1	Partial
				DE.DP-02	Detection activities comply with all applicable requirements	Compliance Related	1	Partial
				ID.RA-03	Threats, both internal and external, are identified and documented	Compliance Related	1	Partial
				PR.DS-05	Protections against data leaks are implemented	Compliance Related	1	Partial
				PR.PT-01	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Compliance Related	1	Partial
				DE.AE-05	Incident alert thresholds are established	Compliance Related	1	Partial

CIP-007-6-R5	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 5: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.	MEDIUM	1.0	DE.CM-03	Personnel activity is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
				DE.CM-06	External service provider activity is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
				DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Cybersecurity Related	1	Partial
				PR.AC-01	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	Compliance Related	1	Partial
				PR.AC-04	Access permissions are managed, incorporating the principles of least privilege and separation of duties	Compliance Related	1	Partial
				PR.AC-07	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Compliance Related	1	Partial
				PR.DS-05	Protections against data leaks are implemented	Cybersecurity Related	1	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	LOWER	1.0	DE.AE-02	Detected events are analyzed to understand attack targets and methods	Compliance Related	1	Partial
				DE.AE-04	Impact of events is determined	Compliance Related	1	Partial
				DE.AE-05	Incident alert thresholds are established	Compliance Related	1	Partial
				DE.DP-01	Roles and responsibilities for detection are well defined to ensure accountability	Cybersecurity Related	1	Partial
				DE.DP-02	Detection activities comply with all applicable requirements	Compliance Related	1	Partial
				DE.DP-04	Event detection information is communicated	Compliance Related	1	Partial
				ID.BE-05	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	Compliance Related	1	Partial
				ID.RA-06	Risk responses are identified and prioritized	Compliance Related	1	Partial
				PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Compliance Related	1	Partial
				RS.AN-01	Notifications from detection systems are investigated	Compliance Related	1	Partial
				RS.AN-02	The impact of the incident is understood	Compliance Related	1	Partial
				RS.AN-03	Forensics are performed	Cybersecurity Related	1	Partial
				RS.AN-04	Incidents are categorized consistent with response plans	Compliance Related	1	Partial
				RS.CO-01	Personnel know their roles and order of operations when a response is needed	Compliance Related	1	Partial
				RS.CO-02	Incidents are reported consistent with established criteria	Compliance Related	1	Partial
				RS.CO-03	Information is shared consistent with response plans	Compliance Related	1	Partial
				RS.CO-04	Coordination with stakeholders occurs consistent with response plans	Compliance Related	1	Partial
				RS.MI-01	Incidents are contained	Compliance Related	1	Partial
				RS.MI-02	Incidents are mitigated	Compliance Related	1	Partial
CIP-008-5-R2	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 2: Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.	LOWER	1.0	DE.AE-02	Detected events are analyzed to understand attack targets and methods	Compliance Related	1	Partial
				DE.DP-03	Detection processes are tested	Compliance Related	1	Partial
				PR.IP-10	Response and recovery plans are tested	Cybersecurity Related	1	Partial
				RS.AN-01	Notifications from detection systems are investigated	Cybersecurity Related	1	Partial
				RS.AN-02	The impact of the incident is understood	Cybersecurity Related	1	Partial
				RS.CO-02	Incidents are reported consistent with established criteria	Cybersecurity Related	1	Partial
				RS.CO-03	Information is shared consistent with response plans	Cybersecurity Related	1	Partial
				RS.CO-04	Coordination with stakeholders occurs consistent with response plans	Cybersecurity Related	1	Partial
				RS.RP-01	Response plan is executed during or after an event	Cybersecurity Related	1	Partial
CIP-008-5-R3	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 3: Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.	LOWER	1.0	DE.DP-05	Detection processes are continuously improved	Compliance Related	1	Partial
				PR.IP-07	Protection processes are improved	Compliance Related	1	Partial
				PR.IP-08	Effectiveness of protection technologies is shared	Compliance Related	1	Partial
				PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Compliance Related	1	Partial
				RS.CO-01	Personnel know their roles and order of operations when a response is needed	Compliance Related	1	Partial
				RS.IM-01	Response plans incorporate lessons learned	Compliance Related	1	Partial
				RS.IM-02	Response strategies are updated	Compliance Related	1	Partial

CIP-009-6-R1	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 1: Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications.	**MEDIUM**	1.0	**ID.BE-05**	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	Compliance Related	1	Partial
				PR.DS-04	Adequate capacity to ensure availability is maintained	Compliance Related	1	Partial
				PR.IP-04	Backups of information are conducted, maintained, and tested	Compliance Related	1	Partial
				PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Compliance Related	1	Partial
				RC.RP-01	Recovery plan is executed during or after an cybersecurity incident	Compliance Related	1	Partial
				RS.AN-03	Forensics are performed	Compliance Related	1	Partial
CIP-009-6-R2	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.	**LOWER**	1.0	**PR.IP-04**	Backups of information are conducted, maintained, and tested	Compliance Related	1	Partial
				PR.IP-10	Response and recovery plans are tested	Compliance Related	1	Partial
				RC.RP-01	Recovery plan is executed during or after an cybersecurity incident	Compliance Related	1	Partial
CIP-009-6-R3	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 3: Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.	**LOWER**	1.0	**PR.IP-07**	Protection processes are improved	Compliance Related	1	Partial
				PR.IP-08	Effectiveness of protection technologies is shared	Compliance Related	1	Partial
				PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Compliance Related	1	Partial
				RC.CO-03	Recovery activities are communicated to internal stakeholders and executive and management teams	Compliance Related	1	Partial
				RC.IM-01	Recovery plans incorporate lessons learned	Compliance Related	1	Partial
				RC.IM-02	Recovery strategies are updated	Compliance Related	1	Partial
CIP-010-2-R1	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.	**MEDIUM**	1.0	**DE.CM-05**	Unauthorized mobile code is detected	Cybersecurity Related	1	Partial
				PR.DS-06	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Compliance Related	1	Partial
				PR.DS-07	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Compliance Related	1	Partial
				PR.IP-01	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	Compliance Related	1	Partial
				PR.IP-03	Configuration change control processes are in place	Compliance Related	1	Partial
				PR.MA-01	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	Compliance Related	1	Partial
				PR.MA-02	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Compliance Related	1	Partial
				PR.PT-03	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Cybersecurity Related	1	Partial
	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that			**PR.DS-06**	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Compliance Related	1	Partial
				PR.IP-01	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	Compliance Related	1	Partial

CIP-010-2-R2	could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R2 – Configuration Monitoring.	MEDIUM	1.0	PR.IP-03	Configuration change control processes are in place	Compliance Related	1	Partial
CIP-010-2-R3	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R3– Vulnerability Assessments.	MEDIUM	1.0	DE.CM-08	Vulnerability scans are performed	Compliance Related	1	Partial
				ID.RA-01	Asset vulnerabilities are identified and documented	Compliance Related	1	Partial
				ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Compliance Related	1	Partial
				ID.RA-06	Risk responses are identified and prioritized	Compliance Related	1	Partial
				PR.IP-12	A vulnerability management plan is developed and implemented	Compliance Related	1	Partial
				RS.AN-05	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	Compliance Related	1	Partial
				RS.MI-03	Newly identified vulnerabilities are mitigated or documented as accepted risks	Compliance Related	1	Partial
CIP-010-2-R4	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.	MEDIUM	1.0	DE.CM-04	Malicious code is detected	Compliance Related	1	Partial
				DE.CM-05	Unauthorized mobile code is detected	Compliance Related	1	Partial
				DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Compliance Related	1	Partial
				PR.PT-02	Removable media is protected and its use restricted according to policy	Compliance Related	1	Partial
				RS.AN-05	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	Compliance Related	1	Partial
				RS.MI-03	Newly identified vulnerabilities are mitigated or documented as accepted risks	Compliance Related	1	Partial
CIP-011-2-R1	Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-2 Table R1 – Information Protection.	MEDIUM	1.0	ID.AM-03	Organizational communication and data flows are mapped	Compliance Related	1	Partial
				PR.DS-01	Data-at-rest is protected	Compliance Related	1	Partial
				PR.DS-02	Data-in-transit is protected	Compliance Related	1	Partial
				PR.DS-05	Protections against data leaks are implemented	Compliance Related	1	Partial
				PR.DS-06	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Compliance Related	1	Partial
CIP-011-2-R2	Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal.	LOWER	1.0	PR.DS-01	Data-at-rest is protected	Compliance Related	1	Partial
				PR.DS-03	Assets are formally managed throughout removal, transfers, and disposition	Compliance Related	1	Partial
				PR.DS-05	Protections against data leaks are implemented	Compliance Related	1	Partial
				PR.IP-06	Data is destroyed according to policy	Compliance Related	1	Partial

CIP-012-1-R1	Purpose: To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers. Requirement 1: The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. (See Sub-Requirements 1.1 through 1.3)	**MEDIUM**	1.0	**PR.IP-01**	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	**MEDIUM**	1.0	**DE.CM-06**	External service provider activity is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
				ID.BE-01	The organization's role in the supply chain is identified and communicated	Compliance Related	1	Partial
				ID.BE-02	The organization's place in critical infrastructure and its industry sector is identified and communicated	Compliance Related	1	Partial
				ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Compliance Related	1	Partial
				ID.RA-06	Risk responses are identified and prioritized	Compliance Related	1	Partial
				ID.RM-01	Risk management processes are established, managed, and agreed to by organizational stakeholders	Compliance Related	1	Partial
				ID.SC-01	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Compliance Related	1	Partial
				ID.SC-02	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	Compliance Related	1	Partial
				ID.SC-03	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	Compliance Related	1	Partial
				ID.SC-04	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	Compliance Related	1	Partial
				ID.SC-05	Response and recovery planning and testing are conducted with suppliers and third-party providers	Compliance Related	1	Partial
				PR.AC-03	Remote access is managed	Compliance Related	1	Partial
				PR.AC-04	Access permissions are managed, incorporating the principles of least privilege and separation of duties	Compliance Related	1	Partial
				PR.AT-03	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Compliance Related	1	Partial
				PR.DS-06	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Compliance Related	1	Partial
				PR.DS-08	Integrity checking mechanisms are used to verify hardware integrity	Compliance Related	1	Partial
				PR.MA-02	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Compliance Related	1	Partial
CIP-013-1-R2	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. (See additional notes in this requirement)	**MEDIUM**	1.0	**ID.BE-01**	The organization's role in the supply chain is identified and communicated	Compliance Related	1	Partial
				ID.BE-02	The organization's place in critical infrastructure and its industry sector is identified and communicated	Compliance Related	1	Partial
				ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Compliance Related	1	Partial
				ID.SC-01	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Compliance Related	1	Partial
				ID.SC-02	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	Compliance Related	1	Partial

				ID.SC-03	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	Compliance Related	1	Partial
CIP-013-1-R3	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 3: Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.	**MEDIUM**	1.0	**ID.BE-01**	The organization's role in the supply chain is identified and communicated	Cybersecurity Related	1	Partial
				ID.BE-02	The organization's place in critical infrastructure and its industry sector is identified and communicated	Cybersecurity Related	1	Partial
				ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Cybersecurity Related	1	Partial
				ID.SC-01	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Cybersecurity Related	1	Partial
				ID.SC-02	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	Cybersecurity Related	1	Partial
				ID.SC-03	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	Cybersecurity Related	1	Partial
CIP-014-2-R5	Purpose: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. Requirement 5: Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). (See Sub-Requirements 5.1 through 5.4)	**HIGH**	1.0	**DE.CM-02**	The physical environment is monitored to detect potential cybersecurity events	Cybersecurity Related	1	Partial

	CIP	NIST CSF	CSF ID	NIST-CSF Category	NIST CSF ID	NIST-CSF Sub-Category	CSF-ID to CIP	Cybersecurity	Risk Tier
CIPv5 ID	Requirement and Parts	*Function*	*Cat*	*Objectives*	*Sub-cat*	*Outcomes*	*Relationship*	*Risk Mgmt Tier*	*Descriptor*
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-01	Physical devices and systems within the organization are inventoried	Compliance Related	2	Risk Informed
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-02	Software platforms and applications within the organization are inventoried	Compliance Related	3	Repeatable
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-03	Organizational communication and data flows are mapped	Compliance Related	4	Adaptive
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-04	External information systems are catalogued	Cybersecurity Related	2	Risk Informed
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-05	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Compliance Related	2	Risk Informed

CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.BE	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-04	Dependencies and critical functions for delivery of critical services are established	Compliance Related	1	Partial
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-04	Potential business impacts and likelihoods are identified	Cybersecurity Related	1	Partial
CIP-002-5.1a-R2	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 2: The Responsible Entity shall: (See Sub-Requirements 2.1 and 2.2)	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-01	Physical devices and systems within the organization are inventoried	Compliance Related	1	Partial
CIP-002-5.1a-R2	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 2: The Responsible Entity shall: (See Sub-Requirements 2.1 and 2.2)	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-02	Software platforms and applications within the organization are inventoried	Compliance Related	1	Partial
CIP-002-5.1a-R2	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 2: The Responsible Entity shall: (See Sub-Requirements 2.1 and 2.2)	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-04	External information systems are catalogued	Cybersecurity Related	1	Partial
CIP-002-5.1a-R2	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 2: The Responsible Entity shall: (See Sub-Requirements 2.1 and 2.2)	IDENTIFY (ID)	ID.BE	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-04	Dependencies and critical functions for delivery of critical services are established	Compliance Related	1	Partial

CIP-002-5.1a-R2	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 2: The Responsible Entity shall: (See Sub-Requirements 2.1 and 2.2)	IDENTIFY (ID)	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-04	Potential business impacts and likelihoods are identified	Cybersecurity Related	1	Partial
CIP-003-8-R1	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: (See Sub-Requirements 1.1 and 1.2)	IDENTIFY (ID)	ID.GV	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-01	Organizational information security policy is established and communicated	Compliance Related	4	Adaptive
CIP-003-8-R1	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: (See Sub-Requirements 1.1 and 1.2)	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-05	Policy and regulations regarding the physical operating environment for organizational assets are met	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	DETECT (DE)	DE.AE	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-02	Detected events are analyzed to understand attack targets and methods	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	DETECT (DE)	DE.AE	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-04	Impact of events is determined	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-02	The physical environment is monitored to detect potential cybersecurity events	Compliance Related	1	Partial

CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	**DETECT (DE)**	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-04	Malicious code is detected	Compliance Related	**1**	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	**DETECT (DE)**	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-05	Unauthorized mobile code is detected	Cybersecurity Related	**1**	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	**DETECT (DE)**	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Compliance Related	**1**	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	**DETECT (DE)**	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-01	Roles and responsibilities for detection are well defined to ensure accountability	Cybersecurity Related	**1**	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	**DETECT (DE)**	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-02	Detection activities comply with all applicable requirements	Compliance Related	**1**	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	**DETECT (DE)**	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-03	Detection processes are tested	Compliance Related	**1**	Partial

CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	DETECT (DE)	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-04	Event detection information is communicated	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	DETECT (DE)	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-05	Detection processes are continuously improved	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	IDENTIFY (ID)	ID.GV	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-01	Organizational information security policy is established and communicated	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-01	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	Cybersecurity Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-02	Physical access to assets is managed and protected	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-03	Remote access is managed	Cybersecurity Related	1	Partial

CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-01	All users are informed and trained	Cybersecurity Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-02	Privileged users understand roles & responsibilities	Cybersecurity Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-03	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Cybersecurity Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-04	Senior executives understand their roles & responsibilities	Cybersecurity Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-05	Physical and cybersecurity personnel understand their roles and responsibilities	Cybersecurity Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-02	Data-in-transit is protected	Cybersecurity Related	1	Partial

CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	PROTECT (PR)	PR.PT	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-02	Removable media is protected and its use restricted according to policy	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	RESPOND (RS)	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-01	Notifications from detection systems are investigated	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	RESPOND (RS)	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-03	Forensics are performed	Cybersecurity Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	RESPOND (RS)	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-04	Incidents are categorized consistent with response plans	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	RESPOND (RS)	RS.CO	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-02	Incidents are reported consistent with established criteria	Compliance Related	1	Partial

CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	RESPOND (RS)	RS.CO	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-03	Information is shared consistent with response plans	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	RESPOND (RS)	RS.CO	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-04	Coordination with stakeholders occurs consistent with response plans	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	RESPOND (RS)	RS.IM	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-01	Response plans incorporate lessons learned	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	RESPOND (RS)	RS.IM	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-02	Response strategies are updated	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	RESPOND (RS)	RS.MI	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-01	Incidents are contained	Compliance Related	1	Partial
CIP-003-8-R2	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	RESPOND (RS)	RS.MI	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-02	Incidents are mitigated	Compliance Related	1	Partial

CIP-003-8-R3	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-06	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Cybersecurity Related	1	Partial
CIP-003-8-R3	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.	IDENTIFY (ID)	ID.GV	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-02	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	Cybersecurity Related	1	Partial
CIP-003-8-R3	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.	DETECT (DE)	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-01	Roles and responsibilities for detection are well defined to ensure accountability	Cybersecurity Related	1	Partial
CIP-003-8-R3	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-04	Senior executives understand their roles & responsibilities	Cybersecurity Related	1	Partial
CIP-003-8-R4	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-06	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Cybersecurity Related	1	Partial
CIP-003-8-R4	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	IDENTIFY (ID)	ID.GV	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-02	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	Cybersecurity Related	1	Partial

CIP-003-8-R4	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	**DETECT (DE)**	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-01	Roles and responsibilities for detection are well defined to ensure accountability	Cybersecurity Related	**1**	Partial
CIP-003-8-R4	Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	**PROTECT (PR)**	PR.AT	Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-04	Senior executives understand their roles & responsibilities	Cybersecurity Related	**1**	Partial
CIP-004-6-R1	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-6 Table R1 – Security Awareness Program.	**PROTECT (PR)**	PR.AT	Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-01	All users are informed and trained	Cybersecurity Related	**1**	Partial
CIP-004-6-R1	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-6 Table R1 – Security Awareness Program.	**PROTECT (PR)**	PR.AT	Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-02	Privileged users understand roles & responsibilities	Cybersecurity Related	**1**	Partial
CIP-004-6-R1	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-6 Table R1 – Security Awareness Program.	**PROTECT (PR)**	PR.AT	Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-03	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Cybersecurity Related	**1**	Partial

CIP-004-6-R1	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-6 Table R1 – Security Awareness Program.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-04	Senior executives understand their roles & responsibilities	Cybersecurity Related	1	Partial
CIP-004-6-R1	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-6 Table R1 – Security Awareness Program.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-05	Physical and cybersecurity personnel understand their roles and responsibilities	Cybersecurity Related	1	Partial
CIP-004-6-R2	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-06	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Compliance Related	1	Partial
CIP-004-6-R2	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.	IDENTIFY (ID)	ID.BE	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-03	Priorities for organizational mission, objectives, and activities are established and communicated	Compliance Related	1	Partial
CIP-004-6-R2	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.	IDENTIFY (ID)	ID.GV	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-01	Organizational information security policy is established and communicated	Compliance Related	1	Partial
CIP-004-6-R2	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-01	All users are informed and trained	Compliance Related	1	Partial

CIP-004-6-R2	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-02	Privileged users understand roles & responsibilities	Compliance Related	1	Partial
CIP-004-6-R2	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-03	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Compliance Related	1	Partial
CIP-004-6-R2	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-04	Senior executives understand their roles & responsibilities	Compliance Related	1	Partial
CIP-004-6-R2	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-05	Physical and cybersecurity personnel understand their roles and responsibilities	Compliance Related	1	Partial
CIP-004-6-R2	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Cybersecurity Related	1	Partial
CIP-004-6-R3	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 3: Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-6 Table R3 – Personnel Risk Assessment Program.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-06	Identities are proofed and bound to credentials and asserted in interactions	Compliance Related	1	Partial

CIP-004-6-R3	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 3: Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-6 Table R3 – Personnel Risk Assessment Program.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Cybersecurity Related	1	Partial
CIP-004-6-R4	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 4: Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.	ID.AM-06	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Cybersecurity Related	1	Partial
CIP-004-6-R4	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 4: Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-01	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	Compliance Related	1	Partial
CIP-004-6-R4	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 4: Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-02	Physical access to assets is managed and protected	Compliance Related	1	Partial
CIP-004-6-R4	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 4: Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-03	Remote access is managed	Cybersecurity Related	1	Partial
CIP-004-6-R4	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 4: Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-04	Access permissions are managed, incorporating the principles of least privilege and separation of duties	Compliance Related	1	Partial

CIP-004-6-R4	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 4: Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-01	Data-at-rest is protected	Cybersecurity Related	1	Partial
CIP-004-6-R4	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 4: Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-02	Data-in-transit is protected	Cybersecurity Related	1	Partial
CIP-004-6-R4	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 4: Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-05	Protections against data leaks are implemented	Cybersecurity Related	1	Partial
CIP-004-6-R4	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 4: Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Cybersecurity Related	1	Partial
CIP-004-6-R5	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 5: Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-01	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	Compliance Related	1	Partial
CIP-004-6-R5	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 5: Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-02	Physical access to assets is managed and protected	Compliance Related	1	Partial

CIP-004-6-R5	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 5: Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-03	Remote access is managed	Compliance Related	1	Partial
CIP-004-6-R5	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 5: Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-04	Access permissions are managed, incorporating the principles of least privilege and separation of duties	Compliance Related	1	Partial
CIP-004-6-R5	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 5: Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-01	Data-at-rest is protected	Cybersecurity Related	1	Partial
CIP-004-6-R5	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 5: Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-02	Data-in-transit is protected	Cybersecurity Related	1	Partial
CIP-004-6-R5	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 5: Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-05	Protections against data leaks are implemented	Cybersecurity Related	1	Partial
CIP-004-6-R5	Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. Requirement 5: Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Cybersecurity Related	1	Partial

CIP-005-5-R1	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-04	External information systems are catalogued	Compliance Related	1	Partial
CIP-005-5-R1	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-03	Remote access is managed	Compliance Related	1	Partial
CIP-005-5-R1	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-05	Network integrity is protected, incorporating network segregation where appropriate	Compliance Related	1	Partial
CIP-005-5-R1	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-07	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Cybersecurity Related	1	Partial
CIP-005-5-R1	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-02	Data-in-transit is protected	Cybersecurity Related	1	Partial
CIP-005-5-R1	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-05	Protections against data leaks are implemented	Cybersecurity Related	1	Partial
CIP-005-5-R1	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-07	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Compliance Related	1	Partial

CIP-005-5-R1	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	PROTECT (PR)	PR.PT	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-04	Communications and control networks are protected	Cybersecurity Related	1	Partial
CIP-005-5-R1	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	DETECT (DE)	DE.AE	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-02	Detected events are analyzed to understand attack targets and methods	Cybersecurity Related	1	Partial
CIP-005-5-R1	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-01	The network is monitored to detect potential cybersecurity events	Cybersecurity Related	1	Partial
CIP-005-5-R1	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-06	External service provider activity is monitored to detect potential cybersecurity events	Cybersecurity Related	1	Partial
CIP-005-5-R1	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Compliance Related	1	Partial
CIP-005-5-R2	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.	ID.AM-03	Organizational communication and data flows are mapped	Compliance Related	1	Partial
CIP-005-5-R2	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-03	Remote access is managed	Cybersecurity Related	1	Partial

CIP-005-5-R2	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-04	Access permissions are managed, incorporating the principles of least privilege and separation of duties	Compliance Related	**1**	Partial
CIP-005-5-R2	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-07	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Cybersecurity Related	**1**	Partial
CIP-005-5-R2	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-02	Data-in-transit is protected	Cybersecurity Related	**1**	Partial
CIP-005-5-R2	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-05	Protections against data leaks are implemented	Cybersecurity Related	**1**	Partial
CIP-005-5-R2	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.	PROTECT (PR)	PR.MA	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-02	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Cybersecurity Related	**1**	Partial
CIP-005-5-R2	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.	PROTECT (PR)	PR.PT	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-04	Communications and control networks are protected	Compliance Related	**1**	Partial

CIP-005-5-R2	Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-06	External service provider activity is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
CIP-006-6-R1	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-02	Physical access to assets is managed and protected	Compliance Related	1	Partial
CIP-006-6-R1	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.	PROTECT (PR)	PR.PT	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-01	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Compliance Related	1	Partial
CIP-006-6-R1	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.	PROTECT (PR)	PR.PT	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-04	Communications and control networks are protected	Cybersecurity Related	1	Partial
CIP-006-6-R1	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-02	The physical environment is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
CIP-006-6-R1	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-03	Personnel activity is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
CIP-006-6-R1	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-06	External service provider activity is monitored to detect potential cybersecurity events	Compliance Related	1	Partial

CIP-006-6-R1	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Compliance Related	1	Partial
CIP-006-6-R2	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-02	Physical access to assets is managed and protected	Compliance Related	1	Partial
CIP-006-6-R2	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program.	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-05	Physical and cybersecurity personnel understand their roles and responsibilities	Compliance Related	1	Partial
CIP-006-6-R2	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program.	PROTECT (PR)	PR.PT	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-01	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Cybersecurity Related	1	Partial
CIP-006-6-R2	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 2: Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-02	The physical environment is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
CIP-006-6-R3	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 3: Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in CIP-006-6 Table R3 – Maintenance and Testing Program.	PROTECT (PR)	PR.MA	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-01	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	Compliance Related	1	Partial
CIP-006-6-R3	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 3: Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in CIP-006-6 Table R3 – Maintenance and Testing Program.	PROTECT (PR)	PR.MA	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-02	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Compliance Related	1	Partial

CIP-006-6-R3	Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. Requirement 3: Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in CIP-006-6 Table R3 – Maintenance and Testing Program.	DETECT (DE)	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-03	Detection processes are tested	Cybersecurity Related	1	Partial
CIP-007-6-R1	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-02	Physical access to assets is managed and protected	Compliance Related	1	Partial
CIP-007-6-R1	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services.	PROTECT (PR)	PR.PT	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-02	Removable media is protected and its use restricted according to policy	Compliance Related	1	Partial
CIP-007-6-R1	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services.	PROTECT (PR)	PR.PT	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-03	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Compliance Related	1	Partial
CIP-007-6-R2	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.	IDENTIFY (ID)	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-01	Asset vulnerabilities are identified and documented	Compliance Related	1	Partial
CIP-007-6-R2	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.	IDENTIFY (ID)	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	Compliance Related	1	Partial

CIP-007-6-R2	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.	IDENTIFY (ID)	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Compliance Related	1	Partial
CIP-007-6-R2	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.	IDENTIFY (ID)	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-06	Risk responses are identified and prioritized	Compliance Related	1	Partial
CIP-007-6-R2	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-03	Configuration change control processes are in place	Cybersecurity Related	1	Partial
CIP-007-6-R2	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-12	A vulnerability management plan is developed and implemented	Cybersecurity Related	1	Partial
CIP-007-6-R2	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.	RESPOND (RS)	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-05	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	Compliance Related	1	Partial
CIP-007-6-R2	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.	RESPOND (RS)	RS.MI	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-03	Newly identified vulnerabilities are mitigated or documented as accepted risks	Compliance Related	1	Partial

CIP-007-6-R3	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention.	**PROTECT (PR)**	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-05	Protections against data leaks are implemented	Compliance Related	**1**	Partial
CIP-007-6-R3	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention.	**PROTECT (PR)**	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-12	A vulnerability management plan is developed and implemented	Cybersecurity Related	**1**	Partial
CIP-007-6-R3	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention.	**DETECT (DE)**	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-04	Malicious code is detected	Cybersecurity Related	**1**	Partial
CIP-007-6-R3	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention.	**DETECT (DE)**	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-05	Unauthorized mobile code is detected	Compliance Related	**1**	Partial
CIP-007-6-R3	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention.	**DETECT (DE)**	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Cybersecurity Related	**1**	Partial
CIP-007-6-R3	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention.	**DETECT (DE)**	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-02	Detection activities comply with all applicable requirements	Compliance Related	**1**	Partial

CIP-007-6-R4	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	IDENTIFY (ID)	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-03	Threats, both internal and external, are identified and documented	Compliance Related	**1**	Partial
CIP-007-6-R4	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-05	Protections against data leaks are implemented	Compliance Related	**1**	Partial
CIP-007-6-R4	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	PROTECT (PR)	PR.PT	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-01	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Compliance Related	**1**	Partial
CIP-007-6-R4	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	DETECT (DE)	DE.AE	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-02	Detected events are analyzed to understand attack targets and methods	Compliance Related	**1**	Partial
CIP-007-6-R4	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	DETECT (DE)	DE.AE	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-03	Event data are collected and correlated from multiple sources and sensors	Compliance Related	**1**	Partial
CIP-007-6-R4	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	DETECT (DE)	DE.AE	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-05	Incident alert thresholds are established	Compliance Related	**1**	Partial

CIP-007-6-R4	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	**DETECT (DE)**	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-03	Personnel activity is monitored to detect potential cybersecurity events	Cybersecurity Related	**1**	Partial
CIP-007-6-R4	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	**DETECT (DE)**	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-04	Malicious code is detected	Compliance Related	**1**	Partial
CIP-007-6-R4	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	**DETECT (DE)**	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-06	External service provider activity is monitored to detect potential cybersecurity events	Compliance Related	**1**	Partial
CIP-007-6-R4	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	**DETECT (DE)**	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Cybersecurity Related	**1**	Partial
CIP-007-6-R4	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	**DETECT (DE)**	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-02	Detection activities comply with all applicable requirements	Compliance Related	**1**	Partial
CIP-007-6-R5	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 5: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.	**PROTECT (PR)**	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-01	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	Compliance Related	**1**	Partial

CIP-007-6-R5	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 5: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-04	Access permissions are managed, incorporating the principles of least privilege and separation of duties	Compliance Related	**1**	Partial
CIP-007-6-R5	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 5: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-07	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Compliance Related	**1**	Partial
CIP-007-6-R5	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 5: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-05	Protections against data leaks are implemented	Cybersecurity Related	**1**	Partial
CIP-007-6-R5	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 5: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.	DETECT (DE)	DE.AE	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-05	Incident alert thresholds are established	Compliance Related	**1**	Partial
CIP-007-6-R5	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 5: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-03	Personnel activity is monitored to detect potential cybersecurity events	Compliance Related	**1**	Partial
CIP-007-6-R5	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 5: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-06	External service provider activity is monitored to detect potential cybersecurity events	Compliance Related	**1**	Partial

CIP-007-6-R5	Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 5: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.	**DETECT (DE)**	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Cybersecurity Related	**1**	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	**IDENTIFY (ID)**	ID.BE	Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-05	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	Compliance Related	**1**	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	**IDENTIFY (ID)**	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-06	Risk responses are identified and prioritized	Compliance Related	**1**	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	**PROTECT (PR)**	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Compliance Related	**1**	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	**DETECT (DE)**	DE.AE	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-02	Detected events are analyzed to understand attack targets and methods	Compliance Related	**1**	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	**DETECT (DE)**	DE.AE	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-04	Impact of events is determined	Compliance Related	**1**	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	**DETECT (DE)**	DE.AE	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-05	Incident alert thresholds are established	Compliance Related	**1**	Partial

CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	DETECT (DE)	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-01	Roles and responsibilities for detection are well defined to ensure accountability	Cybersecurity Related	1	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	DETECT (DE)	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-02	Detection activities comply with all applicable requirements	Compliance Related	1	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	DETECT (DE)	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-04	Event detection information is communicated	Compliance Related	1	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	RESPOND (RS)	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-01	Notifications from detection systems are investigated	Compliance Related	1	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	RESPOND (RS)	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-02	The impact of the incident is understood	Compliance Related	1	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	RESPOND (RS)	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-03	Forensics are performed	Cybersecurity Related	1	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	RESPOND (RS)	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-04	Incidents are categorized consistent with response plans	Compliance Related	1	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	RESPOND (RS)	RS.CO	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-01	Personnel know their roles and order of operations when a response is needed	Compliance Related	1	Partial

CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	RESPOND (RS)	RS.CO	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-02	Incidents are reported consistent with established criteria	Compliance Related	1	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	RESPOND (RS)	RS.CO	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-03	Information is shared consistent with response plans	Compliance Related	1	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	RESPOND (RS)	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.CO-04	Coordination with stakeholders occurs consistent with response plans	Compliance Related	1	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	RESPOND (RS)	RS.MI	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-01	Incidents are contained	Compliance Related	1	Partial
CIP-008-5-R1	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	RESPOND (RS)	RS.MI	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-02	Incidents are mitigated	Compliance Related	1	Partial
CIP-008-5-R2	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 2: Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-10	Response and recovery plans are tested	Cybersecurity Related	1	Partial
CIP-008-5-R2	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 2: Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.	DETECT (DE)	DE.AE	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-02	Detected events are analyzed to understand attack targets and methods	Compliance Related	1	Partial
CIP-008-5-R2	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 2: Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.	DETECT (DE)	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-03	Detection processes are tested	Compliance Related	1	Partial

CIP-008-5-R2	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 2: Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.	RESPOND (RS)	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-01	Notifications from detection systems are investigated	Cybersecurity Related	1	Partial
CIP-008-5-R2	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 2: Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.	RESPOND (RS)	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-02	The impact of the incident is understood	Cybersecurity Related	1	Partial
CIP-008-5-R2	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 2: Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.	RESPOND (RS)	RS.CO	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-02	Incidents are reported consistent with established criteria	Cybersecurity Related	1	Partial
CIP-008-5-R2	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 2: Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.	RESPOND (RS)	RS.CO	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-03	Information is shared consistent with response plans	Cybersecurity Related	1	Partial
CIP-008-5-R2	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 2: Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.	RESPOND (RS)	RS.CO	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-04	Coordination with stakeholders occurs consistent with response plans	Cybersecurity Related	1	Partial
CIP-008-5-R2	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 2: Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.	RESPOND (RS)	RS.RP	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-01	Response plan is executed during or after an event	Cybersecurity Related	1	Partial
CIP-008-5-R3	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 3: Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-07	Protection processes are improved	Compliance Related	1	Partial
CIP-008-5-R3	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 3: Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-08	Effectiveness of protection technologies is shared	Compliance Related	1	Partial

CIP-008-5-R3	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 3: Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Compliance Related	1	Partial
CIP-008-5-R3	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 3: Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.	DETECT (DE)	DE.DP	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-05	Detection processes are continuously improved	Compliance Related	1	Partial
CIP-008-5-R3	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 3: Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.	RESPOND (RS)	RS.CO	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-01	Personnel know their roles and order of operations when a response is needed	Compliance Related	1	Partial
CIP-008-5-R3	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 3: Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.	RESPOND (RS)	RS.IM	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-01	Response plans incorporate lessons learned	Compliance Related	1	Partial
CIP-008-5-R3	Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Requirement 3: Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.	RESPOND (RS)	RS.IM	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-02	Response strategies are updated	Compliance Related	1	Partial
CIP-009-6-R1	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 1: Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications.	IDENTIFY (ID)	ID.BE	Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-05	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	Compliance Related	1	Partial
CIP-009-6-R1	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 1: Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-04	Adequate capacity to ensure availability is maintained	Compliance Related	1	Partial
CIP-009-6-R1	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 1: Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-04	Backups of information are conducted, maintained, and tested	Compliance Related	1	Partial
CIP-009-6-R1	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 1: Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Compliance Related	1	Partial

CIP-009-6-R1	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 1: Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications.	RESPOND (RS)	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-03	Forensics are performed	Compliance Related	1	Partial
CIP-009-6-R1	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 1: Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications.	RECOVER (RC)	RC.RP	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-01	Recovery plan is executed during or after an cybersecurity incident	Compliance Related	1	Partial
CIP-009-6-R2	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-04	Backups of information are conducted, maintained, and tested	Compliance Related	1	Partial
CIP-009-6-R2	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-10	Response and recovery plans are tested	Compliance Related	1	Partial
CIP-009-6-R2	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.	RECOVER (RC)	RC.RP	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-01	Recovery plan is executed during or after an cybersecurity incident	Compliance Related	1	Partial
CIP-009-6-R3	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 3: Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-07	Protection processes are improved	Compliance Related	1	Partial
CIP-009-6-R3	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 3: Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-08	Effectiveness of protection technologies is shared	Compliance Related	1	Partial
CIP-009-6-R3	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 3: Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Compliance Related	1	Partial
CIP-009-6-R3	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 3: Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.	RECOVER (RC)	RC.CO	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-03	Recovery activities are communicated to internal stakeholders and executive and management teams	Compliance Related	1	Partial

CIP-009-6-R3	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 3: Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.	RECOVER (RC)	RC.IM	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-01	Recovery plans incorporate lessons learned	Compliance Related	1	Partial
CIP-009-6-R3	Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement 3: Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.	RECOVER (RC)	RC.IM	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-02	Recovery strategies are updated	Compliance Related	1	Partial
CIP-010-2-R1	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-06	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Compliance Related	1	Partial
CIP-010-2-R1	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-07	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Compliance Related	1	Partial
CIP-010-2-R1	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-01	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	Compliance Related	1	Partial
CIP-010-2-R1	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-03	Configuration change control processes are in place	Compliance Related	1	Partial
CIP-010-2-R1	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.	PROTECT (PR)	PR.MA	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-01	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	Compliance Related	1	Partial

CIP-010-2-R1	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.	PROTECT (PR)	PR.MA	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-02	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Compliance Related	1	Partial
CIP-010-2-R1	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.	PROTECT (PR)	PR.PT	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-03	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Cybersecurity Related	1	Partial
CIP-010-2-R1	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-05	Unauthorized mobile code is detected	Cybersecurity Related	1	Partial
CIP-010-2-R2	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R2 – Configuration Monitoring.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-06	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Compliance Related	1	Partial
CIP-010-2-R2	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R2 – Configuration Monitoring.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-01	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	Compliance Related	1	Partial
CIP-010-2-R2	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R2 – Configuration Monitoring.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-03	Configuration change control processes are in place	Compliance Related	1	Partial

CIP-010-2-R3	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R3– Vulnerability Assessments.	**IDENTIFY (ID)**	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-01	Asset vulnerabilities are identified and documented	Compliance Related	**1**	Partial
CIP-010-2-R3	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R3– Vulnerability Assessments.	**IDENTIFY (ID)**	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Compliance Related	**1**	Partial
CIP-010-2-R3	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R3– Vulnerability Assessments.	**IDENTIFY (ID)**	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-06	Risk responses are identified and prioritized	Compliance Related	**1**	Partial
CIP-010-2-R3	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R3– Vulnerability Assessments.	**PROTECT (PR)**	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-12	A vulnerability management plan is developed and implemented	Compliance Related	**1**	Partial
CIP-010-2-R3	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R3– Vulnerability Assessments.	**DETECT (DE)**	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-08	Vulnerability scans are performed	Compliance Related	**1**	Partial
CIP-010-2-R3	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R3– Vulnerability Assessments.	**RESPOND (RS)**	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-05	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	Compliance Related	**1**	Partial

CIP-010-2-R3	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 3: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R3– Vulnerability Assessments.	RESPOND (RS)	RS.MI	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-03	Newly identified vulnerabilities are mitigated or documented as accepted risks	Compliance Related	1	Partial
CIP-010-2-R4	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.	PROTECT (PR)	PR.PT	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-02	Removable media is protected and its use restricted according to policy	Compliance Related	1	Partial
CIP-010-2-R4	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-04	Malicious code is detected	Compliance Related	1	Partial
CIP-010-2-R4	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-05	Unauthorized mobile code is detected	Compliance Related	1	Partial
CIP-010-2-R4	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	Compliance Related	1	Partial
CIP-010-2-R4	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.	RESPOND (RS)	RS.AN	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-05	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	Compliance Related	1	Partial

CIP-010-2-R4	Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 4: Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.	RESPOND (RS)	RS.MI	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-03	Newly identified vulnerabilities are mitigated or documented as accepted risks	Compliance Related	1	Partial
CIP-011-2-R1	Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-2 Table R1 – Information Protection.	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.	ID.AM-03	Organizational communication and data flows are mapped	Compliance Related	1	Partial
CIP-011-2-R1	Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-2 Table R1 – Information Protection.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-01	Data-at-rest is protected	Compliance Related	1	Partial
CIP-011-2-R1	Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-2 Table R1 – Information Protection.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-02	Data-in-transit is protected	Compliance Related	1	Partial
CIP-011-2-R1	Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-2 Table R1 – Information Protection.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-05	Protections against data leaks are implemented	Compliance Related	1	Partial
CIP-011-2-R1	Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 1: Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-2 Table R1 – Information Protection.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-06	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Compliance Related	1	Partial
CIP-011-2-R2	Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-01	Data-at-rest is protected	Compliance Related	1	Partial

CIP-011-2-R2	Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-03	Assets are formally managed throughout removal, transfers, and disposition	Compliance Related	1	Partial
CIP-011-2-R2	Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal.	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-05	Protections against data leaks are implemented	Compliance Related	1	Partial
CIP-011-2-R2	Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). Requirement 2: Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal.	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-06	Data is destroyed according to policy	Compliance Related	1	Partial
CIP-012-1-R1	Purpose: To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers. Requirement 1: The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. (See Sub-Requirements 1.1 through 1.3)	PROTECT (PR)	PR.IP	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-01	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	IDENTIFY (ID)	ID.BE	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-01	The organization's role in the supply chain is identified and communicated	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	IDENTIFY (ID)	ID.BE	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-02	The organization's place in critical infrastructure and its industry sector is identified and communicated	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	IDENTIFY (ID)	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Compliance Related	1	Partial

CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	IDENTIFY (ID)	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-06	Risk responses are identified and prioritized	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	IDENTIFY (ID)	ID.RM	Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-01	Risk management processes are established, managed, and agreed to by organizational stakeholders	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	IDENTIFY (ID)	ID.SC	Supply Chain Risk Management (ID.SC): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.	ID.SC-01	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	IDENTIFY (ID)	ID.SC	Supply Chain Risk Management (ID.SC): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.	ID.SC-02	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	IDENTIFY (ID)	ID.SC	Supply Chain Risk Management (ID.SC): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.	ID.SC-03	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	IDENTIFY (ID)	ID.SC	Supply Chain Risk Management (ID.SC): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.	ID.SC-04	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	IDENTIFY (ID)	ID.SC	Supply Chain Risk Management (ID.SC): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.	ID.SC-05	Response and recovery planning and testing are conducted with suppliers and third-party providers	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-03	Remote access is managed	Compliance Related	1	Partial

CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	PROTECT (PR)	PR.AC	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-04	Access permissions are managed, incorporating the principles of least privilege and separation of duties	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	PROTECT (PR)	PR.AT	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-03	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-06	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	PROTECT (PR)	PR.DS	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-08	Integrity checking mechanisms are used to verify hardware integrity	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	PROTECT (PR)	PR.MA	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-02	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Compliance Related	1	Partial
CIP-013-1-R1	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. (See Sub-Requirements 1.1 and 1.2)	DETECT (DE)	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-06	External service provider activity is monitored to detect potential cybersecurity events	Compliance Related	1	Partial
CIP-013-1-R2	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. (See additional notes in this requirement)	IDENTIFY (ID)	ID.BE	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-01	The organization's role in the supply chain is identified and communicated	Compliance Related	1	Partial
CIP-013-1-R2	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. (See additional notes in this requirement)	IDENTIFY (ID)	ID.BE	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-02	The organization's place in critical infrastructure and its industry sector is identified and communicated	Compliance Related	1	Partial

CIP-013-1-R2	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. (See additional notes in this requirement)	IDENTIFY (ID)	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Compliance Related	1	Partial
CIP-013-1-R2	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. (See additional notes in this requirement)	IDENTIFY (ID)	ID.SC	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.	ID.SC-01	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Compliance Related	1	Partial
CIP-013-1-R2	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. (See additional notes in this requirement)	IDENTIFY (ID)	ID.SC	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.	ID.SC-02	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	Compliance Related	1	Partial
CIP-013-1-R2	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 2: Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. (See additional notes in this requirement)	IDENTIFY (ID)	ID.SC	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.	ID.SC-03	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	Compliance Related	1	Partial
CIP-013-1-R3	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 3: Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.	IDENTIFY (ID)	ID.BE	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-01	The organization's role in the supply chain is identified and communicated	Cybersecurity Related	1	Partial
CIP-013-1-R3	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 3: Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.	IDENTIFY (ID)	ID.BE	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-02	The organization's place in critical infrastructure and its industry sector is identified and communicated	Cybersecurity Related	1	Partial
CIP-013-1-R3	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 3: Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.	IDENTIFY (ID)	ID.RA	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Cybersecurity Related	1	Partial
CIP-013-1-R3	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 3: Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.	IDENTIFY (ID)	ID.SC	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.	ID.SC-01	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Cybersecurity Related	1	Partial

CIP-013-1-R3	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 3: Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.	IDENTIFY (ID)	ID.SC	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.	ID.SC-02	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	Cybersecurity Related	**1**	Partial
CIP-013-1-R3	Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. Requirement 3: Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.	IDENTIFY (ID)	ID.SC	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.	ID.SC-03	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	Cybersecurity Related	**1**	Partial
CIP-014-2-R5	Purpose: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. Requirement 5: Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). (See Sub-Requirements 5.1 through 5.4)	**DETECT (DE)**	DE.CM	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-02	The physical environment is monitored to detect potential cybersecurity events	Cybersecurity Related	**1**	Partial

CIP ID	Purpose and Requirements	VRF Rating
CIP-002-5.1a-R1	**Purpose:** To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. **Requirement 1:** Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	HIGH
CIP-002-5.1a-R2	**Purpose:** To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. **Requirement 2:** The Responsible Entity shall: ***(See Sub-Requirements 2.1 and 2.2)***	LOWER
CIP-003-8-R1	**Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 1:** Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: **(See Sub-Requirements 1.1 and 1.2)**	MEDIUM
CIP-003-8-R2	**Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 2:** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	LOWER

CIP-003-8-R3	**Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 3:** Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.	MEDIUM
CIP-003-8-R4	**Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 4:** The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	LOWER
CIP-004-6-R1	**Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. **Requirement 1:** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-6 Table R1 – Security Awareness Program.	LOWER
CIP-004-6-R2	**Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. **Requirement 2:** Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.	LOWER

CIP-004-6-R3	**Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. **Requirement 3:** Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-6 Table R3 – Personnel Risk Assessment Program.	MEDIUM
CIP-004-6-R4	**Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. **Requirement 4:** Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.	MEDIUM
CIP-004-6-R5	**Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. **Requirement 5:** Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.	MEDIUM
CIP-005-5-R1	**Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. **Requirement 1:** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	MEDIUM

CIP-005-5-R2	**Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. **Requirement 2:** Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.	MEDIUM
CIP-006-6-R1	**Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. **Requirement 1:** Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.	MEDIUM

CIP-006-6-R2	**Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. **Requirement 2:** Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program.	MEDIUM
CIP-006-6-R3	**Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. **Requirement 3:** Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in CIP-006-6 Table R3 – Maintenance and Testing Program.	MEDIUM
CIP-007-6-R1	**Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 1:** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services.	MEDIUM

CIP-007-6-R2	**Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 2:** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.	MEDIUM
CIP-007-6-R3	**Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 3:** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention.	MEDIUM
CIP-007-6-R4	**Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 4:** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	MEDIUM

CIP-007-6-R5	**Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 5:** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.	MEDIUM
CIP-008-5-R1	**Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. **Requirement 1:** Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	LOWER
CIP-008-5-R2	**Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. **Requirement 2:** Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.	LOWER
CIP-008-5-R3	**Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. **Requirement 3:** Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.	LOWER
CIP-009-6-R1	**Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. **Requirement 1:** Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications.	MEDIUM

CIP-009-6-R2	**Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. **Requirement 2:** Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.	LOWER
CIP-009-6-R3	**Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. **Requirement 3:** Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.	LOWER
CIP-010-2-R1	**Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 1:** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.	MEDIUM
CIP-010-2-R2	**Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 2:** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R2 – Configuration Monitoring.	MEDIUM
CIP-010-2-R3	**Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 3:** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R3– Vulnerability Assessments.	MEDIUM

CIP-010-2-R4	**Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 4:** Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.	MEDIUM
CIP-011-2-R1	**Purpose:** To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 1:** Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-2 Table R1 – Information Protection.	MEDIUM
CIP-011-2-R2	**Purpose:** To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES). **Requirement 2:** Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal.	LOWER
CIP-012-1-R1	**Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers. **Requirement 1:** The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. **(See Sub-Requirements 1.1 through 1.3)**	MEDIUM

CIP-013-1-R1	**Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. **Requirement 1:** Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. **(See Sub-Requirements 1.1 and 1.2)**	MEDIUM
CIP-013-1-R2	**Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. **Requirement 2:** Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. **(See additional notes in this requirement)**	MEDIUM
CIP-013-1-R3	**Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. **Requirement 3:** Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.	MEDIUM
CIP-014-2-R1	**Purpose:** To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. **Requirement 1:** Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. **(See Sub-Requirements 1.1 and 1.2)**	HIGH

CIP-014-2-R2	**Purpose:** To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. **Requirement 2:** Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. **(See Sub-Requirements 2.1 through 2.4)**	MEDIUM
CIP-014-2-R3	**Purpose:** To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. **Requirement 3:** For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. **(See Sub-Requirement 3.1)**	LOWER
CIP-014-2-R4	**Purpose:** To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. **Requirement 4:** Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. **(See Sub-Requirements 4.1 through 4.3)**	MEDIUM

CIP-014-2-R5	**Purpose:** To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. **Requirement 5:** Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). **(See Sub-Requirements 5.1 through 5.4)**	HIGH
CIP-014-2-R6	**Purpose:** To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection. **Requirement 6:** Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5.**(See Sub-Requirements 6.1 through 6.4)**	MEDIUM

		Outcomes		*Outcomes*	*Informative References*				
Function		**Category**	**ID**	**Sub-Categories**	*NIST 800-53 Rev. 4*	*CIS CSC*	*COBIT*	*ISA*	*ISO*
	ID.AM	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-01**	Physical devices and systems within the organization are inventoried	CM-8, PM-5	CIS CSC 1	BAI09.01, BAI09.02	ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8	ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
			ID.AM-02	Software platforms and applications within the organization are inventoried	CM-8, PM-5	CIS CSC 2	BAI09.01, BAI09.02, BAI09.05	ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8	ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1
			ID.AM-03	Organizational communication and data flows are mapped	AC-4, CA-3, CA-9, PL-8	CIS CSC 12	DSS05.02	ISA 62443-2-1:2009 4.2.3.4	ISO/IEC 27001:2013 A.13.2.1
			ID.AM-04	External information systems are catalogued	AC-20, SA-9	CIS CSC 12	APO02.02, APO10.04, DSS01.02	N/A	ISO/IEC 27001:2013 A.11.2.6
			ID.AM-05	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, SA-14, SC-6	CIS CSC 13, 14	APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02	ISA 62443-2-1:2009 4.2.3.6	ISO/IEC 27001:2013 A.8.2.1
			ID.AM-06	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CP-2, PS-7, PM-11	CIS CSC 17, 19	APO01.02, APO07.06, APO13.01, DSS06.03	ISA 62443-2-1:2009 4.3.2.3.3	ISO/IEC 27001:2013 A.6.1.1
	ID.BE	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-01**	The organization's role in the supply chain is identified and communicated	CP-2, SA-12	N/A	APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05	N/A	ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
			ID.BE-02	The organization's place in critical infrastructure and its industry sector is identified and communicated	PM-8	N/A	APO02.06, APO03.01	N/A	ISO/IEC 27001:2013 Clause 4.1
			ID.BE-03	Priorities for organizational mission, objectives, and activities are established and communicated	PM-11, SA-14	N/A	APO02.01, APO02.06, APO03.01	ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6	N/A
			ID.BE-04	Dependencies and critical functions for delivery of critical services are established	CP-8, PE-9, PE-11, PM-8, SA-14	N/A	APO10.01, BAI04.02, BAI09.02	N/A	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3
			ID.BE-05	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	CP-2, CP-11, SA-13, SA-14	N/A	BAI03.02, DSS04.02	N/A	ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1
	ID.GV	**Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-01**	Organizational information security policy is established and communicated	-1 controls from all security control families	CIS CSC 19	APO01.03, EDM01.01, EDM01.02	ISA 62443-2-1:2009 4.3.2.6	ISO/IEC 27001:2013 A.5.1.1
			ID.GV-02	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	PS-7, PM-1, PM-2	CIS CSC 19	APO01.02, APO10.03, APO13.02, DSS05.04	ISA 62443-2-1:2009 4.3.2.3.3	ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1
			ID.GV-03	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	-1 controls from all security control families	CIS CSC 19	BAI02.01, MEA03.01, MEA03.04	ISA 62443-2-1:2009 4.4.3.7	ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5
			ID.GV-04	Governance and risk management processes address cybersecurity risks	SA-2, PM-3, PM-7, PM-9, PM-10, PM-11	N/A	EDM03.02, APO12.02, APO12.05, DSS04.02	ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3	ISO/IEC 27001:2013 Clause 6

IDENTIFY (ID)	**ID.RA**	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-01**	Asset vulnerabilities are identified and documented	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	CIS CSC 4	APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02	ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12	ISO/IEC 27001:2013 A.12.6.1, A.18.2.3
			ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	PM-15, PM-16, SI-5	CIS CSC 4	BAI08.01	ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12	ISO/IEC 27001:2013 A.6.1.4
			ID.RA-03	Threats, both internal and external, are identified and documented	RA-3, SI-5, PM-12, PM-16	CIS CSC 4	APO12.01, APO12.02, APO12.03, APO12.04	ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12	ISO/IEC 27001:2013 Clause 6.1.2
			ID.RA-04	Potential business impacts and likelihoods are identified	RA-2, RA-3, PM-9, PM-11, SA-14	CIS CSC 4	DSS04.02	ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12	ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2
			ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	RA-2, RA-3, PM-16	CIS CSC 4	APO12.02	N/A	ISO/IEC 27001:2013 A.12.6.1
			ID.RA-06	Risk responses are identified and prioritized	PM-4, PM-9	CIS CSC 4	APO12.05, APO13.02	N/A	ISO/IEC 27001:2013 Clause 6.1.3
	ID.RM	**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-01**	Risk management processes are established, managed, and agreed to by organizational stakeholders	PM-9	CIS CSC 4	APO12.04, APO12.05,	ISA 62443-2-1:2009 4.3.4.2	ISO/IEC 27001:2013 Clause
			ID.RM-02	Organizational risk tolerance is determined and clearly expressed	PM-9	N/A	APO12.06	ISA 62443-2-1:2009 4.3.2.6.5	ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3
			ID.RM-03	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	PM-8, PM-9, PM-11, SA-14	N/A	APO12.02	N/A	ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3
	ID.SC	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.	**ID.SC-01**	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	SA-9, SA-12, PM-9	CIS CSC: 4.8	APO10.01, APO10.04,	ISA 62443-2-1:2009: 4.3.4.2	ISO/IEC 27001:2013:
			ID.SC-02	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	RA-2, RA-3, SA-12, SA-14, SA-15, PM-9	N/A	APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03	ISA 62443-2-1:2009: 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14	ISO/IEC 27001:2013: A.15.2.1, A.15.2.2
			ID.SC-03	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	SA-9, SA-11, SA-12, PM-9	N/A	APO10.01, APO10.02, APO10.03, APO10.04, APO10.05	ISA 62443-2-1:2009: 4.3.2.6.4, 4.3.2.6.7	ISO/IEC 27001:2013: A.15.1.1, A.15.1.2, A.15.1.3
			ID.SC-04	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12	N/A	APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05	ISA 62443-2-1:2009: 4.3.2.6.7 ISA 62443-3-3:2013: SR 6.1	ISO/IEC 27001:2013: A.15.2.1, A.15.2.2

			ID.SC-05	Response and recovery planning and testing are conducted with suppliers and third-party providers	CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9	CIS CSC: 19.7, 20.3	DSS04.04	ISA 62443-2-1:2009: 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013: SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4	ISO/IEC 27001:2013 A.17.1.3
	PR.AC	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-01**	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA	CIS CSC 1, 5, 15, 16	DSS05.04, DSS06.03	ISA 62443-2-1:2009 4.3.3.5.1	ISO/IEC 27001:2013 A.9.2.1,
			PR.AC-02	Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-8	N/A	DSS01.04, DSS05.05	ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8	ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8
			PR.AC-03	Remote access is managed	AC-1, AC-17, AC-19, AC-20, SC-15	CIS CSC 12	APO13.01, DSS01.04, DSS05.03	ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6	ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1
			PR.AC-04	Access permissions are managed, incorporating the principles of least privilege and separation of duties	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	CIS CSC 3, 5, 12, 14, 15, 16, 18	DSS05.04	ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1	ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5
			PR.AC-05	Network integrity is protected, incorporating network segregation where appropriate	AC-4, AC-10, SC-7	CIS CSC 9, 14, 15, 18	DSS01.05, DSS05.02	ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8	ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
			PR.AC-06	Identities are proofed and bound to credentials and asserted in interactions	AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	CIS CSC, 16	DSS05.04, DSS05.05, DSS05.07, DSS06.03	ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1	ISO/IEC 27001:2013, A.7.1.1, A.9.2.1
			PR.AC-07	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)	AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11	CIS CSC 1, 12, 15, 16	DSS05.04, DSS05.10, DSS06.10	ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10	ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4
	PR.AT	**Awareness and Training (PR.AT):** The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-01**	All users are informed and trained	AT-2, PM-13	CIS CSC 17, 18	APO07.03, BAI05.07	ISA 62443-2-1:2009 4.3.2.4.2	ISO/IEC 27001:2013 A.7.2.2, A.12.2.1
			PR.AT-02	Privileged users understand roles & responsibilities	AT-3, PM-13	CIS CSC 5, 17, 18	APO07.02, DSS05.04, DSS06.03	ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3	ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
			PR.AT-03	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	PS-7, SA-9, SA-16	CIS CSC 17	APO07.03, APO07.06, APO10.04, APO10.05	ISA 62443-2-1:2009 4.3.2.4.2	ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
			PR.AT-04	Senior executives understand their roles & responsibilities	AT-3, PM-13	CIS CSC 17, 19	EDM01.01, APO01.02, APO07.03	ISA 62443-2-1:2009 4.3.2.4.2	ISO/IEC 27001:2013 A.6.1.1, A.7.2.2,

PROTECT (PR)			**PR.AT-05**	Physical and cybersecurity personnel understand their roles and responsibilities	AT-3, IR-2, PM-13	CIS CSC 17	APO07.03	ISA 62443-2-1:2009 4.3.2.4.2	ISO/IEC 27001:2013 A.6.1.1, A.7.2.2,
	PR.DS	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-01**	Data-at-rest is protected	MP-8, SC-12, SC-28	CIS CSC 13, 14	APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06	ISA 62443-3-3:2013 SR 3.4, SR 4.1	ISO/IEC 27001:2013 A.8.2.3
			PR.DS-02	Data-in-transit is protected	SC-8, SC-11, SC-12	CIS CSC 13, 14	APO01.06, DSS05.02, DSS06.06	ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2	ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
			PR.DS-03	Assets are formally managed throughout removal, transfers, and disposition	CM-8, MP-6, PE-16	CIS CSC 1	BAI09.03	ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 ISA 62443-3-3:2013 SR 4.2	ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7
			PR.DS-04	Adequate capacity to ensure availability is maintained	AU-4, CP-2, SC-5	CIS CSC 1, 2, 13	APO13.01, BAI04.04	ISA 62443-3-3:2013 SR 7.1, SR 7.2	ISO/IEC 27001:2013 A.12.1.3, A.17.2.1
			PR.DS-05	Protections against data leaks are implemented	AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4	CIS CSC 13	APO01.06, DSS05.04, DSS05.07, DSS06.02	ISA 62443-3-3:2013 SR 5.2	ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
			PR.DS-06	Integrity checking mechanisms are used to verify software, firmware, and information integrity	SC-16, SI-7	CIS CSC 2, 3	APO01.06, BAI06.01, DSS06.02	ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8	ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4
			PR.DS-07	Integrity checking mechanisms are used to verify software, firmware, and information integrity	CM-2	CIS CSC 18, 20	BAI07.04	N/A	ISO/IEC 27001:2013 A.12.1.4
			PR.DS-08	Integrity checking mechanisms are used to verify hardware integrity	SA-10, SI-7	N/A	BAI03.05	ISA 62443-2-1:2009 4.3.4.4.4	ISO/IEC 27001:2013 A.11.2.4
			PR.IP-01	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	CIS CSC 3, 9, 11	BAI10.01, BAI10.02, BAI10.03, BAI10.05	ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6	ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
			PR.IP-02	A System Development Life Cycle to manage systems is implemented	PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17	CIS CSC 18	APO13.01, BAI03.01, BAI03.02, BAI03.03	ISA 62443-2-1:2009 4.3.4.3.3	ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5
			PR.IP-03	Configuration change control processes are in place	CM-3, CM-4, SA-10	CIS CSC 3, 11	BAI06.01, BAI01.06	ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6	ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4

	PR.IP	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-04**	Backups of information are conducted, maintained, and tested	CP-4, CP-6, CP-9	CIS CSC 10	APO13.01, DSS01.01, DSS04.07	ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4	ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3
			PR.IP-05	Policy and regulations regarding the physical operating environment for organizational assets are met	PE-10, PE-12, PE-13, PE-14, PE-15, PE-18	N/A	DSS01.04, DSS05.05	ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6	ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
			PR.IP-06	Data is destroyed according to policy	MP-6	N/A	BAI09.03	ISA 62443-2-1:2009 4.3.4.4.4 ISA 62443-3-3:2013 SR 4.2	ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
			PR.IP-07	Protection processes are improved	CA-2, CA-7, CP-2, IR-8, PL-2, PM-6	N/A	APO11.06, APO12.06, DSS04.05	ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8	ISO/IEC 27001:2013 A.16.1.6, Clause 9, Clause 10
			PR.IP-08	Effectiveness of protection technologies is shared	AC-21, CA-7, SI-4	N/A	BAI08.04, DSS03.04	N/A	ISO/IEC 27001:2013 A.16.1.6
			PR.IP-09	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17	CIS CSC 19	APO12.06, DSS04.03	ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1	ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3
			PR.IP-10	Response and recovery plans are tested	CP-4, IR-3, PM-14	CIS CSC 19, 20	DSS04.04	ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 3.3	ISO/IEC 27001:2013 A.17.1.3
			PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21	CIS CSC 5, 16	APO07.01, APO07.02, APO07.03, APO07.04, APO07.05	ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3	ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4
			PR.IP-12	A vulnerability management plan is developed and implemented	RA-3, RA-5, SI-2	CIS CSC 4, 18, 20	BAI03.10, DSS05.01, DSS05.02	N/A	ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3
	PR.MA	**Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-01**	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	MA-2, MA-3, MA-5	N/A	BAI09.03	ISA 62443-2-1:2009 4.3.3.3.7	ISO/IEC 27001:2013
			PR.MA-02	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	MA-4	CIS CSC 3, 5	DSS05.04	ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8	ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1
			PR.PT-01	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU Family	CIS CSC 1, 3, 5, 6, 14, 15, 16	APO11.04, BAI03.05,	ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8,	ISO/IEC 27001:2013
			PR.PT-02	Removable media is protected and its use restricted according to policy	MP-2, MP-3, MP-4, MP-5, MP-7, MP-8	CIS CSC 8, 13	APO13.01, DSS05.02, DSS05.06	ISA 62443-3-3:2013 SR 2.3	ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9

	PR.PT	**Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-03**	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	AC-3, CM-7	CIS CSC 3, 11, 14	DSS05.02, DSS05.05, DSS06.06	ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7	ISO/IEC 27001:2013 A.9.1.2
			PR.PT-04	Communications and control networks are protected	AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	CIS CSC 8, 12, 15	DSS05.02, APO13.01	ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6	ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3
			PR.PT-05	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6	N/A	BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05	ISA 62443-2-1:2009 4.3.2.5.2 ISA 62443-3-3:2013 SR 7.1, SR 7.2	ISO/IEC 27001:2013 A.17.1.2, A.17.2.1
	DE.AE	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-01**	A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SI-4	CIS CSC 1, 4, 6, 12, 13, 15, 16	DSS03.01	ISA 62443-2-1:2009 4.4.3.3	ISO/IEC 27001:2013
			DE.AE-02	Detected events are analyzed to understand attack targets and methods	AU-6, CA-7, IR-4, SI-4	CIS CSC 3, 6, 13, 15	DSS05.07	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2	ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4
			DE.AE-03	Event data are collected and correlated from multiple sources and sensors	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16	BAI08.02	ISA 62443-3-3:2013 SR 6.1	ISO/IEC 27001:2013 A.12.4.1, A.16.1.7
			DE.AE-04	Impact of events is determined	CP-2, IR-4, RA-3, SI -4	CIS CSC 4, 6	APO12.06, DSS03.01	N/A	ISO/IEC 27001:2013 A.16.1.4
			DE.AE-05	Incident alert thresholds are established	IR-4, IR-5, IR-8	CIS CSC 6, 19	APO12.06, DSS03.01	ISA 62443-2-1:2009 4.2.3.10	ISO/IEC 27001:2013 A.16.1.4
			DE.CM-01	The network is monitored to detect potential cybersecurity events	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	CIS CSC 1, 7, 8, 12, 13, 15, 16	DSS01.03, DSS03.05, DSS05.07	ISA 62443-3-3:2013 SR 6.2	N/A
			DE.CM-02	The physical environment is monitored to detect potential cybersecurity events	CA-7, PE-3, PE-6, PE-20	N/A	DSS01.04, DSS01.05	ISA 62443-2-1:2009 4.3.3.3.8	ISO/IEC 27001:2013 A.11.1.1, A.11.1.2
			DE.CM-03	Personnel activity is monitored to detect potential cybersecurity events	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	CIS CSC 5, 7, 14, 16	DSS05.07	ISA 62443-3-3:2013 SR 6.2	ISO/IEC 27001:2013 A.12.4.1, A.12.4.3

DETECT (DE)	**DE.CM**	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-04**	Malicious code is detected	SI-3, SI-8	CIS CSC 4, 7, 8, 12	DSS05.01	ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2	ISO/IEC 27001:2013 A.12.2.1
			DE.CM-05	Unauthorized mobile code is detected	SC-18, SI-4. SC-44	CIS CSC 7, 8	DSS05.01	ISA 62443-3-3:2013 SR 2.4	ISO/IEC 27001:2013 A.12.5.1, A.12.6.2
			DE.CM-06	External service provider activity is monitored to detect potential cybersecurity events	CA-7, PS-7, SA-4, SA-9, SI-4	N/A	APO07.06, APO10.05	N/A	ISO/IEC 27001:2013 A.14.2.7, A.15.2.1
			DE.CM-07	Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16	DSS05.02, DSS05.05	N/A	ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1
			DE.CM-08	Vulnerability scans are performed	RA-5	CIS CSC 4, 20	BAI03.10, DSS05.01	ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7	ISO/IEC 27001:2013 A.12.6.1
	DE.DP	**Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-01**	Roles and responsibilities for detection are well defined to ensure accountability	CA-2, CA-7, PM-14	CIS CSC 5	APO01.02, DSS05.01,	ISA 62443-2-1:2009 4.4.3.1	ISO/IEC 27001:2013 A.6.1.1,
			DE.DP-02	Detection activities comply with all applicable requirements	CA-2, CA-7, PM-14, SI-4	N/A	DSS06.01, MEA03.03, MEA03.04	ISA 62443-2-1:2009 4.4.3.2	ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3
			DE.DP-03	Detection processes are tested	CA-2, CA-7, PE-3, SI-3, SI-4, PM-14	N/A	APO13.02, DSS05.02	ISA 62443-2-1:2009 4.4.3.2 ISA 62443-3-3:2013 SR 3.3	ISO/IEC 27001:2013 A.14.2.8
			DE.DP-04	Event detection information is communicated	AU-6, CA-2, CA-7, RA-5, SI-4	CIS CSC 19	APO08.04, APO12.06, DSS02.05	ISA 62443-2-1:2009 4.3.4.5.9 ISA 62443-3-3:2013 SR 6.1	ISO/IEC 27001:2013 A.16.1.2, A.16.1.3
			DE.DP-05	Detection processes are continuously improved	CA-2, CA-7, PL-2, RA-5, SI-4, PM-14	N/A	APO11.06, APO12.06, DSS04.05	ISA 62443-2-1:2009 4.4.3.4	ISO/IEC 27001:2013 A.16.1.6
RESPOND (RS)	**RS.RP**	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-01**	Response plan is executed during or after an event	CP-2, CP-10, IR-4, IR-8	CIS CSC 19	APO12.06, BAI01.10	ISA 62443-2-1:2009 4.3.4.5.1	ISO/IEC 27001:2013 A.16.1.5
	RS.CO	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-01**	Personnel know their roles and order of operations when a response is needed	CP-2, CP-3, IR-3, IR-8	CIS CSC 19	EDM03.02, APO01.02, APO12.03	ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4	ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1
			RS.CO-02	Incidents are reported consistent with established criteria	AU-6, IR-6, IR-8	CIS CSC 19	DSS01.03	ISA 62443-2-1:2009 4.3.4.5.5	ISO/IEC 27001:2013 A.6.1.3, A.16.1.2
			RS.CO-03	Information is shared consistent with response plans	CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI 4	CIS CSC 19	DSS03.04	ISA 62443-2-1:2009 4.3.4.5.2	ISO/IEC 27001:2013 A.16.1.2, Clause 7.4, Clause 16.1.2
			RS.CO-04	Coordination with stakeholders occurs consistent with response plans	CP-2, IR-4, IR-8	CIS CSC 19	DSS03.04	ISA 62443-2-1:2009 4.3.4.5.5	ISO/IEC 27001:2013 Clause 7.4
			RS.CO-05	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	PM-15, SI-5	CIS CSC 19	BAI08.04	N/A	ISO/IEC 27001:2013 A.6.1.4
			RS.AN-01	Notifications from detection systems are investigated	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	CIS CSC 4, 6, 8, 19	DSS02.04, DSS02.07	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 6.1	ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5
			RS.AN-02	The impact of the incident is understood	CP-2, IR-4	N/A	DSS02.02	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8	ISO/IEC 27001:2013 A.16.1.4, A.16.1.6

	RS.AN	**Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-03**	Forensics are performed	AU-7, IR-4	N/A	APO12.06, DSS03.02, DSS05.07	ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1	ISO/IEC 27001:2013 A.16.1.7
			RS.AN-04	Incidents are categorized consistent with response plans	CP-2, IR-4, IR-5, IR-8	CIS CSC 19	DSS02.02	ISA 62443-2-1:2009 4.3.4.5.6	ISO/IEC 27001:2013 A.16.1.4
			RS.AN-05	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	SI-5, PM-15	CIS CSC 4, 19	EDM03.02, DSS05.07	N/A	N/A
	RS.MI	**Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-01**	Incidents are contained	IR-4	CIS CSC 19	APO12.06	ISA 62443-2-1:2009 4.3.4.5.6	ISO/IEC 27001:2013
			RS.MI-02	Incidents are mitigated	IR-4	CIS CSC 4, 19	APO12.06	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10	ISO/IEC 27001:2013 A.12.2.1, A.16.1.5
			RS.MI-03	Newly identified vulnerabilities are mitigated or documented as accepted risks	CA-7, RA-3, RA-5	CIS CSC 4	APO12.06	N/A	ISO/IEC 27001:2013 A.12.6.1
	RS.IM	**Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-01**	Response plans incorporate lessons learned	CP-2, IR-4, IR-8	N/A	BAI01.13	ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4	ISO/IEC 27001:2013 A.16.1.6, Clause 10
			RS.IM-02	Response strategies are updated	CP-2, IR-4, IR-8	N/A	BAI01.13, DSS04.08	N/A	ISO/IEC 27001:2013
RECOVER (RC)	**RC.RP**	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-01**	Recovery plan is executed during or after an cybersecurity incident	CP-10, IR-4, IR-8	CIS CSC 10	APO12.06, DSS02.05, DSS03.04	N/A	ISO/IEC 27001:2013 A.16.1.5
	RC.IM	**Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-01**	Recovery plans incorporate lessons learned	CP-2, IR-4, IR-8	N/A	APO12.06, BAI05.07, DSS04.08	ISA 62443-2-1:2009 4.4.3.4	ISO/IEC 27001:2013 A.16.1.6, Clause 10
			RC.IM-02	Recovery strategies are updated	CP-2, IR-4, IR-8	N/A	APO12.06, BAI07.08	N/A	ISO/IEC 27001:2013
	RC.CO	**Communications (RC.CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-01**	Public relations are managed	N/A	N/A	EDM03.02	N/A	ISO/IEC 27001:2013 A.6.1.4, Clause 7.4
			RC.CO-02	Reputation after an event is repaired after an incident	N/A	N/A	MEA03.02	N/A	ISO/IEC 27001:2013 Clause 7.4
			RC.CO-03	Recovery activities are communicated to internal stakeholders and executive and management teams	CP-2, IR-4	N/A	APO12.06	N/A	ISO/IEC 27001:2013 Clause 7.4

Security Guideline	Security Guideline for the Electricity Sector: Assessing and Reducing Risk
Instructions	**Please use this form to submit comments on the draft Security Guideline. Comments must be submitted within the review period below to Tom Hofstetter (tom.hofstetter@nerc.net) with the words "Security Guideline: Assessing and Reducing Risk Comments" in the subject line. Only comments submitted in this Microsoft Excel format will be accepted. Both general and specific comments should be provided within this form.** Comments may be submitted by individuals or organizations. Please provide the requested information in Row 6. If comments are submitted on behalf of multiple organizations, list all organizations in Row 6. Please provide the Industry Segment and Region (if applicable) in Rows 7 and 8 and provide the requested contact information in Rows 9 and 10. If you have any questions regarding this process, please contact Tom Hofstetter (tom.hofstetter@nerc.net)
Review Period	December 18, 2020 -February 1, 2021

Name of Individual or Organization(s) (list multiple if submitted by a group):	Georgia System Operations Oglethorpe Power Corporation Georgia Transmission Corporation
Industry Segment (if applicable)	3
Region (if applicable)	SERC
Contact Telephone	770-270-7902
Contact Email	christina.bigelow@gasoc.com

Organization(s)	Page #	Line / Paragraph	Comment	Proposed Change	NERC Response - summarized category
Georgia System Operations Oglethorpe Power Corporation Georgia Transmission Corporation			We want to thank the team for developing this guideline and tool. It will be a great help to responsible entities and, in particular, we think the guideline and tool will be very beneficial to us.	**None**	No action necessary
Georgia System Operations Oglethorpe Power Corporation Georgia Transmission Corporation			All CIP requirements do not apply to all entities. Accordingly, such entities may not have a response to a particular mapping, e.g., it is not applicable to that entity. As proposed, the Implementation Tier doesn't account for 'not applicable' items.	**Modify implementation tiers to allow for a selection of "Not Applicable"**	Thank you for the feedback and suggestion. The final published tool will not be password protected and each entity is free to change the "CSF-ID to CIP Relationship" value to what is appropriate / applicable to them (e.g. Compliance Related vs Cybersecurity related). Regarding the Implementation Tiers, the intent of the team and the tool were to levarge the native definitions from the NIST Cyber Security Framework. We believe having the option to change the relationship will address this comment. Further, in the final document, password protection will be removed, enabling entities to update the Implementation Tiers and the Dashboard formulas to suit their needs.
Georgia System Operations Oglethorpe Power Corporation Georgia Transmission Corporation			This tool provides significant benefit; however, the continued evolution of the CIP standards and NIST framework could render it less useful as requirements "age out" and change. As an example, the tool refers to CIP-008-5 and CIP-008-6 became effective on January 1, 2021. Is there a plan to maintain this guideline and tool as the standards and frameworks evolve?	**Suggest proposing a maintenance process for this valuable deliverable.**	Thank you for the suggestion and the team agrees. We will be proposing the formation of a team to reviw and perform updates annually of the CIP Standards and NIST CSF tabs
Georgia System Operations Oglethorpe Power Corporation Georgia Transmission Corporation		162	A potential spelling error was identified in line 162.	**Suggest that 'annul' should be 'annual.'**	Document spelling change
Georgia System Operations Oglethorpe Power Corporation Georgia Transmission Corporation		100	Use of the phrase "intimately familiar" at line 100 may not be the most applicable descriptor.	Suggest modification to "substantive knowledge of...:	Document gramar change

Security Guideline	Security Guideline for the Electricity Sector: Assessing and Reducing Risk
Instructions	**Please use this form to submit comments on the draft Security Guideline. Comments must be submitted within the review period below to Tom Hofstetter (tom.hofstetter@nerc.net) with the words "Security Guideline: Assessing and Reducing Risk Comments" in the subject line. Only comments submitted in this Microsoft Excel format will be accepted. Both general and specific comments should be provided within this form.** Comments may be submitted by individuals or organizations. Please provide the requested information in Row 6. If comments are submitted on behalf of multiple organizations, list all organizations in Row 6. Please provide the Industry Segment and Region (if applicable) in Rows 7 and 8 and provide the requested contact information in Rows 9 and 10. If you have any questions regarding this process, please contact Tom Hofstetter (tom.hofstetter@nerc.net)
Review Period	December 18, 2020 -February 1, 2021

Name of Individual or Organization(s) (list multiple if submitted by a group):	
Industry Segment (if applicable)	
Region (if applicable)	
Contact Telephone	
Contact Email	

Organization(s)	**Page #**	**Line / Paragraph**	**Comment**	**Proposed Change**	**NERC Response - summarized category**
SERC		342-344	Link to document is broken	Fix link	Document link fix
SERC			Column H on Implementation Dashboard is not working as it give #NAME? in place of Directly Relates/Indirectly Relates	Fix formula	It appears there may be a versioning issue - the version of the tool provided for 45-day comment has only "Compliance Related" or "Cybersecurity Related" as options and currently no "#NAME" reference issues. Thank you for bringing this to our attention, after review and verificaiton, we believe you may unfortunately have a copy of what was used during the Pilot phase with a select view volunteers.
SERC	5	131	Why does orange have higher numbers than green	Change numbers	Document will be changed to align with tool: Orange will be corrected to reflect 1.5 - 2.5, instead of 3.5 - 4.5 typo
SERC	5	138	Mentions 1 to 5, but there are only four ratings, 1 to 4.	Adjust to reflect what's on the data validation values tab.	Document will be changed to align with tool
SERC	11	294	Figure 7 part - the cells should be 9 and 10, not 16 and 17	Adjust to acurately reflect lines 9 and 10.	Document will be changed to align with tool

Security Guideline	Security Guideline for the Electricity Sector: Assessing and Reducing Risk
Instructions	**Please use this form to submit comments on the draft Security Guideline. Comments must be submitted within the review period below to Tom Hofstetter (tom.hofstetter@nerc.net) with the words "Security Guideline: Assessing and Reducing Risk Comments" in the subject line. Only comments submitted in this Microsoft Excel format will be accepted. Both general and specific comments should be provided within this form.** Comments may be submitted by individuals or organizations. Please provide the requested information in Row 6. If comments are submitted on behalf of multiple organizations, list all organizations in Row 6. Please provide the Industry Segment and Region (if applicable) in Rows 7 and 8 and provide the requested contact information in Rows 9 and 10. If you have any questions regarding this process, please contact Tom Hofstetter (tom.hofstetter@nerc.net)
Review Period	December 18, 2020 -February 1, 2021

Name of Individual or Organization(s) (list multiple if submitted by a group):	Johnny Gest - Manager, Engineering and System Performance
Industry Segment (if applicable)	Regional Entity
Region (if applicable)	ReliabilityFirst
Contact Telephone	216.409-5428
Contact Email	johnny.gest@rfirst.org

Organization(s)	**Page #**	**Line / Paragraph**	**Comment**	**Proposed Change**	**NERC Response - summarized category**
ReliabilityFirst	2	54	Change "basked" to "based"	...developing risk based business justifications....	Document spelling change
ReliabilityFirst	1	7, 8, 9	It seems this line is missing critical components such as safety and resiliency. Safety of the customers and the people within the industry that work on bulk power system, should be above all other things. Additionally, Resiliency addresses the capability of the BPS when controls and protections fail, how can the system be brought back up.	Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that impact bulk power system (BPS) operations, safety, planning, security, and resiliency.	Document content change
ReliabilityFirst	1	14-15	Further emphasize the consideration of both the guidelines within this document AND the Reliability Standards.	......with the practices set forth in this guideline in coordination with the Reliability Guidelines.	Document content change
ReliabilityFirst	2	41-42	Formatting issue	Add a space between lines 41 and 42	Document format change
ReliabilityFirst	2	54	Add period to end of sentence.		Document gramar change
ReliabilityFirst	2	57	Add period to end of sentence.		Document gramar change
ReliabilityFirst	4	106/107	Sentence is missing something - needs clarification	...cybersecurity program against (missing something here) to identify potential gaps.	Document language clarification
ReliabilityFirst	5	162	Misspelling	"correct "annul" to "annual"	Document content change
ReliabilityFirst	6	170	ISO 27001 only talks about Information Security Management System (ISMS) framework which is a high-level governance framework that is made up of clauses that the management systems is "working." It does not contain the security controls within the ISO 27000 series. That is contained within the ISO 27002 document. This should also be changed in the DRAFT_Assessing and Reducing Risk Self Assessment Too_v1.0.xlsx . The mapping in the self assessment reference both the ISO 27001 clauses and 27002 controls. This should be changed in the Cyber Security Framework tab.	Security Programs: cybersecurity teams utilize NIST 800-53 or ISO 27001/ISO 27002 comprehensive security controls to compare implemented security programs	Document content change
ReliabilityFirst	9	263/264	Grammatically incorrect statement and inconsistent language - match language as shown in lines 274/275.	"Note: normalized/standardize ID" needs to be updated. Also use "Pivot Table" instead of "pivot table"	Document gramar change Will possibly change to "the normalized/standardize ID in Column A was created..."
ReliabilityFirst	11	301	Clarification needed.	Should "requirements" be "requirement"?	Document spelling change
ReliabilityFirst	11	307/312	Add period to end of sentence.		Document gramar change
ReliabilityFirst	General	General	Addition of a disclaimer	Determining that your organization has a lower risk based on the implementation levels does not guarantee compliance with the Reliability Standards.	Thank you for the feedback - both the self-assessment tool and associated job aid document will be updated to include a disclaimer consistent with the Supply Chain Working group products: "The objective of this tool is to distribute key practices and information on specific issues critical to promote and maintain a highly reliable and secure bulk power system (BPS). Security Guidelines are not binding norms or parameters to the level that"

ReliabilityFirst	General	General	Potential additional reference of ongoing efforts related to cyber security improvements	FERC NOPR 12-17-2020 incentives effort	Thank you for the suggestion. The NOPR was posted after the self-assessment tool and associated job aid document were complete, but the team will review and consider including as an additiona reference
ReliabilityFirst	N/A	N/A	The DRAFT_Assessing and Reducing Risk Self Assessment Tool_v1.0.xlsx does not contain document details on how an organization is meeting the default or organizationally defined tier. There should be a column added the self-assessment tab that could be used to keep notes or details as to what department/business area was reviewed, what policies/procedures were reviewed, and any follow up questions and interviews performed. Without an organization documenting those items, it would be difficult or impossible to identify gaps, next steps, after action items, and/or an overall roadmap that would be successful.	May want to provide a column or multiple columns for an organization to document the applicable Business Area/Business unit, Policies/Procedures reviewed, processes assessed and/or sampled, interviews performed, and/or follow-up questions and responses to the follow-up questions.	For the purposes of the 45-Day comment response, the spreadsheet was password protected, with capabilities to modify formual related values on the "data_validation_values" tab. The final approved version will have password restrictions removed so individual companies are free to update and modify to best meet their needs. One other possibility, if enough interest exist and another volunteer team is formed, additional capabilities could be added in a future release

Security Guideline	Security Guideline for the Electricity Sector: Assessing and Reducing Risk
Instructions	**Please use this form to submit comments on the draft Security Guideline. Comments must be submitted within the review period below to Tom Hofstetter (tom.hofstetter@nerc.net) with the words "Security Guideline: Assessing and Reducing Risk Comments" in the subject line. Only comments submitted in this Microsoft Excel format will be accepted. Both general and specific comments should be provided within this form.** Comments may be submitted by individuals or organizations. Please provide the requested information in Row 6. If comments are submitted on behalf of multiple organizations, list all organizations in Row 6. Please provide the Industry Segment and Region (if applicable) in Rows 7 and 8 and provide the requested contact information in Rows 9 and 10. If you have any questions regarding this process, please contact Tom Hofstetter (tom.hofstetter@nerc.net)
Review Period	December 18, 2020 -February 1, 2021

Name of Individual or Organization(s) (list multiple if submitted by a group):	Edison Electric Institute (Contact: Andrea Koch)
Industry Segment (if applicable)	N/A
Region (if applicable)	N/A
Contact Telephone	704-907-0392
Contact Email	akoch@eei.org

Organization(s)	**Page #**	**Line / Paragraph**	**Comment**	**Proposed Change**	**NERC Response**
Edison Electric Institute (Contact: Andrea Koch)			General Comments: EEI recommends that NERC convert this guideline to guidance or other resource tool to support industry security activities. NERC Guidelines are used "when addressing moderate impact sustained risks that are unlikely, and low impact sustained risks that are unlikely or likely (such as reduced or lack of equipment maintenance resulting in the loss of an individual element which is a low impact to BPS reliability, while the probability of failure increases over time). Reliability Guidelines are also used for those issues that are or are not in the ERO's jurisdiction, but are practices that improve reliability." Guidelines are an approach for managing a potential risk to reliability and outline approaches for managing potential risks to reliability in a particular area, including new or rapidly evolving risks. However, this document is a self-assessment tool to improve security. Specifically, this document is focused on assessing the security and compliance posture of a particular entity. Additionally, this guideline prescribes a particular approach for assessing risk and compliance posture and similar models currently exist that may be more appropriate for a particular entity or program. Because this document has a different purpose than a Guideline, and industry already uses various tools and models to assess security and level of maturity (e.g., DOE Cybersecurity Capability Maturity Model (C2M2) Program), EEI recommends that this self-assessment tool be included in another vehicle other than a guideline, such as guidance or other resource tool. Because a guideline imposes certain expectations on registered entities, if NERC determines that this document should remain a Guideline, EEI requests that NERC provide additional time to evaluate it		Thank you for the response - SWG and RSTC are actively working with NERC to identify best platform to hose such guidance as this. Regarding various other tools such as C2M2, the initial intent was to incorporate C2M2 into this verion of the tool (we had C2M2 representation on the team), but decided to wait until a future version to incoporate that until C2M2 2.0 is released. The other point the team considered, was Risk Management capabilities levels (CSF Risk Tiers) vs Maturity levels, we again decided to wait to see if C2M2 2.0 brings greater clarity and distinctions betwen the two .

Security Guideline	Security Guideline for the Electricity Sector: Assessing and Reducing Risk
Instructions	**Please use this form to submit comments on the draft Security Guideline. Comments must be submitted within the review period below to Tom Hofstetter (tom.hofstetter@nerc.net) with the words "Security Guideline: Assessing and Reducing Risk Comments" in the subject line. Only comments submitted in this Microsoft Excel format will be accepted. Both general and specific comments should be provided within this form.** Comments may be submitted by individuals or organizations. Please provide the requested information in Row 6. If comments are submitted on behalf of multiple organizations, list all organizations in Row 6. Please provide the Industry Segment and Region (if applicable) in Rows 7 and 8 and provide the requested contact information in Rows 9 and 10. If you have any questions regarding this process, please contact Tom Hofstetter (tom.hofstetter@nerc.net)
Review Period	December 18, 2020 -February 1, 2021

Name of Individual or Organization(s) (list multiple if submitted by a group):	Beverly Laios on behalf of American Electric Power
Industry Segment (if applicable)	
Region (if applicable)	
Contact Telephone	614-716-2307
Contact Email	bblaios@aep.com

Organization(s)	**Page #**	**Line / Paragraph**	**Comment**	**Proposed Change**	**NERC Response**
Beverly Laios on behalf of American Electric Power	N/A	N/A	While AEP appreciates the diligent efforts of all those who were involved in developing the content within this proposed Security Guideline and the self-assessment tool, AEP does not believe this tool and documentation is in a complete enough state for the Security Guideline to be approved. AEP's comments below outline some of the suggested changes that should be considered before finalizing the guideline. We also recommend that NERC convert this guideline to be a resource tool to support industry's security activities rather than a guideline once the identified mapping issues are addressed. A number of minor changes to grammar, spelling, and wording are recommended on the draft document. We also identified a number of inconsistencies in the wording/terminology referenced in the draft guideline document and the self-assessment tool. In additon, we identified several mapping issues between CIP and NIST. Listed below are the recommendations and observations.		Thank you for the feedback - the goal of the 45-day comment period was to obtain feedback such as this to help prepare it for final publication. The noted grammar and tool formula errors will be corrected and provided back for your review. Regarding guideline vs resource tool, that too is an active conversation underway between RSTC and NERC - the intent of SWG is to also provide resource tools such as this.
Beverly Laios on behalf of American Electric Power	DRAFT_Assessing and Reducing Risk Guide_v1.0.pdf	Page 5, Line 131	Numbers listed are incorrect.	"Orange for between 3.5-4.5 – moderate risk" should be corrected to read "Orange for between 1.5-2.5 – moderate risk".	Document will be changed to align with tool
Beverly Laios on behalf of American Electric Power	DRAFT_Assessing and Reducing Risk Guide_v1.0.pdf	Page 5, Line 138	Maturity level does not match assessment tool	"Level 5 represents high or very mature capabilities" should be corrected to read "Level 4 represents high or very mature capabilities" to match the assessment tool.	Document will be changed to align with tool
Beverly Laios on behalf of American Electric Power	DRAFT_Assessing and Reducing Risk Guide_v1.0.pdf	Page 5, Line 157	Formatting error	"Cybersecurity focus:" should be in boldface type to match lines 148 and 152.	Document boldface type will be changed to match
Beverly Laios on behalf of American Electric Power	DRAFT_Assessing and Reducing Risk Self Assessment Tool_v1.0.xlsx	data_validation_values tab & Self-Assessment tab	In the "data_validation_values" tab, the Tiers are described "Implementation Tier". In the "Self-Assessment" tab, the Tiers (columns I & J) are described as "Cybersecurity Risk Mgmt Tier" and "Risk Tier Descriptor".	The Framework should consider consistent naming.	Agreed - consistent naming will be helpful. The tool descriptors will be adjusted to "Implementation Tier" throughout for consistency

Beverly Laios on behalf of American Electric Power	DRAFT_Assessing and Reducing Risk Self Assessment Tool_v1.0.xlsx	Self-Assessment tab	It seems that what is noted as “Compliance related” in Column H may not be required by the NERC Standard.		Response - this team used the recently published NERC / NIST CIP to CSF mappings as a reference for the corresponding mappings to identify CSF-Subcategories with a Compliance relationship. Having said that, it is noted that with such cross-mappings there will be cases where a particular row will not be clearly Security or Compliance related - in the end, the intent was to deliver a tool to aid Responsible Entities in identifying areas of potential improvement and REs are free to change the provided relationships
Beverly Laios on behalf of American Electric Power	DRAFT_Assessing and Reducing Risk Self Assessment Tool_v1.0.xlsx	Self-Assessment tab	Not all the “CIP Requirement and Parts” (Column B) are matched correctly to the outcomes identified in Column G. For example, in cell G8, it is stated “Dependencies and critical functions for delivery of critical services are established” for CIP-002 R1. However, this is not a requirement for CIP-002. Another example, cell G10 noted “Physical devices and systems within the organization are inventoried” for CIP-002 R2. This mapping is incorrect and should be mapped to CIP-005. Another example of this is cell G11 which noted “Software platforms and applications within the organization are inventoried” for CIP-002 R2. This mapping is incorrect, this should be mapped to CIP-010.		Document language clarification Response - this team used the recently published NERC / NIST CIP to CSF mappings as a reference for the corresponding mappings to identify CSF-Subcategories with a Compliance relationship. Based on this feedback, the associated job aid document will be updated to include a statement along the lines: ... the outcomes in column G are not necessarily requirements (or that they equate with the NERC CIP requirement), but that they can be helpful for REs to improve their security posture while helping demonstrate compliance with NERC CIP requirements
Beverly Laios on behalf of American Electric Power	NIST CSF 1.1 to NERC CIP FINAL.XLSX	Guidance for combined NERC CIP and NIST CSF: Row 6	Cell H6 states that an Entity "Must establish a methodology that identifies the Bulk Electric System (BES) Cyber Systems which perform BES reliability operating services (BROS)" which implies that the BROS are a statement in the requirements of CIP-002 which they are not. The "BROS" only exist in the CIP-002 G&TB and thereby not mandatory nor enforceable.	The use of "Must" should be weakened or the reference to the "BROS" removed.	We appreciate the comment. The CIP to CSF mapping document was created by a collaborative NERC / NIST effort outside of this working group. Your comment will be passed to them for consideration in updates to the mapping.
Beverly Laios on behalf of American Electric Power	NIST CSF 1.1 to NERC CIP FINAL.XLSX	Guidance for combined NERC CIP and NIST CSF: Row 8	Cell H8 has a grammatical error in item 1 with the placement of the word "all" 1. Ensure inventory includes OT and IT all software that support reliable operations 2 Ensure for all registered functions that all BES reliability operating services preformed are identified and evaluated. Reference CIP-002 Guidelines and Technical Basis. - Dynamic Response to BES conditions - Balancing Load and Generation - Controlling Frequency (Real Power) - Controlling Voltage (Reactive Power) - Managing Constraints - Monitoring & Control - Restoration of BES - Situational Awareness - Inter-Entity Real-Time Coordination and Communication	"1. Ensure inventory includes OT and IT *all* software…" should be changed to "1. Ensure inventory includes *all* OT and IT software…"	We appreciate the comment. The CIP to CSF mapping document was created by a collaborative NERC / NIST effort outside of this working group. Your comment will be passed to them for consideration in updates to the mapping.
Beverly Laios on behalf of American Electric Power	NIST CSF 1.1 to NERC CIP FINAL.XLSX	Guidance for combined NERC CIP and NIST CSF: Row 8	Cell H8 item 2 references the BROS with the directive language "ensure". The integration of the BROS concept is neither mandatory nor enforceable and, as such, the use of "ensure" should be softened or removed.	Replace the inclusion of the BROS with languange requiring all of the Reliability Functions assigned by the NERC Functional model be included in evaluation (based on the Registration of the Entity).	We appreciate the comment. The CIP to CSF mapping document was created by a collaborative NERC / NIST effort outside of this working group. Your comment will be passed to them for consideration in updates to the mapping.
Beverly Laios on behalf of American Electric Power	NIST CSF 1.1 to NERC CIP FINAL.XLSX	CIP Mapping Logic: Row 10	Inclusion of the language "…especially consider the pending CIP-012-1 implementation plans" is not clear on scope as CIP-012 is specific to data linkds between control centers and not "between BCS" as this language would insinuate.	Update language to "Data communications between BCS should be documented as good security practice. This would include links/networks in-scope of CIP-012"	We appreciate the comment. The CIP to CSF mapping document was created by a collaborative NERC / NIST effort outside of this working group. Your comment will be passed to them for consideration in updates to the mapping.

Beverly Laios on behalf of American Electric Power	NIST CSF 1.1 to NERC CIP FINAL.XLSX	Guidance for combined NERC CIP and NIST CSF: Row 13	Cell H13 references BROS which is a concept that is neither mandatory nor enforceable.	If the goal is to ensure that all applicable BCS are covered, the reference should be changed from BROS to the Funtional Reliability Tasks assigned based on Registration and the NERC Functional Model.	We appreciate the comment. The CIP to CSF mapping document was created by a collaborative NERC / NIST effort outside of this working group. Your comment will be passed to them for consideration in updates to the mapping.
Beverly Laios on behalf of American Electric Power	NIST CSF 1.1 to NERC CIP FINAL.XLSX	Guidance for combined NERC CIP and NIST CSF: Row 15	Cell H15 references BROS which is a concept that is neither mandatory nor enforceable.	If the goal is to ensure that all applicable BCS are covered, the reference should be changed from BROS to the Funtional Reliability Tasks assigned based on Registration and the NERC Functional Model.	We appreciate the comment. The CIP to CSF mapping document was created by a collaborative NERC / NIST effort outside of this working group. Your comment will be passed to them for consideration in updates to the mapping.
Beverly Laios on behalf of American Electric Power	NIST CSF 1.1 to NERC CIP FINAL.XLSX	CIP Mapping Logic: Row 19	CIP Mapping Logic is Blank (Cell G19)	"CIP-004 Access Management programs should be inclusive of all parties with access to Applicable Systems as also described in ID.AM-6"	We appreciate the comment. The CIP to CSF mapping document was created by a collaborative NERC / NIST effort outside of this working group. Your comment will be passed to them for consideration in updates to the mapping.
Beverly Laios on behalf of American Electric Power	NIST CSF 1.1 to NERC CIP FINAL.XLSX	Guidance for combined NERC CIP and NIST CSF: Row 20	Cell H20 references BROS which is a concept that is neither mandatory nor enforceable.	If the goal is to ensure that all applicable BCS are covered, the reference should be changed from BROS to the Funtional Reliability Tasks assigned based on Registration and the NERC Functional Model.	We appreciate the comment. The CIP to CSF mapping document was created by a collaborative NERC / NIST effort outside of this working group. Your comment will be passed to them for consideration in updates to the mapping.
Beverly Laios on behalf of American Electric Power	NIST CSF 1.1 to NERC CIP FINAL.XLSX	Guidance for combined NERC CIP and NIST CSF: Row 21	Cell H21 references BROS which is a concept that is neither mandatory nor enforceable.	If the goal is to ensure that all applicable BCS are covered, the reference should be changed from BROS to the Funtional Reliability Tasks assigned based on Registration and the NERC Functional Model.	We appreciate the comment. The CIP to CSF mapping document was created by a collaborative NERC / NIST effort outside of this working group. Your comment will be passed to them for consideration in updates to the mapping.
Beverly Laios on behalf of American Electric Power	NIST CSF 1.1 to NERC CIP FINAL.XLSX	General	There are a significant number of spelling errors identified when running spell-check.	Once all entity comments are incorporated, perform final spell-check to correct errors.	We appreciate the comment. The CIP to CSF mapping document was created by a collaborative NERC / NIST effort outside of this working group. Your comment will be passed to them for consideration in updates to the mapping.

Agenda Item 9
Reliability and Security
Technical Committee Meeting
June 8, 2021

Implementation Guidance: Cloud Solutions and Encrypting BES Cyber System Information

Action

Endorse

Summary

The purpose of this Compliance Implementation Guidance is to provide examples for how encryption can be utilized to secure and restrict access to BES Cyber System Information in various commonly used cloud services. The RSTC endorsed this Compliance Implementation Guidance in June of 2020 and it was submitted to the ERO for approval. The ERO Enterprise identified some concerns with the guidance document and provided feedback to the team. The SWG made revisions to the document to address the ERO Enterprise's concerns and are seeking RSTC endorsement to submit the document to the ERO for endorsement as Compliance Implementation Guidance.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Compliance Implementation Guidance

Cloud Solutions and Encrypting BES Cyber System Information

June 2021

RELIABILITY | RESILIENCE | SECURITY

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

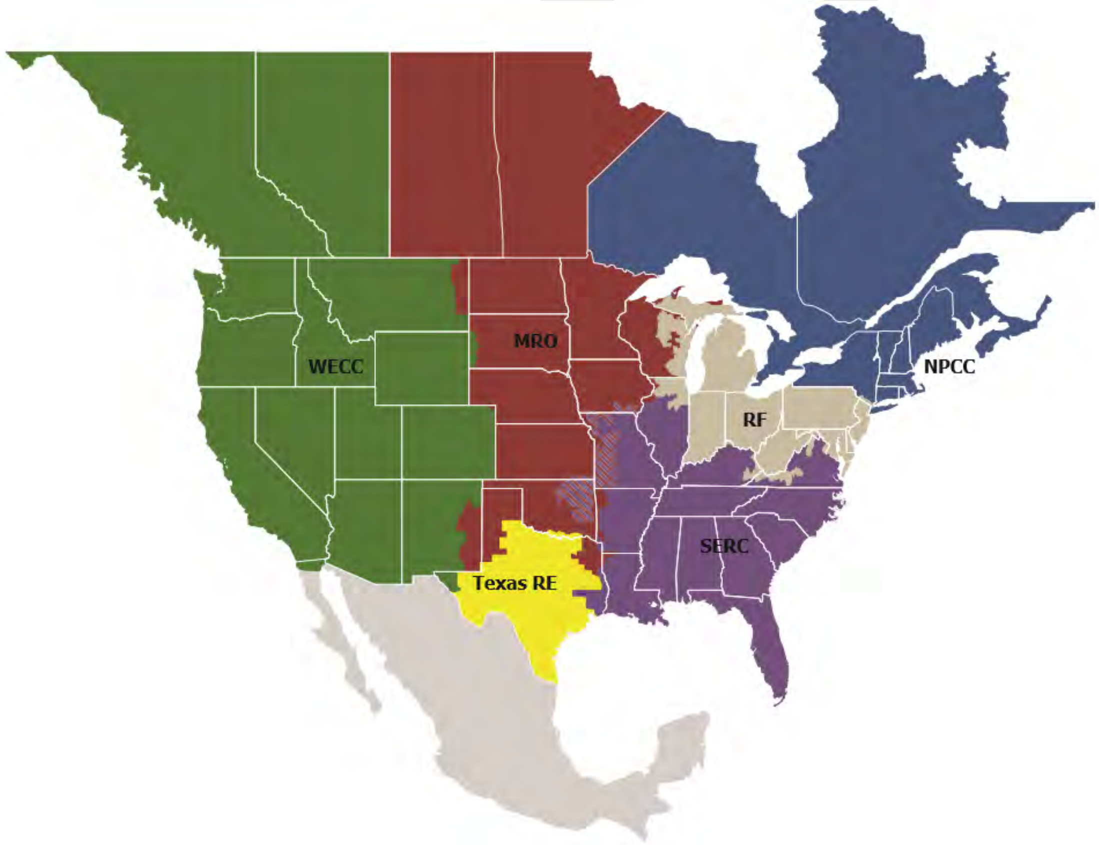
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners /Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Introduction

The following scenarios are intended to represent common use cases where BES Cyber System Information (BCSI) is in a cloud environment where encryption along with key management is being utilized to prevent unauthorized access and provide access control. The reference scenarios incorporate comprehensive analysis of two key supporting documents,

- ERO Enterprise CMEP Practice Guide: BES Cyber System Information
- Security Guideline for Electricity Sector: Primer for Cloud Solutions and Encrypting BCSI

This document focuses on compliant use of encryption, even though other methods to secure BCSI in the Cloud exist. This document is not intended to establish new requirements under NERC's Reliability Standards, to modify the requirements in any existing Reliability Standards, nor provide an interpretation under Section 7 of the Standard Processes Manual[1]. Additionally, there may be other ways to fulfill the obligations of the Requirements that are not expressed within this document.

Listed below are fundamental terms and considerations to keep in mind when reviewing the scenarios. This does not include all possible terms for cloud and encryption:

Terms

- Encryption – The reversible transformation of data into a form unreadable by anyone without the decryption key. Encryption preserves privacy by keeping the information hidden from anyone for whom it is not intended, even when the encrypted data is visible to the user
- Shared Responsibility Model – In cloud-based solutions, security and compliance responsibilities are shared between the
- Cloud Service Provider (CSP) and the Responsible Entity. The Responsible Entity maintains responsibility of implementing due diligence assurance measures/configurations over the CSP's portion of implemented security and compliance controls. NOTE: Controls associated with the Overlay and Underlay may also be referred to as a Shared Responsibility model. See **Appendix B** for a description and visual depiction.

Considerations

- The Responsible Entity needs to account for any BCSI being utilized on its own premise, separate from what is being utilized in the cloud environment, for all states (at rest, in transit and use). This document only addresses the cloud environment.
- Access for the Responsible Entity's personnel, and associated evidence, is not in scope of this document. This is focused on the CSP access
- If CSP personnel concurrently have access to the keys (for support, etc.) and the encrypted BCSI, then those individuals are considered to have the ability to "obtain and use" BCSI and therefore are considered having electronic access to BCSI. However, unauthorized individuals who obtain encrypted BCSI, but have no ability to use it within a meaningful timeframe, are not considered to have access. [2]
- If CSP personnel have physical access to the location where the Responsible Entity's encrypted BCSI is stored, they are deemed to have physical access per CIP-004-6 R4.1.3 only if those same personnel also have the

[1] https://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

[2] ERO Enterprise CMEP Practice Guide: BES Cyber System Information 4/26/2019

encryption key(s). Personnel with physical access, but no access to encrypted keys, are deemed to not have physical access to BCSI.[3]

- The terms ‘storage’ and ‘at rest’ are synonymous
- Terms listed in the scenarios may not correspond as exact matches with all cloud solutions
- Responsible Entity has identified the applicable data states (transit, storage, use) for their cloud implementation
- Responsible Entity has provisions in place ensuring current encryption best practices are maintained (e.g. Federal Information Protection Standards (FIPS) 140-2)
- Most of the requirements referenced below do not apply to Medium Impact BES Cyber Systems without ERC
- Use of BCSI is not addressed in the scenarios below, as BCSI in the cloud environment may not have a “use” state; it is up to each entity as to how they define “use” and whether that state exists in their specific implementation.

[3] ERO Enterprise CMEP Practice Guide: BES Cyber System Information 4/26/2019

Chapter 1: Cloud Specific Scenarios

Some typical scenarios using specific vendors for implementations of cloud technology are shown in this chapter. Options exist in structuring arrangements between the Responsible Entity and the CSP. These scenarios present possible options for providing CIP requirements assurance evidence measures within a cloud environment. Note: The specific products, security solutions and associated nomenclature may change over time. Additionally, any mention of specific vendors and their services is not considered an endorsement of any kind. These scenarios are simply intended to illustrate security concepts and the compliance impacts associated with each.

Microsoft 365

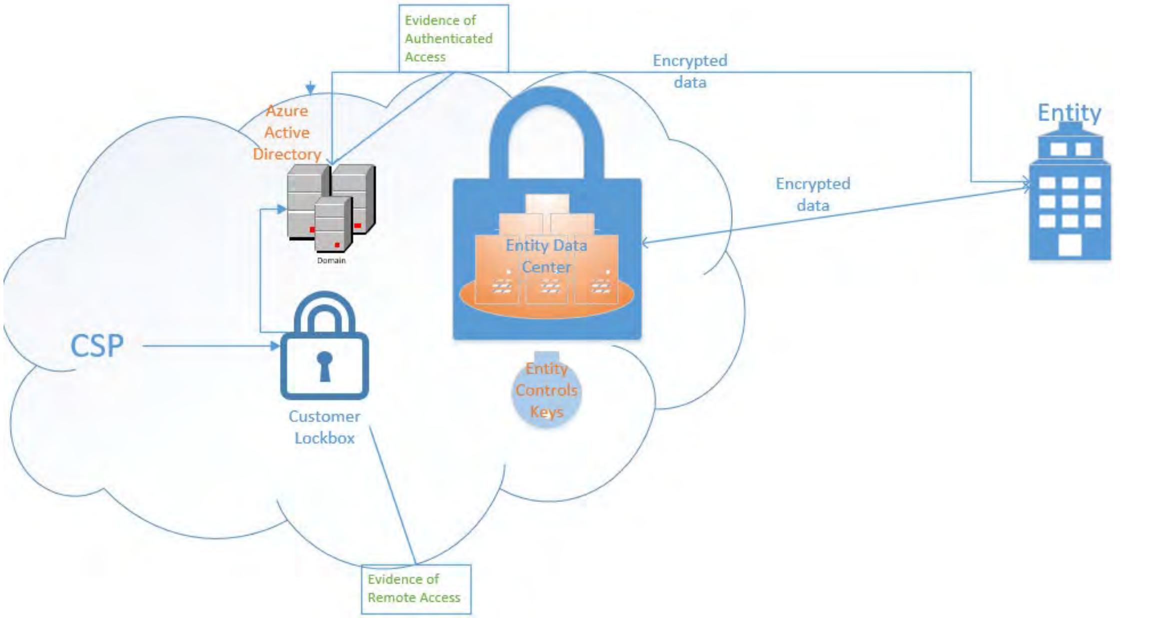
The following scenarios are intended to reflect what evidence may be used to demonstrate compliance, depending on how the registered entity chose to implement the solution.

1. **CSP manages keys and stores keys**

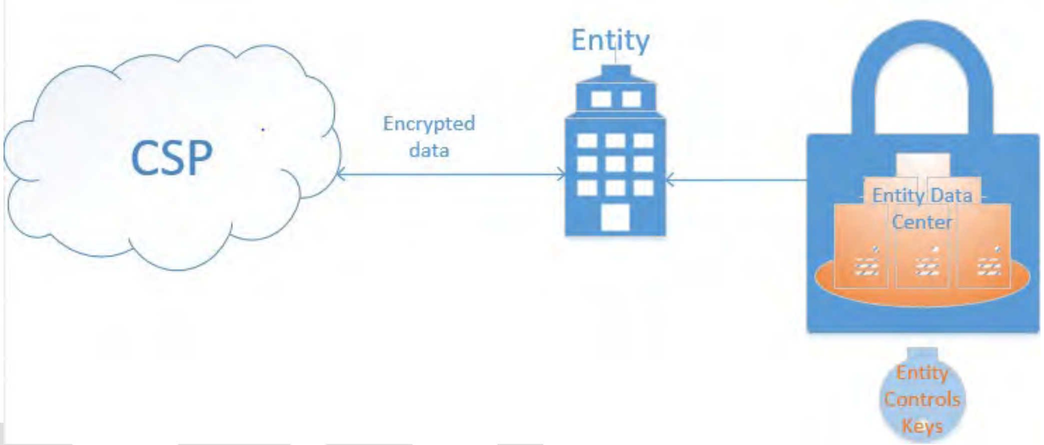
Compliance Impact	Evidence Examples	Applicable Requirements
CSP has access to BCSI	Examples of evidence may include: • Documentation of the security controls implemented within CSP's environment that satisfy the applicable requirements, • Documented authorization process (CIP-004-6 R4.1.3), • List of CSP individuals with access (CIP-004-6 R4.1.3), • 15-month access review for CSP personnel (CIP-004-6 R4.4), • Revocation within 24 hours of notification for terminations (CIP-004-6 R5.3), and • Evidence of the application of encryption (CIP-011-2 R1.2)	CIP-004-6 R4.1.3 R4.4 R5.3 CIP-011-2 R1.2
	Additional Supporting Evidence	
	The following are additional evidence examples that could be utilized to demonstrate that security controls have been implemented by the CSP and are meeting the security objectives, along with the Responsible Entity's due diligence of such: • Independent audit validating the implementation of the documented security controls and effectiveness of those controls, • Contractual language binding the CSP to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.	

2. **Responsible Entity provides root keys (Customer Key) and manages and stores those keys in Azure vault (CSP) and CSP access is managed by Customer Lockbox**

Compliance Impact	Evidence Examples	Applicable Requirements
CSP has access to key store (and therefore could have electronic access to BCSI)	Examples of evidence may include: • Documentation of the security controls implemented within CSP's environment or solution that satisfy the applicable requirements, • List of authorized personnel from Azure Active Directory (CIP-004-6 R4.1.3 and 4.4), • Evidence of implementation of Customer Lockbox to manage support access requests and authorization (CIP-004-6 R4.1.3), • Logs showing each Customer Lockbox access / usage (including start and end date/time for each use) and associated authorization (CIP-004-6 R4.4 and 5.3), • Evidence of the application of encryption at rest and in transit (CIP-011-2 R1.2),	CIP-004-6 R4.1.3 R4.4 R5.3 CIP-011-2 R1.2
	Additional Supporting Evidence	
	The following are additional evidence examples that could be utilized to demonstrate that security controls have been implemented by the CSP and are meeting the security objectives, along with the Responsible Entity's due diligence of such: • Independent audit validating the implementation of the documented security controls and effectiveness of those controls, • Contractual language binding the CSP to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.	

Compliance Impact	Evidence Examples	Applicable Requirements
		

3. **Bring Your Own Key (BYOK) and the Responsible Entity stores them onsite or outside the cloud environment (Responsible Entity privately creates/manages keys and does not use Azure to store keys)**

Compliance Impact	Evidence Examples	Applicable Requirements
CSP personnel do not have access to BCSI	Responsible Entity must demonstrate that BCSI is encrypted and not accessible by CSP personnel (CIP-011-2 R1.2). Evidence of this may include any of the following: • Evidence that keys are being managed on premise or by a third party, such as report or screenshot from the key management tool. • Agreement or purchase order with CSP showing what services have been implemented, including detail of how the services have been implemented • Evidence to show encryption of information determined by the Responsible Entity such as a firewall policy or configuration output report	CIP-011-2 R1.2
	 CSP Encrypted data Entity Entity Data Center Entity Controls Keys	

ServiceNow Ticketing System

The following scenarios are intended to reflect what evidence may be used to demonstrate compliance, depending on how the registered entity chose to implement the solution.

1. **CSP manages keys and stores keys**

Compliance Impact	Evidence Examples	Applicable Requirements
CSP has access to BCSI	Examples of evidence may include: • Documentation of the security controls implemented within CSP's environment or solution that satisfy the applicable requirements, • Documented authorization process (CIP-004-6 R4.1.3), • List of CSP individuals with access (CIP-004-6 R4.1.3), • 15-month access review for CSP personnel (CIP-004-6 R4.4), • Revocation within 24 hours of notification for terminations (CIP-004-6 R5.3), and	CIP-004-6 R4.1.3 R4.4 R5.3 CIP-011-2 R1.2

Compliance Impact	Evidence Examples	Applicable Requirements
	• Evidence of the application of encryption at rest and in transit (CIP-011-2 R1.2)	
	Additional Supporting Evidence	
	The following are additional evidence examples that could be utilized to demonstrate that security controls have been implemented by the CSP and are meeting the security objectives, along with the Responsible Entity's due diligence of such: • Independent audit validating the implementation of the documented security controls and effectiveness of those controls, • Contractual language binding the CSP to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.	

2. **Responsible Entity manages key and stores in vault provided by the CSP; the CSP does not inherently have access to key store nor the Responsible Entity's data**

Compliance Impact	Evidence Examples	Applicable Requirement
CSP could be provisioned access to key store and/or data (both would be necessary to access BCSI)	Examples of evidence may include: • Documentation of the security controls implemented within CSP's environment that satisfy the applicable requirements, • Documented authorization process (CIP-004-6 R4.1.3), • List of CSP individuals with access to BCSI, if any (CIP-004-6 R4.1.3), • 15-month access review for CSP personnel (CIP-004-6 R4.4), • Revocation within 24 hours of notification, for terminations (CIP-004-6 R5.3), and • Evidence of the application of encryption at rest and in transit (CIP-011-2 R1.2)	CIP-004-6 R4.1.3 R4.4 R5.3 CIP-011-2 R1.2
	Additional Supporting Evidence	
	The following are additional evidence examples that could be utilized to demonstrate that security controls have been implemented by the CSP and are meeting the security objectives, along with the Responsible Entity's due diligence of such: • Independent audit validating the implementation of the documented security controls and effectiveness of those controls, • Contractual language binding the CSP to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.	

Compliance Impact	Evidence Examples	Applicable Requirement

3. **BYOK and Client Storage (the Responsible Entity stores the keys on premise or with a third party outside the cloud environment)**

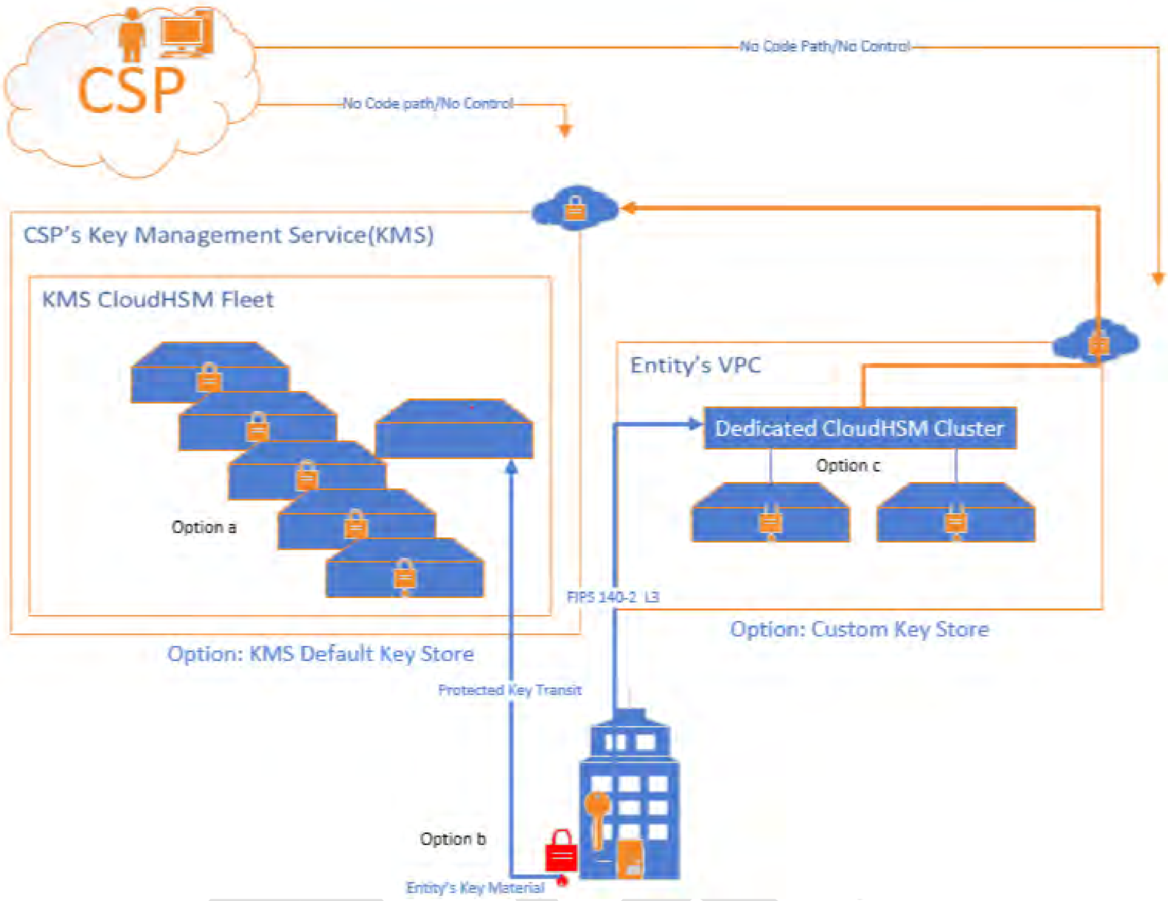
Compliance Impact	Evidence Examples	Applicable Requirements
CSP personnel do not have access to BCSI	Responsible Entity must demonstrate that BCSI is encrypted and not accessible by CSP personnel (CIP-011-2 R1.2). Evidence of this may include any of the following: • Evidence that keys are being managed on premise or by a third party, such as report or screenshot from the key management tool. • Agreement or purchase order with CSP showing what services have been implemented, including detail of how the services have been implemented • Evidence to show encryption of information determined by the Responsible Entity such as a firewall policy or configuration output report	CIP-011-2 R1.2

Amazon Web Services

Amazon Web Services (AWS) Key Management System (KMS) is integrated with AWS services to encrypt data at rest and in transit. Customer master keys (CMK) are owned and managed by the Customer (Responsible Entity) within their account. Most AWS services that are integrated with KMS support customer-managed CMKs which allows the customer to manage the keys themselves. Other services may only support AWS-managed CMKs — these CMKs are still unique to the customer's AWS account and provide the same audit visibility to log files. Data protection controls are also provided by other services depending on the functional operations of the actual implementation. The scenarios listed here illustrate three arrangement options for a Responsible Entity to manage keys in AWS KMS and store data that the Responsible Entity determines to contain BCSI in cloud storage service:

- Responsible Entity manages key and stores in AWS KMS (CSP) - Multi-tenant Hardware Security Module (HSM)
- Responsible Entity brings own keys and manages key in AWS KMS -- Multi-tenant HSM
- Responsible Entity manages key and stores in AWS KMS (CSP), Dedicated HSM

In all three scenarios, AWS personnel do not have an ability to access the keys.

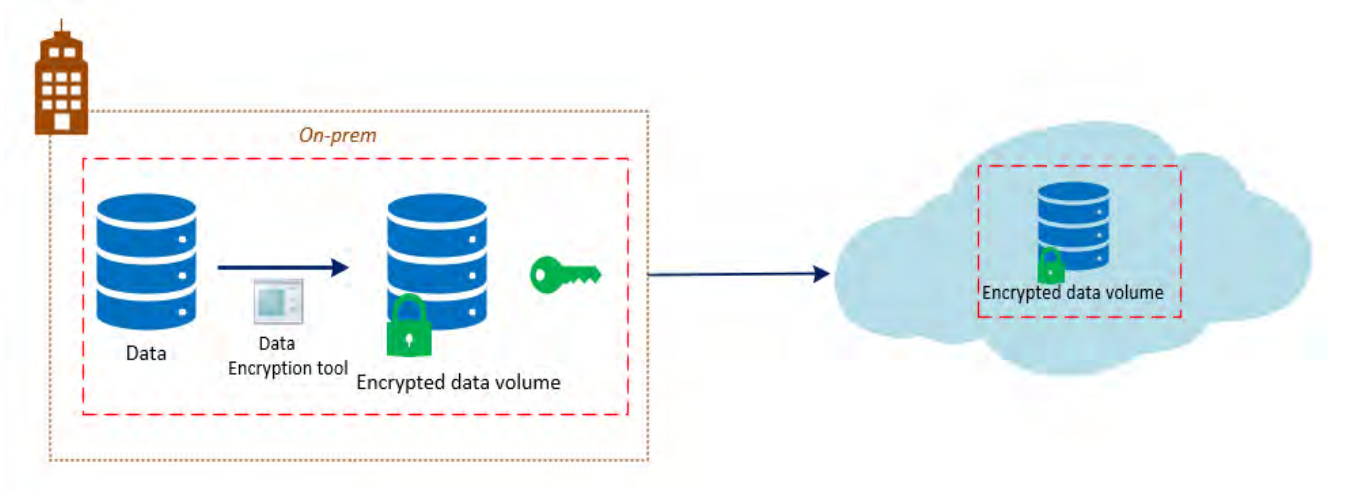


Compliance Impact	Evidence Examples	Applicable Requirements
CSP does not have access to key material or BCSI and no 'code path' access exists As part of Shared Responsibility, the Responsible Entity manages access to the BCSI	Responsible Entity must demonstrate that BCSI is encrypted and not accessible by CSP personnel (CIP-011-2 R1.2). Evidence of this may include any of the following: • Evidence that keys are being managed on premise or by a third party, such as report or screenshot from the key management tool. • Agreement or purchase order with CSP showing what services have been implemented, including detail of how the services have been implemented • Evidence to show encryption of information determined by the Responsible Entity such as a firewall policy or configuration output report	CIP-011-2 R1.2

CommVault Storage/Backup in the cloud

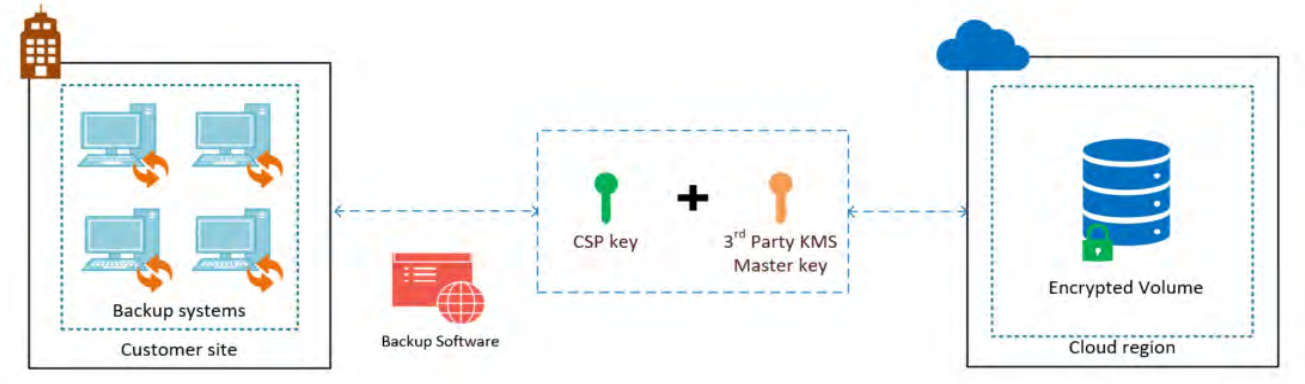
The following scenarios are intended to reflect what evidence may be used to demonstrate compliance, depending on how the registered entity chose to implement the solution.

1. **Encrypted BCSI repository storage (backup) and BYOK – Registered entity encrypts BCSI repositories on-prem using their own keys and stores these repositories in the cloud.**

Compliance Impact	Evidence Examples	Applicable Requirements
CSP does not have access to BCSI	Responsible Entity must demonstrate that BCSI is encrypted and not accessible by CSP personnel (CIP-011-2 R1.2). Evidence of this may include any of the following: • Evidence that keys are being managed on premise or by a third party, such as report or screenshot from the key management tool. • Agreement or purchase order with CSP showing what services have been implemented, including detail of how the services have been implemented • Evidence to show encryption of information determined by the Responsible Entity such as a firewall policy or configuration output report	CIP-011-2 R1.2
 On-prem Data Data Encryption tool Encrypted data volume Encrypted data volume		

2. **Registered entity encrypts BCSI on-prem – Using a master key provided by third party KMS in combination with the key provided by CSP to encrypt the BCSI. Once encrypted, BCSI is stored in the CSP environment. Therefore, only the Responsible Entity personnel have access to BCSI.**

Compliance Impact	Evidence Example	Applicable Requirements
Neither the CSP nor the third party KMS have access to BCSI	Responsible Entity must demonstrate that BCSI is encrypted and not accessible by CSP personnel (CIP-011-2 R1.2). Evidence of this may include any of the following: • Evidence that keys are being managed on premise or by a third party, such as report or screenshot from the key management tool. • Agreement or purchase order with CSP showing what services have been implemented, including detail of how the services have been implemented	CIP-011-2 R1.2

<table>
<tr><th>Compliance Impact</th><th>Evidence Example</th><th>Applicable Requirements</th></tr>
<tr><td></td><td>• Evidence to show encryption of information determined by the Responsible Entity such as a firewall policy or configuration output report
• Evidence to show BCSI repository is stored only in encrypted form in the cloud and keys Cannot be used by CSP where the repository is stored</td><td></td></tr>
<tr><td colspan="3">
</td></tr>
</table>

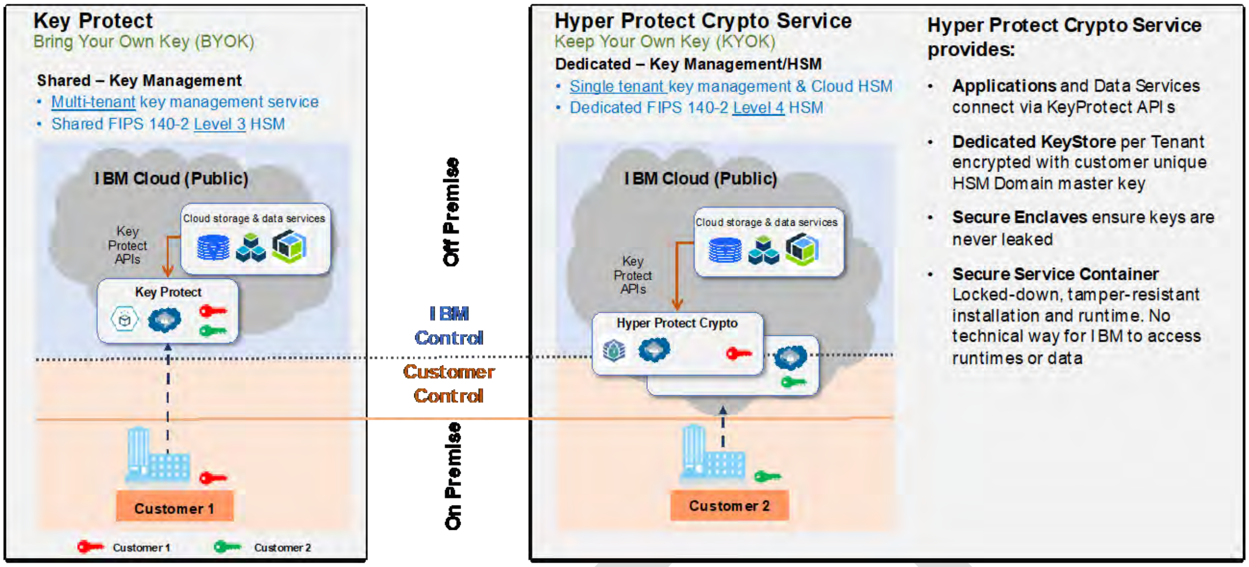
IBM Cloud

IBM Cloud has two options for Key Management Systems:

- IBM Cloud Key Protect – Multi-tenant key management system that enables Bring Your Own Key (BYOK) on a FIPS 140-2 level 3, multi-tenant hardware security module (HSM) device
- Hyper Protect Crypto Services (HPCS) – Single-tenant FIPS 140-2 level 4 HSM key management system that enables registered entities to Keep Your Own Key (KYOK)

Both Key Protect and HPCS are integrated with a number of IBM Cloud Services to enable encryption for data at rest and in transit with BYOK/KYOK.

KYOK further allows for complete isolation and control of stored data. In a KYOK scenario the customer takes ownership of the HSM through a Key Ceremony and becomes the custodian of the HSM that is dedicated to the HPCS instance the customer provisions. Once a customer takes ownership, the CSP has no access to the HSM and therefore no access to the data. Only the registered entity can access/decrypt.


Key Protect
Bring Your Own Key (BYOK)
Shared – Key Management
• Multi-tenant key management service
• Shared FIPS 140-2 Level 3 HSM
IBM Cloud (Public)
Cloud storage & data services
Key Protect APIs
Key Protect
Customer 1
Customer 1
Customer 2
Off Premise
IBM Control
Customer Control
On Premise
Hyper Protect Crypto Service
Keep Your Own Key (KYOK)
Dedicated – Key Management/HSM
• Single tenant key management & Cloud HSM
• Dedicated FIPS 140-2 Level 4 HSM
IBM Cloud (Public)
Cloud storage & data services
Key Protect APIs
Hyper Protect Crypto
Customer 2

Hyper Protect Crypto Service provides:

- **Applications** and Data Services connect via KeyProtect APIs
- **Dedicated KeyStore** per Tenant encrypted with customer unique HSM Domain master key
- **Secure Enclaves** ensure keys are never leaked
- **Secure Service Container** Locked-down, tamper-resistant installation and runtime. No technical way for IBM to access runtimes or data

The following scenarios are intended to reflect what evidence may be used to demonstrate compliance, depending on how the registered entity chose to implement the solution.

1. **Key Protect/Bring Your Own Key (BYOK) – Registered entity creates and manages keys outside the cloud environment; keys are stored in the CSP's multi-tenant HSM where some CSP personnel have access.**

Compliance Impact	Evidence Example	Applicable Requirements
CSP could have access to BCSI (Electronic Only)	Examples of evidence may include: • Documentation of the security controls implemented within CSP's environment that satisfy the applicable requirements, • Evidence that keys are being managed on premise or by a third party, such as report or screenshot from the key management tool • Documented authorization process (CIP-004-6 R4.1.3), • List of CSP individuals with access (CIP-004-6 R4.1.3), • 15-month access review for CSP personnel (CIP-004-6 R4.4), • Revocation within 24 hours of notification for terminations (CIP-004-6 R5.3), • Evidence of the application of encryption (CIP-011-2 R1.2),	CIP-004-6 R4.1.3 R4.4 R5.3 CIP-011-2 R1.2
	Additional Supporting Evidence	
	The following are additional evidence examples that could be utilized to demonstrate that security controls have been implemented by the CSP and are meeting the security objectives, along with the Responsible Entity's due diligence of such: • Independent audit validating the implementation of the documented security controls and effectiveness of those controls,	

Compliance Impact	Evidence Example	Applicable Requirements
	- Contractual language binding the CSP to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.	

2. **HPCS/Keep Your Own Key (KYOK) - Registered entity creates and manages keys outside the cloud environment; keys are stored in the CSP's single tenant HSM; the CSP does not have access to the HSM, once the key ceremony has occurred.**

Compliance Impact	Evidence Example	Applicable Requirements
CSP has no access to BCSI (KYOK Scenario)	Responsible Entity must demonstrate that BCSI is encrypted and not accessible by CSP personnel. Examples of evidence may include: • Key Ceremony registry (to demonstrate Master Key creation and sharding) • Logging and alerting of unauthorized access to the HSM • Evidence that keys, including KYOK master, are being managed on premise or by a third party, such as report or screenshot from the key management tool. • Agreement or purchase order with CSP showing what services have been implemented, including detail of how the services have been implemented • Evidence to show BCSI repository is stored only in encrypted form in the cloud • Evidence to show that data repository is encrypted	CIP-011-2 R1.2

Appendix A: References

Microsoft
https://docs.microsoft.com/en-us/microsoft-365/compliance/service-encryption-with-customer-key-faq
https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption
https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security
https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests
https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-service-encryption?view=o365-worldwide

Amazon Web Service
https://aws.amazon.com/compliance/services-in-scope/
https://marketplace.fedramp.gov/#/products?sort=productName
https://aws.amazon.com/blogs/security/are-kms-custom-key-stores-right-for-you/
https://d1.awsstatic.com/whitepapers/aws-support-compliance-nerc-cip-standards.pdf?did=wp_card&trk=wp_card

IBM
https://www.ibm.com/cloud
https://www.ibm.com/cloud/hyper-protect-crypto
https://www.ibm.com/cloud/hyper-protect-dbaas
https://www.ibm.com/cloud/hyper-protect-virtual-servers
https://www.ibm.com/cloud/compliance
https://www.ibm.com/security/cryptocards/hsms

FIPS/NIST Encryption Standards
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

NERC CIPC/RSTC Security Guidelines
Risks related to CSPs: https://www.nerc.com/comm/CIPC_Security_Guidelines_DL/Security_Guideline-Cloud_Computing.pdf
Security Guideline for Electricity Sector: Primer for Cloud Solutions and Encrypting BCSI

Appendix B: Recommended Controls

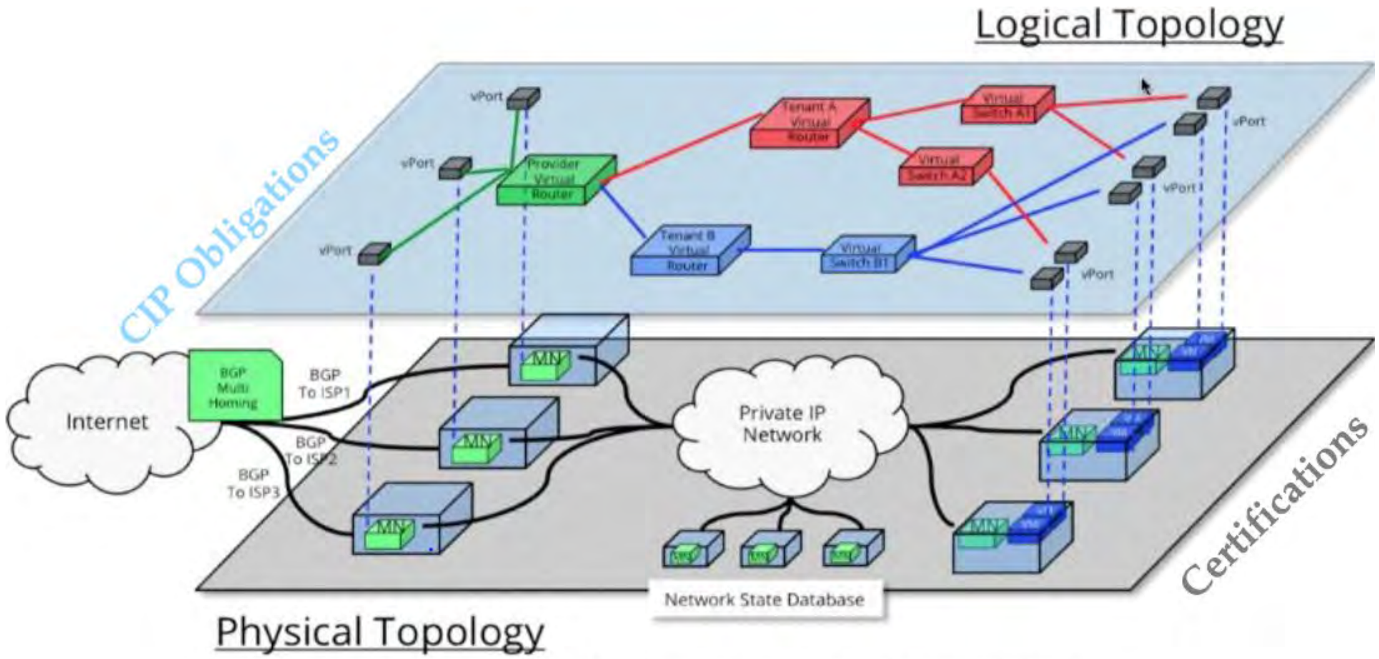
The following is a list of recommended controls that the registered entity should ensure are implemented for their cloud scenario. For more detail about these controls and their associated certifications, visit the Cloud Security Alliance website[4].

- Implements cryptographic mechanisms to protect the confidentiality and integrity of information stored during transport and at rest,
- Prevent unauthorized disclosure of information and detect changes to information,
- Protects the authenticity of communication sessions,
- Employs the principle of least privilege, allowing only authorized accesses for users which are necessary to accomplish assigned tasks,
- Monitors information system accounts for atypical use and reports atypical usage of information system accounts,
- Authorizes access to the information system,
- Employs automated mechanisms to support the management of information system accounts,
- Terminates user and shared/group account credentials when members leave the group,
- Reviews accounts annually,
- Monitors information system accounts for atypical use and reports atypical usage of information system accounts

Underlay and Overlay Model

- Underlay (security of the cloud) – Infrastructure (and associated controls) implemented by the CSP that runs all services offered by the CSP. This infrastructure could be composed of the hardware, software, networking, and facilities that run Cloud services offered. The security and controls associated with this infrastructure is likely verified through certifications or other internal/external activities such as penetration testing. (see picture below)
- Overlay (security in the cloud) – The portion of the cloud service/product that sits on top of the underlay and has been developed for the customer's use. In some cloud environments, the CSP may have the ability to access data in portions of the Overlay. Whereas in other cloud environments the CSP has no ability to access data in the Overlay.(see picture below)

[4] https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1-info-sheet/



http://bradhedlund.com/2012/10/06/mind-blowing-l2-l4-network-virtualization-by-midokura-midonet/

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

~~Compliance Implementation Guidance~~

~~Cloud Solutions and Encrypting BCSI | June 10, 2020~~

~~Chapter 1Introduction~~

Compliance Implementation Guidance

Cloud Solutions and Encrypting BES Cyber System Information

June 2021

RELIABILITY | RESILIENCE | SECURITY

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

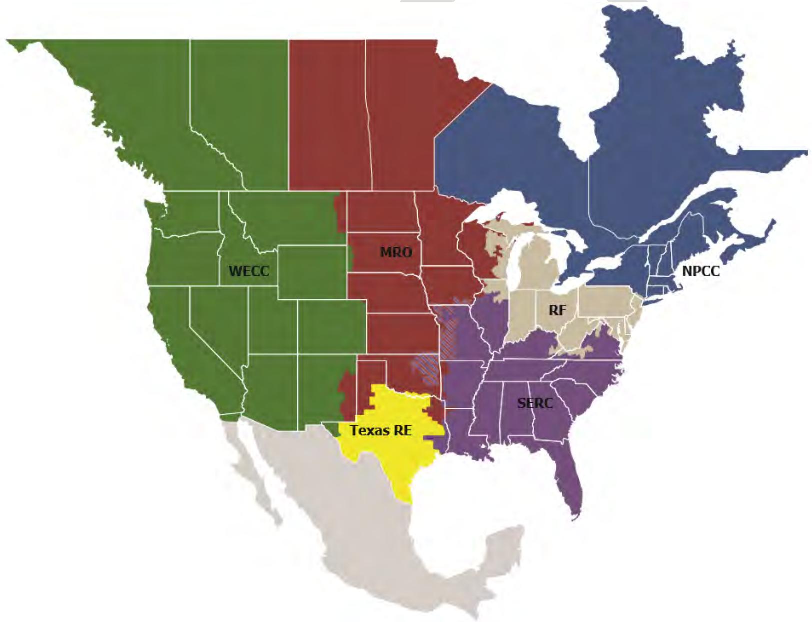
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Introduction

The following scenarios are intended to represent common use cases where ~~bulk electric system (~~BES~~)~~ Cyber System Information (BCSI) is in a cloud environment where encryption along with key management is being utilized to prevent unauthorized access and provide access control. The reference scenarios incorporate comprehensive analysis of two key supporting documents,

~~1. ERO Enterprise CMEP Practice Guide: BES Cyber System Information~~

- ~~Security Guideline for Electricity Sector: Primer for Cloud Solutions and Encrypting BCSI~~ ERO Enterprise CMEP Practice Guide: BES Cyber System Information
- Security Guideline for Electricity Sector: Primer for Cloud Solutions and Encrypting BCSI

This document focuses on compliant use of encryption, even though other methods to secure BCSI in the Cloud exist. This document is not intended to establish new requirements under NERC's Reliability Standards, to modify the requirements in any existing Reliability Standards, nor provide an interpretation under Section 7 of the Standard Processes Manual~~.~~[1]. Additionally, there may be other ways to fulfill the obligations of the Requirements that are not expressed within this document.

~~Terms~~

Listed below are fundamental terms and considerations to keep in mind when reviewing the scenarios. This does not include all possible terms for cloud and encryption:

Terms

- Encryption ~~-~~– The reversible transformation of data into a form unreadable by anyone without the decryption key. Encryption preserves privacy by keeping the information hidden from anyone for whom it is not intended, even when the encrypted data is visible to the user
- Shared Responsibility Model – In cloud-based solutions, security and compliance responsibilities are shared between the ~~cloud service provider~~
- Cloud Service Provider (CSP) and the Responsible Entity. The Responsible Entity maintains responsibility of implementing due diligence assurance measures/configurations over the ~~cloud service provider's~~CSP's portion of implemented security and compliance controls. NOTE: Controls associated with the Overlay and Underlay may also be referred to as a Shared Responsibility model. See ~~the **Appendix**~~**Appendix B** for a description and visual depiction.

Considerations

- The Responsible Entity needs to account for any BCSI being utilized on its own ~~premises~~premise, separate from what is being utilized in the cloud environment, for all states (at rest, in transit and use). This ~~documents~~document only addresses the cloud environment.
- Access for the Responsible Entity's personnel, and associated evidence, is not in scope of this document. This is focused on the ~~Cloud Service Provider~~CSP access
- If ~~Cloud Service Provider~~CSP personnel concurrently have access to the keys (for support, etc.) and the encrypted BCSI, then those individuals are considered to have the ability to "obtain and use" BCSI and therefore are considered having electronic access to BCSI. However, unauthorized individuals who obtain

[1] https://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

encrypted BCSI, but have no ability to use it within a meaningful timeframe, are not considered to have access. [2]

- If ~~Cloud Service Provider~~CSP personnel have physical access to the location where the Responsible Entity's encrypted BCSI is stored, they are deemed to have physical access per CIP-004-6 R4.1.3 only if those same personnel also have the encryption key(s). Personnel with physical access, but no access to encrypted keys, are deemed to not have physical access to BCSI~~.~~~~[1]~~.[3]
- The terms '~~*Storage'*~~storage' and '~~*At Rest'*~~at rest' are synonymous
- Terms listed in the scenarios may not correspond as exact matches with all cloud solutions
- Responsible Entity has identified the applicable data states (transit, storage, use) for their cloud implementation
- Responsible Entity has provisions in place ensuring current encryption best practices are maintained (e.g. Federal Information Protection Standards (FIPS) 140-2)
- Most of the requirements referenced below do not apply to Medium Impact BES Cyber Systems without ERC
- Use of BCSI is not addressed in the scenarios below, as BCSI in the cloud environment may not have a "use" state; it is up to each entity as to how they define "use" and whether that state exists in their specific implementation.

[2] ~~See the 4/26/2019 ERO Enterprise CMEP Practice Guide: BES Cyber System Information~~ ERO Enterprise CMEP Practice Guide: BES Cyber System Information 4/26/2019

[3] ERO Enterprise CMEP Practice Guide: BES Cyber System Information 4/26/2019

~~Chapter 2~~Chapter 1: Cloud ~~–~~Specific Scenarios

~~Below are some~~

Some typical scenarios using specific vendors for implementations of cloud technology~~.~~ are shown in this chapter. Options exist in structuring arrangements between the Responsible Entity and the ~~Cloud Service Provider~~CSP. These scenarios present possible options for providing CIP requirements assurance evidence measures within a cloud environment. Note: The specific products, security solutions and associated nomenclature may change over time. Additionally, any mention of specific vendors and their services is not considered an endorsement of any kind. These scenarios are simply intended to illustrate security concepts and the compliance impacts associated with each.

Microsoft 365

The following scenarios are intended to reflect what evidence may be used to demonstrate compliance, depending on how the registered entity chose to implement the solution.

1. **~~Cloud Service Provider~~ CSP manages keys and stores keys**

Compliance Impact	Evidence ~~Example~~Examples	Applicable Requirements
~~Cloud Service Provider~~ CSP has access to BCSI	~~All~~Examples of ~~the following would be required~~evidence may include: • Documentation of the security controls implemented within ~~Cloud Service Provider's~~CSP's environment that satisfy the applicable requirements, • ~~Independent audit validating the implementation of the documented security controls and effectiveness of those controls,~~ • ~~Contractual language binding the cloud service provider to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.~~ • Documented authorization process (CIP-004-6 R4.1.3), • List of ~~Cloud Service Provider~~CSP individuals with access (CIP-004-6 R4.1.3), • ~~Logging and monitoring of BCSI storage location user activity, if possible/available (to confirm accuracy of the list of Cloud Service Provider individuals) (CIP-004-6 R4.1.3 and R4.4)~~ • 15-month access review for ~~Cloud Service Provider~~CSP personnel (CIP-004-6 R4.4), • Revocation within 24 hours of notification for terminations (CIP-004-6 R5.3), and • Evidence of the application of encryption (CIP-011-2 R1.2)	CIP-004-6 R4.1.3 R4.4 R5.3 CIP-011-2 R1.2
	Additional Supporting Evidence	
	The following are additional evidence examples that could be utilized to demonstrate that security controls have been implemented by the CSP	

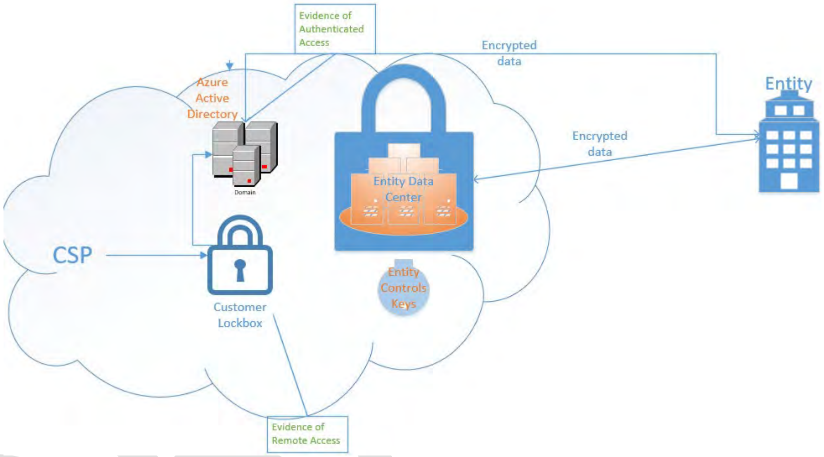
	and are meeting the security objectives, along with the Responsible Entity’s due diligence of such: • Independent audit validating the implementation of the documented security controls and effectiveness of those controls, • Contractual language binding the CSP to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.	

2. **Responsible Entity provides root keys (Customer Key) and manages and stores those keys in Azure vault (~~Cloud Service Provider) and Cloud Service Provider~~ CSP) and CSP access is managed by Customer Lockbox**

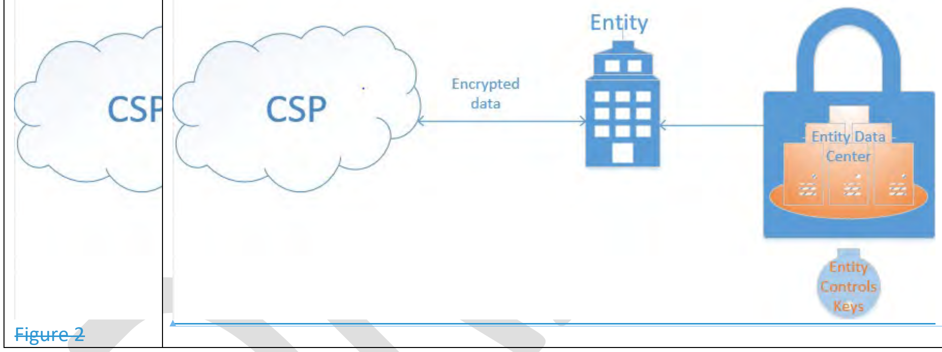
Compliance Impact	Evidence ~~Example~~Examples	Applicable Requirements
~~Cloud Service Provider~~ CSP has access to key store (and therefore could have electronic access to BCSI)	~~All~~Examples of ~~the following would be required~~evidence may include: • Documentation of the security controls implemented within ~~Cloud Service Provider's~~CSP's environment or solution that satisfy the applicable requirements, • ~~Independent audit validating the implementation of the documented security controls and effectiveness of those controls,~~ • ~~Contractual language binding the cloud service provider to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.~~ • List of authorized personnel from Azure Active Directory (CIP-004-6 R4.1.3 and 4.4), • Evidence of implementation of Customer Lockbox to manage support access requests and authorization (CIP-004-6 R4.1.3), • Logs showing each Customer Lockbox access / usage (including start and end date/time for each use) and associated authorization (CIP-004-6 R4.4 and 5.3), • Evidence of the application of encryption at rest and in transit (CIP-011-2 R1.2),	CIP-004-6 R4.1.3 R4.4 R5.3 CIP-011-2 R1.2
CSP ~~Figure 1~~	Additional Supporting Evidence	
	The following are additional evidence examples that could be utilized to demonstrate that security controls have been implemented by the CSP and	

Inserted Cells

Inserted Cells

Compliance Impact	Evidence ~~Example~~Examples	Applicable Requirements
	are meeting the security objectives, along with the Responsible Entity's due diligence of such: • Independent audit validating the implementation of the documented security controls and effectiveness of those controls, • Contractual language binding the CSP to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.	
	 Evidence of Authenticated Access Encrypted data Azure Active Directory Domain Entity Encrypted data Entity Data Center CSP Customer Lockbox Entity Controls Keys Evidence of Remote Access	

3. **Bring Your Own Key (BYOK) and the Responsible Entity stores them onsite or outside ~~of~~ the cloud environment (Responsible Entity privately creates/manages keys and does not use Azure to store keys)**

Compliance Impact	Evidence ~~Example~~Examples	Applicable Requirements
~~Cloud Service Provider~~ CSP personnel do not have access to BCSI	Responsible Entity must demonstrate that BCSI is encrypted and not accessible by ~~Cloud Service Provider~~CSP personnel (CIP-011-2 R1.2). ~~This~~Evidence of this may include any of the following: • Evidence that keys are being managed on~~-premises~~ premise or by a third party, such as report or screenshot from the key management tool. • Agreement or purchase order with ~~Cloud Service Provider~~CSP showing what services have been implemented, including detail of how the services have been implemented • Evidence to show encryption of information determined by the Responsible Entity such as a firewall policy or configuration output report	CIP-011-2 R1.2
 CSP CSP Encrypted data Entity Entity Data Center Entity Controls Keys ~~Figure 2~~		

Inserted Cells

ServiceNow Ticketing System

The following scenarios are intended to reflect what evidence may be used to demonstrate compliance, depending on how the registered entity chose to implement the solution.

1. **~~Cloud Service Provider~~ CSP manages keys and stores keys**

Compliance Impact	Evidence ~~Example~~Examples	Applicable Requirements
~~Cloud Service Provider~~ CSP has access to BCSI	~~All~~Examples of ~~the following would be required~~evidence may include: • Documentation of the security controls implemented within ~~Cloud Service Provider's~~CSP's environment or solution that satisfy the applicable requirements, • ~~Independent audit validating the implementation of the documented security controls and effectiveness of those controls,~~	CIP-004-6 R4.1.3 R4.4 R5.3 CIP-011-2 R1.2

Compliance Impact	Evidence ~~Example~~Examples	Applicable Requirements
	~~• Contractual language binding the cloud service provider to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.~~ • Documented authorization process (CIP-004-6 R4.1.3), • List of ~~Cloud Service Provider~~CSP individuals with access (CIP-004-6 R4.1.3), ~~• Logging and monitoring of BCSI storage location user activity, if possible/available (to confirm accuracy of the list of Cloud Service Provider individuals) (CIP-004-6 R4.1.3 and R4.4)~~ • 15-month access review for ~~Cloud Service Provider~~CSP personnel (CIP-004-6 R4.4), • Revocation within 24 hours of notification for terminations (CIP-004-6 R5.3), and • Evidence of the application of encryption at rest and in transit (CIP-011-2 R1.2)	
	Additional Supporting Evidence	
	The following are additional evidence examples that could be utilized to demonstrate that security controls have been implemented by the CSP and are meeting the security objectives, along with the Responsible Entity's due diligence of such: • Independent audit validating the implementation of the documented security controls and effectiveness of those controls, • Contractual language binding the CSP to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.	

2. Responsible Entity manages key and stores in vault provided by the ~~Cloud Service Provider~~CSP; the ~~Cloud Service Provider~~CSP does not inherently have access to key store nor the Responsible Entity's data

Compliance Impact	Evidence ~~Example~~Examples	Applicable ~~Requirements~~ Requirement
~~Cloud Service Provider~~ CSP could be provisioned access to key store and/or data (both	~~All~~Examples of ~~the following would be required~~evidence may include: • Documentation of the security controls implemented within ~~Cloud Service Provider's~~CSP's environment that satisfy the applicable requirements, ~~• Independent audit validating the implementation of the documented security controls and effectiveness of those controls,~~	CIP-004-6 R4.1.3 R4.4 R5.3 CIP-011-2 R1.2

Compliance Impact	Evidence ~~Example~~Examples	Applicable ~~Requirements~~ Requirement
would be necessary to access BCSI)	- ~~Contractual language binding the cloud service provider to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.~~ - Documented authorization process (CIP-004-6 R4.1.3), - List of ~~Cloud Service Provider~~CSP individuals with access to BCSI, if any (CIP-004-6 R4.1.3), - ~~Logging and monitoring of BCSI storage location user activity, if possible/available (to confirm accuracy of the list of Cloud Service Provider individuals) (CIP-004-6 R4.1.3 and R4.4)~~ - 15-month access review for ~~Cloud Service Provider~~CSP personnel (CIP-004-6 R4.4), - Revocation within 24 hours of notification, for terminations (CIP-004-6 R5.3), and - Evidence of the application of encryption at rest and in transit (CIP-011-2 R1.2)	
	Additional Supporting Evidence	
	The following are additional evidence examples that could be utilized to demonstrate that security controls have been implemented by the CSP and are meeting the security objectives, along with the Responsible Entity's due diligence of such: - Independent audit validating the implementation of the documented security controls and effectiveness of those controls, - Contractual language binding the CSP to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.	

3. **BYOK and Client Storage (the Responsible Entity stores the keys on~~-premises~~ premise or with a ~~3rd~~third party outside ~~of~~ the cloud environment)**

Compliance Impact	Evidence ~~Example~~Examples	Applicable Requirements
~~Cloud Service Provider~~ CSP personnel do not have access to BCSI	Responsible Entity must demonstrate that BCSI is encrypted and not accessible by ~~Cloud Service Provider~~CSP personnel (CIP-011-2 R1.2). ~~This~~Evidence of this may include any of the following: - Evidence that keys are being managed on~~-premises~~ premise or by a third party, such as report or screenshot from the key management tool.	CIP-011-2 R1.2

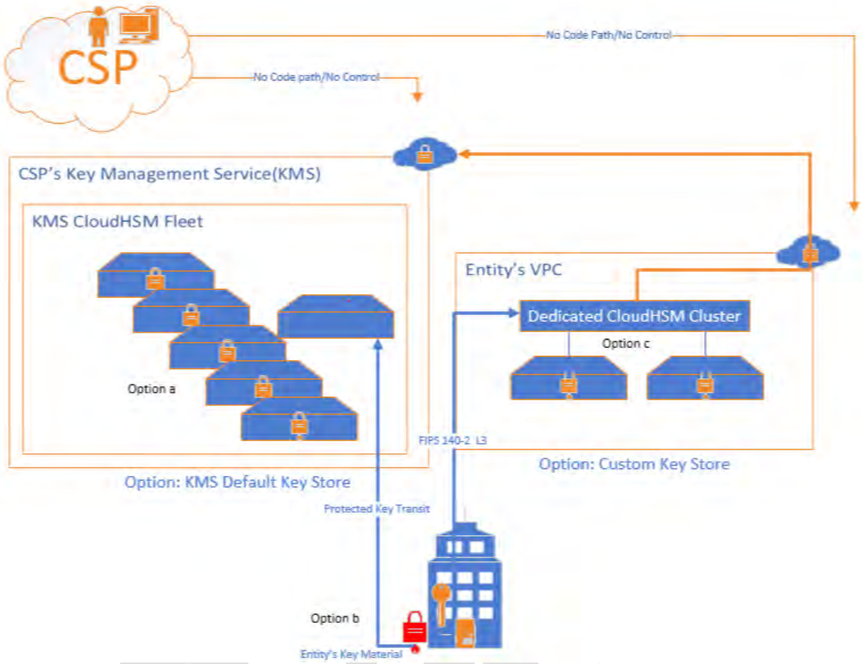
Compliance Impact	Evidence ~~Example~~Examples	Applicable Requirements
	• Agreement or purchase order with ~~Cloud Service Provider~~CSP showing what services have been implemented, including detail of how the services have been implemented • Evidence to show encryption of information determined by the Responsible Entity such as a firewall policy or configuration output report	

Amazon Web Services

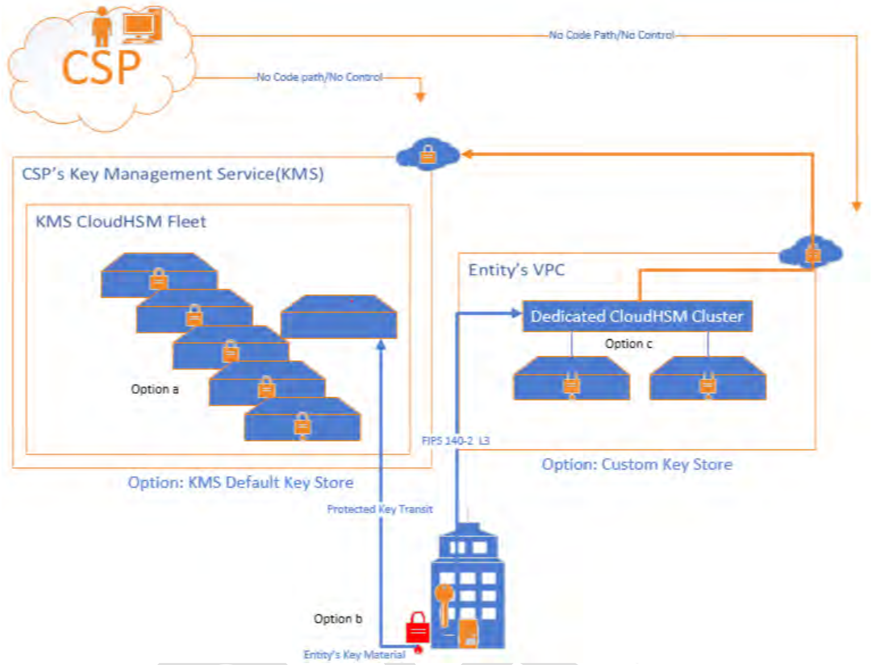
Amazon Web Services (AWS) Key Management System (KMS) is integrated with AWS services to encrypt data at rest and in transit. Customer master keys (CMK) are owned and managed by the Customer (Responsible Entity) within their account. Most AWS services that are integrated with KMS support customer-managed CMKs which allows the customer to manage the keys themselves. Other services may only support AWS-managed CMKs — these CMKs are still unique to the customer's AWS account and provide the same audit visibility to log files. Data protection controls are also provided by other services depending on the functional operations of the actual implementation. The scenarios listed here illustrate three arrangement options for a Responsible Entity to manage keys in AWS KMS and store data that the Responsible Entity determines to contain BCSI in cloud storage service:

- Responsible Entity manages key and stores in AWS KMS (~~Cloud Service Provider~~ CSP) - Multi-tenant Hardware Security Module (HSM)
- Responsible Entity brings own keys and manages key in AWS KMS -- Multi-tenant HSM
- Responsible Entity manages key and stores in AWS KMS (~~Cloud Service Provider~~ CSP), Dedicated HSM

In all three scenarios, AWS personnel do not have an ability to access the keys.


CSP
No Code Path/No Control
No Code path/No Control
CSP's Key Management Service(KMS)
KMS CloudHSM Fleet
Option a
Option: KMS Default Key Store
Entity's VPC
Dedicated CloudHSM Cluster
Option c
FIPS 140-2 L3
Option: Custom Key Store
Protected Key Transit
Option b
Entity's Key Material

~~Figure 3~~



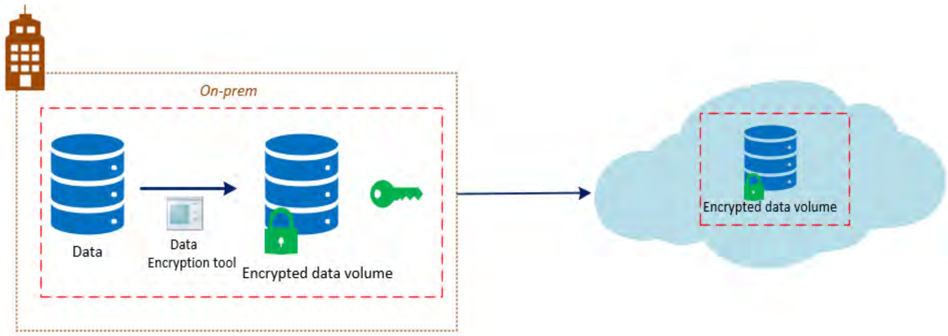
Compliance Impact	Evidence ~~Example~~Examples	Applicable Requirements
~~Cloud Service Provider~~ CSP does not have access to key material or BCSI and no 'code path' access exists As part of Shared Responsibility, the Responsible Entity manages access to the BCSI	Responsible Entity must demonstrate that BCSI is encrypted and not accessible by ~~Cloud Service Provider~~CSP personnel (CIP-011-2 R1.2). ~~This~~Evidence of this may include any of the following: • Evidence that keys are being managed on~~-premises~~ premise or by a third party, such as report or screenshot from the key management tool. • Agreement or purchase order with ~~Cloud Service Provider~~CSP showing what services have been implemented, including detail of how the services have been implemented • Evidence to show encryption of information determined by the Responsible Entity such as a firewall policy or configuration output report	CIP-011-2 R1.2

CommVault Storage/Backup in the cloud

The following scenarios are intended to reflect what evidence may be used to demonstrate compliance, depending on how the registered entity chose to implement the solution.

1. **Encrypted BCSI repository storage (backup) and BYOK – Registered entity encrypts BCSI repositories on-~~premises~~prem using their own keys and stores these repositories in the cloud.**

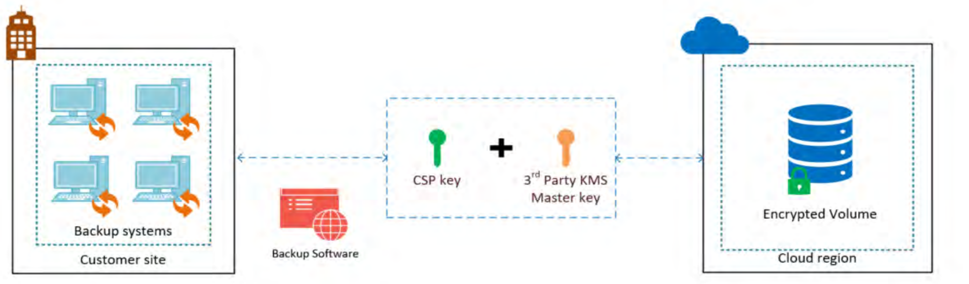
Compliance Impact	Evidence ~~Example~~Examples	Applicable Requirements
~~Cloud Service Provider~~ CSP does not have access to BCSI	Responsible Entity must demonstrate that BCSI is encrypted and not accessible by ~~Cloud Service Provider~~CSP personnel (CIP-011-2 R1.2). ~~This~~Evidence of this may include any of the following: • Evidence that keys are being managed on~~-premises~~ premise or by a third party, such as report or screenshot from the key management tool. • Agreement or purchase order with ~~Cloud Service Provider~~CSP showing what services have been implemented, including detail of how the services have been implemented • Evidence to show encryption of information determined by the Responsible Entity such as a firewall policy or configuration output report	CIP-011-2 R1.2



~~Figure 4~~

2. **Registered entity encrypts BCSI on-~~premises~~prem – Using a master key provided by third party KMS in combination with the key provided by ~~Cloud Service Provider~~CSP to encrypt the BCSI. Once encrypted, BCSI is stored in the ~~Cloud Service Provider~~CSP environment. Therefore, only the Responsible Entity personnel have access to BCSI.**

Compliance Impact	Evidence Example	Applicable Requirements
Neither the ~~Cloud Service Provider~~CSP nor the third party KMS have access to BCSI	Responsible Entity must demonstrate that BCSI is encrypted and not accessible by ~~Cloud Service Provider~~CSP personnel (CIP-011-2 R1.2). ~~This~~Evidence of this may include any of the following: • Evidence that keys are being managed on~~-premises~~ premise or by a third party, such as report or screenshot from the key management tool.	CIP-011-2 R1.2

Compliance Impact	Evidence Example	Applicable Requirements
	• Agreement or purchase order with ~~Cloud Service Provider~~CSP showing what services have been implemented, including detail of how the services have been implemented • Evidence to show encryption of information determined by the Responsible Entity such as a firewall policy or configuration output report • Evidence to show BCSI repository is stored only in encrypted form in the cloud and keys Cannot be used by ~~Cloud Service Provider~~CSP where the repository is stored	
 Backup systems Customer site Backup Software CSP key + 3rd Party KMS Master key Encrypted Volume Cloud region ~~Figure 5~~		

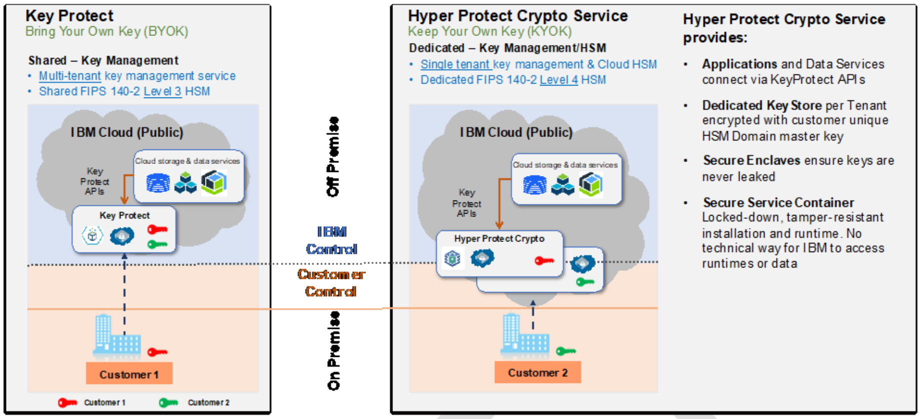
IBM Cloud

IBM Cloud has two options for Key Management Systems:

- IBM Cloud Key Protect – Multi-tenant key management system that enables Bring Your Own Key (BYOK) on a FIPS 140-2 level 3, multi-tenant hardware security module (HSM) device
- Hyper Protect Crypto Services (HPCS) – Single-tenant FIPS 140-2 level 4 HSM key management system that enables registered entities to Keep Your Own Key (KYOK)

Both Key Protect and HPCS are integrated with a number of IBM Cloud Services to enable encryption for data at rest and in transit with BYOK/KYOK.

KYOK further allows for complete isolation and control of stored data. In a KYOK scenario the customer takes ownership of the HSM through a Key Ceremony and becomes the custodian of the HSM that is dedicated to the HPCS instance the customer provisions. Once a customer takes ownership, the CSP has no access to the HSM and therefore no access to the data. Only the registered entity can access/decrypt.


Key Protect
Bring Your Own Key (BYOK)
Shared – Key Management
• Multi-tenant key management service
• Shared FIPS 140-2 Level 3 HSM
IBM Cloud (Public)
Cloud storage & data services
Key Protect APIs
Key Protect
Customer 1
Customer 1
Customer 2
Off Premise
IBM Control
Customer Control
On Premise
Hyper Protect Crypto Service
Keep Your Own Key (KYOK)
Dedicated – Key Management/HSM
• Single tenant key management & Cloud HSM
• Dedicated FIPS 140-2 Level 4 HSM
IBM Cloud (Public)
Cloud storage & data services
Key Protect APIs
Hyper Protect Crypto
Customer 2
Hyper Protect Crypto Service provides:
• Applications and Data Services connect via KeyProtect APIs
• Dedicated Key Store per Tenant encrypted with customer unique HSM Domain master key
• Secure Enclaves ensure keys are never leaked
• Secure Service Container Locked-down, tamper-resistant installation and runtime. No technical way for IBM to access runtimes or data

~~Figure 6~~

The following scenarios are intended to reflect what evidence may be used to demonstrate compliance, depending on how the registered entity chose to implement the solution.

1. **Key Protect/Bring Your Own Key (BYOK) – Registered entity creates and manages keys outside ~~of~~ the cloud environment; keys are stored in the ~~Cloud Service Provider's~~CSP's multi-tenant HSM where some CSP personnel have access.**

Compliance Impact	Evidence Example	Applicable Requirements
~~Cloud Service Provider~~CSP could have access to BCSI (Electronic Only)	~~All~~Examples of ~~the following would be required~~evidence may include: • Documentation of the security controls implemented within ~~Cloud Service Provider's~~CSP's environment that satisfy the applicable requirements, • ~~Independent audit validating the implementation of the documented security controls and effectiveness of those controls,~~ • ~~Contractual language binding the cloud service provider to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.~~ • Evidence that keys are being managed on~~ premises~~ premise or by a third party, such as report or screenshot from the key management tool • Documented authorization process (CIP-004-6 R4.1.3), • List of ~~Cloud Service Provider~~CSP individuals with access (CIP-004-6 R4.1.3),	CIP-004-6 R4.1.3 R4.4 R5.3 CIP-011-2 R1.2

Compliance Impact	Evidence Example	Applicable Requirements
	- ~~Logging and monitoring of BCSI storage location user activity, if possible/available (to confirm accuracy of the list of Cloud Service Provider individuals) (CIP-004-6 R4.1.3 and R4.4)~~ - 15-month access review for ~~Cloud Service Provider~~CSP personnel (CIP-004-6 R4.4), - Revocation within 24 hours of notification for terminations (CIP-004-6 R5.3), - Evidence of the application of encryption (CIP-011-2 R1.2),	
	Additional Supporting Evidence	
	The following are additional evidence examples that could be utilized to demonstrate that security controls have been implemented by the CSP and are meeting the security objectives, along with the Responsible Entity's due diligence of such: - Independent audit validating the implementation of the documented security controls and effectiveness of those controls, - Contractual language binding the CSP to maintain the applicable security controls and notify the Responsible Entity of material changes or failings of those security controls within defined time frames.	

2. **HPCS/Keep Your Own Key (KYOK) - ~~registered~~Registered entity creates and manages keys outside ~~of~~ the cloud environment; keys are stored in the ~~Cloud Service Provider's~~CSP's single tenant HSM; the ~~Cloud Service Provider~~CSP does not have access to the HSM, once the key ceremony has occurred.**

Compliance Impact	Evidence Example	Applicable Requirements
~~Cloud Service Provider~~CSP has no access to BCSI (KYOK Scenario)	Responsible Entity must demonstrate that BCSI is encrypted and not accessible by ~~Cloud Service Provider~~CSP personnel. Examples of evidence may include: - Key Ceremony registry (to demonstrate Master Key creation and sharding) - Logging and alerting of unauthorized access to the HSM - Evidence that keys, including KYOK master, are being managed on~~-premises~~ premise or by a third party, such as report or screenshot from the key management tool. - Agreement or purchase order with ~~Cloud Service Provider~~CSP showing what services have been implemented, including detail of how the services have been implemented	CIP-011-2 R1.2

Compliance Impact	Evidence Example	Applicable Requirements
	• Evidence to show BCSI repository is stored only in encrypted form in the cloud • Evidence to show that data repository is encrypted	

Appendix A: References

Microsoft~~:~~
https://docs.microsoft.com/en-us/microsoft-365/compliance/service-encryption-with-customer-key-faq
https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption
https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security
https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests
https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-service-encryption?view=o365-worldwide

Amazon Web Service
https://aws.amazon.com/compliance/services-in-scope/
https://marketplace.fedramp.gov/#/products?sort=productName
https://aws.amazon.com/blogs/security/are-kms-custom-key-stores-right-for-you/
https://d1.awsstatic.com/whitepapers/aws-support-compliance-nerc-cip-standards.pdf?did=wp_card&trk=wp_card

IBM~~:~~
https://www.ibm.com/cloud
https://www.ibm.com/cloud/hyper-protect-crypto
https://www.ibm.com/cloud/hyper-protect-dbaas
https://www.ibm.com/cloud/hyper-protect-virtual-servers
https://www.ibm.com/cloud/compliance
https://www.ibm.com/security/cryptocards/hsms

FIPS/NIST Encryption Standards~~:~~
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

NERC ~~Critical Infrastructure Protection Committee/Reliability and Security Technical Committee (~~**CIPC/RSTC**~~)~~
Security Guidelines ~~:~~

- Risks related to ~~Cloud Service Providers:~~
CSPs: https://www.nerc.com/comm/CIPC_Security_Guidelines_DL/Security_Guideline-Cloud_Computing.pdf

- ~~Security Guideline for Electricity Sector: Primer for Cloud Solutions and Encrypting BCSI~~

~~Appendix~~Security Guideline for Electricity Sector: Primer for Cloud Solutions and Encrypting BCSI

Appendix B: Recommended Controls

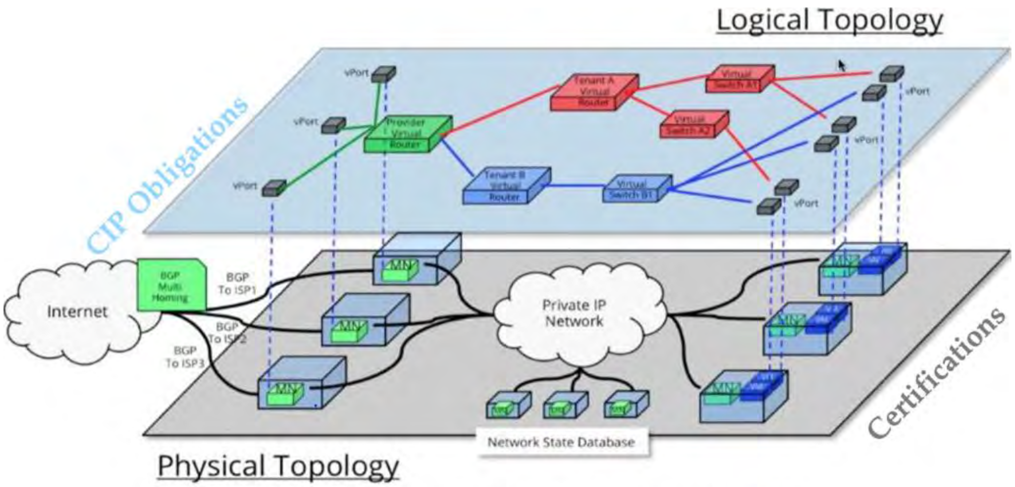
The following is a list of recommended controls that the registered entity should ensure are implemented for their cloud scenario. ~~More~~For more detail about these controls and their associated certifications~~ can be found on~~, visit the ~~Cloud Security Alliance~~Cloud Security Alliance website[4].

- Implements cryptographic mechanisms to protect the confidentiality and integrity of information stored during transport and at rest,
- Prevent unauthorized disclosure of information and detect changes to information,
- Protects the authenticity of communication sessions,
- Employs the principle of least privilege, allowing only authorized accesses for users which are necessary to accomplish assigned tasks,
- Monitors information system accounts for atypical use and reports atypical usage of information system accounts,
- Authorizes access to the information system,
- Employs automated mechanisms to support the management of information system accounts,
- Terminates user and shared/group account credentials when members leave the group,
- Reviews accounts annually,
- Monitors information system accounts for atypical use and reports atypical usage of information system accounts

Underlay and Overlay Model

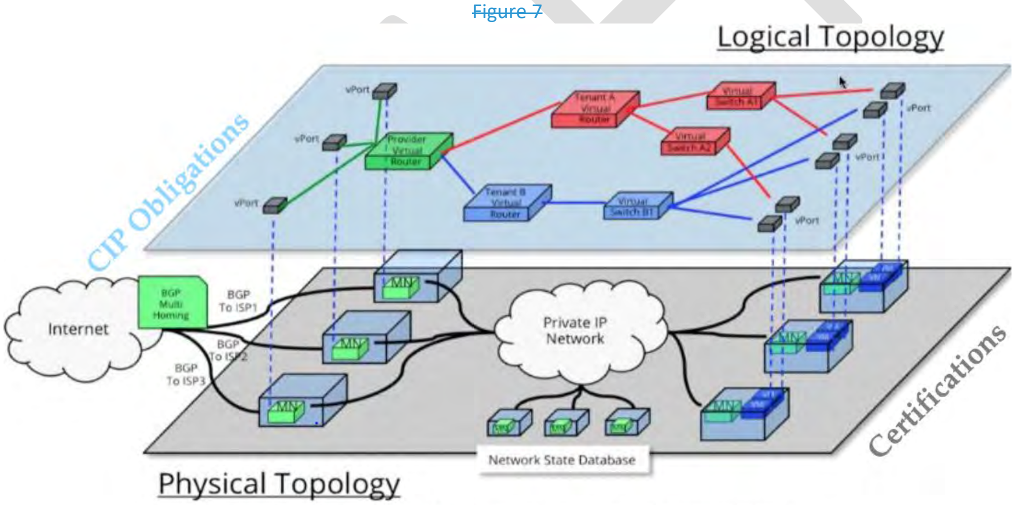
- Underlay (security of the cloud) – Infrastructure (and associated controls) implemented by the ~~Cloud Service Provider~~CSP that runs all services offered by the ~~Cloud Service Provider~~CSP. This infrastructure could be composed of the hardware, software, networking, and facilities that run Cloud services offered. The security and controls associated with this infrastructure is likely verified through certifications or other internal/external activities such as penetration testing. ~~**(Figure 7)**~~(see picture below)
- Overlay (security in the cloud) – The portion of the cloud service/product that sits on top of the underlay and has been developed for the customer's use. In some cloud environments, the ~~Cloud Service Provider~~CSP may have the ability to access data in portions of the Overlay. Whereas in other cloud environments the ~~Cloud Service Provider~~CSP has no ability to access data in the Overlay~~. **(Figure 7)**~~. (see picture below)

[4] https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1-info-sheet/



http://bradhedlund.com/2012/10/06/mind-blowing-l2-l4-network-virtualization-by-midokura-midonet/

~~Figure 7~~



http://bradhedlund.com/2012/10/06/mind-blowing-l2-l4-network-virtualization-by-midokura-midonet/

Agenda Item 10
Reliability and Security
Technical Committee Meeting
June 8, 2021

MOD-032 Technical Reference Document

Action

Approve MOD-032 Technical Reference Document

Approve to disband the PPMVTF

Summary

This technical reference document provides useful information and materials for entities regarding the development of models for interconnection-wide base case creation. The reference document focuses specifically on the provision of data and models by generator owners to the transmission planner and planning coordinator following MOD-032 requirements. The document provides details regarding the types of information provided. This action completes the scope of work for the PPMVTF and the Chair requests RSTC approval.

The Chair request that the RSTC approve to disband the PPMVTF.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Technical Reference Document

Considerations for MOD-032 Data Requirements for Generating Resources

June 2021

RELIABILITY | RESILIENCE | SECURITY

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

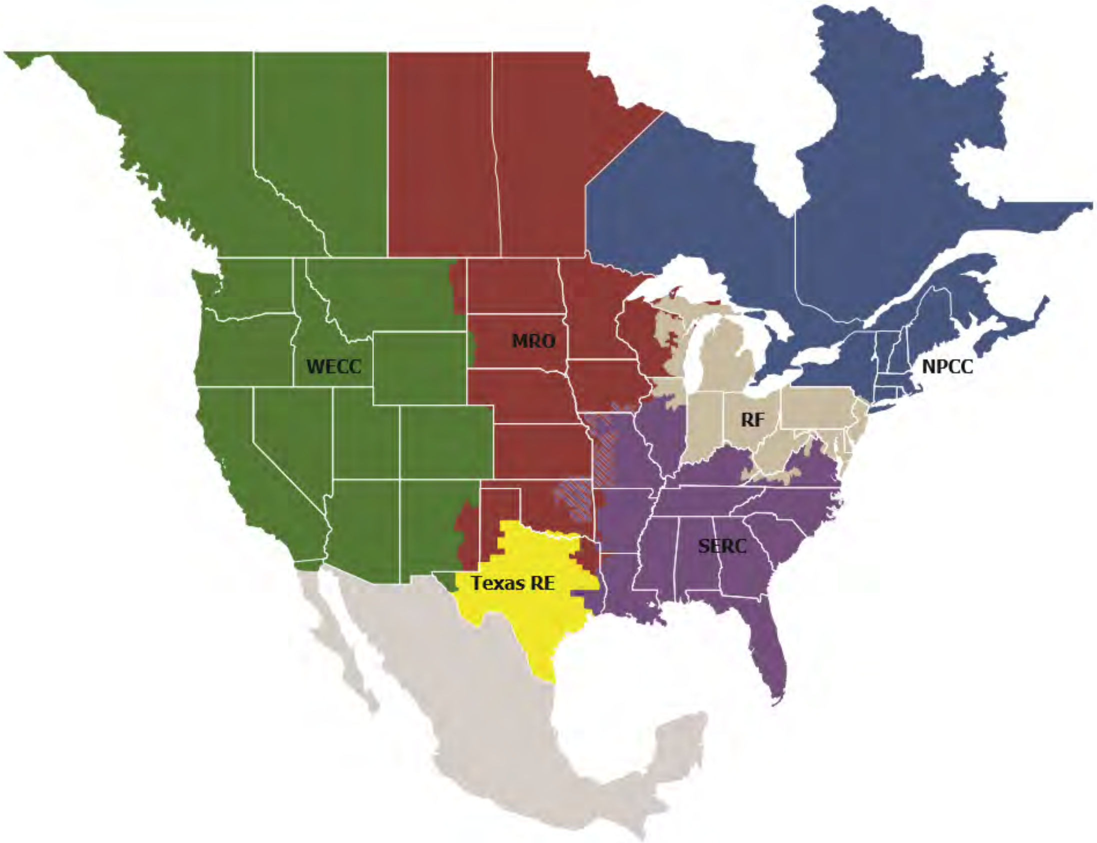
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

NERC Reliability Standard MOD-032: *Data for Power System Modeling and Analysis* establishes "consistent modeling data requirements and reporting procedures for development of planning horizon cases necessary to support analysis of the reliability of the interconnected transmission system."[1] The standard focuses on steady-state, dynamic, and short-circuit modeling practices and data collection, and requires data submission by applicable data owners to their respective Transmission Planners (TPs) and Planning Coordinators (PCs) to support the interconnection-wide case building process in each Interconnection. Those interconnection-wide cases serve as the foundation of system reliability studies. The TP and PC use these interconnection-wide models to represent the external system outside their footprint and will likely make localized or regional updates for specific studies. However, many types of reliability studies depend on an interconnection-wide model since the overall system performance (including the outside system) can have an impact on study results. Therefore, having data available for the purposes of modeling and ensuring that this data is of sufficient accuracy and fidelity is essential to reliability of the BPS.

The North American Generator Forum (NAGF),[2] a forum of Generator Owners (GOs) and Generator Operators (GOPs) in North America focused on addressing "issues related to registration, compliance, standards development, and other NERC-related topics," provided a letter to NERC seeking guidance related to MOD-032. This letter identified four key areas of the standard that they believed warranted additional clarity and guidance, including the following:

- The "level of detail to which equipment shall be modeled" and the use of engineering estimates where modeling information is not reasonably available or obtainable
- Methods for delivering steady-state, dynamics, and short circuit modeling data requirements and reporting procedures as well as data flow between associated parties
- The communications path for modeling data and the timing for compiling and providing this data
- Annual data submission versus submission of data changes only and consideration for defining what "significant" changes may include

This reference document seeks to address these issues identified by the NAGF, focusing solely on MOD-032 data requirements and reporting procedures for GOs:

- **Chapter 1** outlines the MOD-032 requirements.
- **Chapter 2** describes recommended modeling approaches.
- **Chapter 3** describes recommended data exchange methods.
- **Chapter 4** describes some key power plant modeling recommendations.
- **Appendices A–D** provide detailed information that pertains to the type of data expected to be requested for MOD-032 related to steady-state modeling, dynamics modeling, short circuit modeling, and geomagnetic disturbance (GMD) modeling, respectively.
- **Appendix E** provides a detailed description of modeling generator step-up (GSU) transformers, for industry reference.

[1] This document refers to MOD-032 without a version number unless relevant to specific requirements. Consult the latest version of the MOD-032 standard.

[2] http://www.generatorforum.org/.

Introduction

The NAGF requested for NERC to develop guidance related to MOD-032. In particular, the NAGF requested the following:

- Provide guidance for the "level of detail to which equipment shall be modeled" as outlined in MOD-032-1 R1.2.2, particularly for conditions where the equipment owners may not have sufficient detail regarding certain model parameter values.
- Describe recommended methods for delivering steady-state, dynamics, and short circuit modeling data requirements and reporting procedures from the PCs and TPs, and recommend that sufficient time is allowed for data and information to flow between entities.
- Provide recommended practices for the communication path regarding the model building process, data submittal, etc. for equipment owners.
- Describe the recommended process for equipment owners to provide model updates to the PC and TP and the interplay between MOD-032 and other MOD standards, such as MOD-026-1 and MOD-027-1. Provide clarity as to what constitutes "changes" in modeling data, with examples of what these changes could entail. Describe how equipment tolerance and parameter accuracies are related to "changes" in data.

The goal of this reference document is to promote consistency and uniformity in data requirements and reporting procedures to the greatest possible extent between PCs, TPs, and GOs. The topics in the list above as well as other relevant aspects of MOD-032 are covered in this document.

Overall Process for MOD-032 Data Requests
NERC Reliability Standard MOD-032 focuses on the collection of data for the "development of planning horizon cases necessary to support analysis of the reliability of the interconnected transmission system." In particular, each PC makes the models available for its planning area, reflecting the data provided under Requirements R2 of MOD-032-1 to the ERO[3] or its designee ("MOD-032 Designee") to support the creation of interconnection-wide planning cases. These cases are used by all PCs and TPs to represent their system[4] and external systems across the Interconnection.

Currently, the MOD-032 designees in each Interconnection are the following entities or organizations:

- **Eastern Interconnection:** Eastern Interconnection Reliability Assessment Group (ERAG)
- **Texas Interconnection:** Texas Reliability Entity (Texas RE)
- **Western Interconnection:** WECC

Pursuant to Requirement R4 of MOD-032-1, NERC has designated the above entities as the interconnection-wide base case creators with the goal of supporting the creation of these cases that include all relevant PCs in their collective footprints. NERC and the MOD-032 designees have signed agreements to develop these cases to NERC's satisfaction, including key functions and attributes included in the agreements. The MOD-032 designees meet these requirements by working with their respective PCs to gather the modeling data necessary to create these cases.

Each PC and each of its respective TPs must, per Requirement R1 of MOD-032-1, develop steady-state, dynamic, and short circuit modeling data requirements and reporting procedures for its planning area to effectively

[3] NERC is the designated ERO for North America.

[4] PCs and TPs often replace their portion of the system for local studies to ensure that the most detailed models and data are used (e.g., proprietary models, detailed models for specific studies).

gather the data necessary to develop these cases for the planning horizon. Recommended data requirements and reporting procedures are described in this reference document.

Requirement R2 of MOD-032-1 specifies that each of the respective equipment owners or model data owners are required to provide the necessary data to the TPs and PC, according the data requirements and reporting procedures specified in Requirement R1. This document also describes the data submittal and data collection processes regarding base case development.

NERC, its MOD-032 designees, the TPs and PCs, and the equipment owners all play a critical role in the development of interconnection-wide base cases used for reliability studies in the planning (and operations) horizon. **Figure I.1** shows the feedback loops between these entities to support improvements in the development of these cases and the quality of the data supplied. Relevant modeling improvement efforts can be found in a number of NERC documents, including the following:[5,6]

- NERC List of Acceptable Models
- NERC MOD-32 Designee Tracking Document
- NERC Modeling Improvements Initiative Update Technical Report
- NERC Case Quality Metrics Assessments

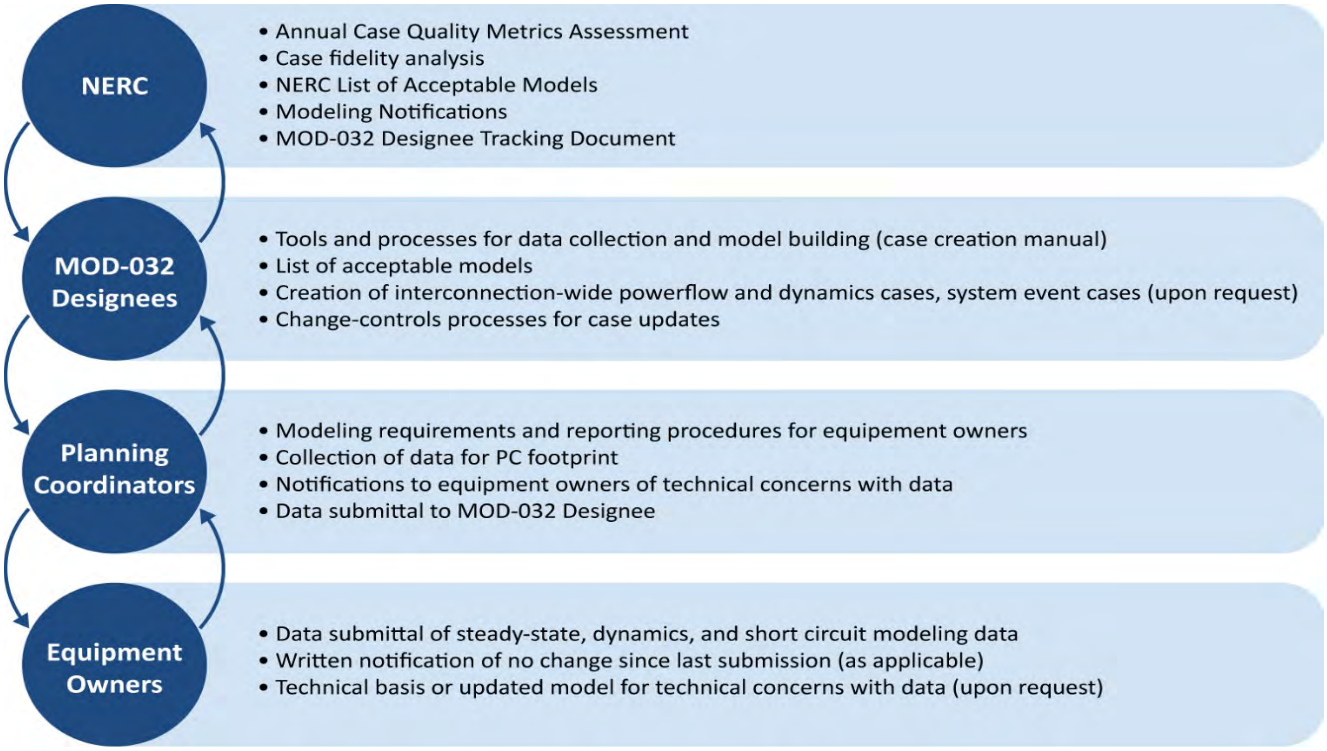

NERC
• Annual Case Quality Metrics Assessment
• Case fidelity analysis
• NERC List of Acceptable Models
• Modeling Notifications
• MOD-032 Designee Tracking Document
MOD-032 Designees
• Tools and processes for data collection and model building (case creation manual)
• List of acceptable models
• Creation of interconnection-wide powerflow and dynamics cases, system event cases (upon request)
• Change-controls processes for case updates
Planning Coordinators
• Modeling requirements and reporting procedures for equipement owners
• Collection of data for PC footprint
• Notifications to equipment owners of technical concerns with data
• Data submittal to MOD-032 Designee
Equipment Owners
• Data submittal of steady-state, dynamics, and short circuit modeling data
• Written notification of no change since last submission (as applicable)
• Technical basis or updated model for technical concerns with data (upon request)

Figure I.1: Overall MOD-032 Data Request Process

[5] https://www.nerc.com/pa/RAPA/ModelAssessment/Pages/default.aspx

[6] https://www.nerc.com/comm/PC/Pages/System-Analysis-and-Modeling-Subcommittee-(SAMS)-2013.aspx

Chapter 1: MOD-032-1 Requirements

The purpose of MOD-032 is to "establish consistent modeling data requirements and reporting procedures for development of planning horizon cases necessary to support analysis of the reliability of the interconnected transmission system." This chapter provides a brief description of the requirements in MOD-032-1. Refer to the latest version of the MOD-032 standard for exact language.

Requirement R1

Requirement R1 states the following:

R1. Each Planning Coordinator and each of its Transmission Planners shall jointly develop steady-state, dynamics, and short circuit modeling data requirements and reporting procedures for the Planning Coordinator's planning area that include:

1.1. The data listed in Attachment 1.

1.2. Specifications of the following items consistent with the procedures for building the Interconnection-wide case(s):

1.2.1. Data format

1.2.2. Level of detail to which equipment shall be modeled

1.2.3. Case types or scenarios to be modeled

1.2.4. A schedule for submission of data at least once every 13 calendar months

1.3. Specifications for distribution or posting of the data requirements and reporting procedures so that they are available to those entities responsible for providing the data.

Requirement R1 indicates that the PC and each of its TPs must jointly develop modeling data requirements and reporting procedures for each PC area. It lays out the elements that must be addressed in each set of requirements and procedures. These sub-topics are described in detail in **Chapter 2**.

Requirement R2

Requirement R2 states the following:

R2. Each Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, and Transmission Service Provider shall provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) according to the data requirements and reporting procedures developed by its Planning Coordinator and Transmission Planner in Requirement R1. For data that has not changed since the last submission, a written confirmation that the data has not changed is sufficient.

Requirement R2 ensures that the respective equipment or data owners within the PC footprint provide their data according to the requirements and reporting procedures set forth by the PC and TP in Requirement R1. It also allows for a written confirmation to the TP and PC if data has not changed since the last submission. This mitigates unnecessary data sharing over time. **Chapter 3** covers this in more detail.

Requirement R3

Requirement R3 states the following:

> R3. Upon receipt of written notification from its Planning Coordinator or Transmission Planner regarding technical concerns with the data submitted under Requirement R2, including the technical basis or reason for the technical concerns, each notified Balancing Authority, Generator Owner, Load Serving Entity, Resource Planner, Transmission Owner, or Transmission Service Provider shall respond to the notifying Planning Coordinator or Transmission Planner as follows:
>
> 3.1. Provide either updated data or an explanation with a technical basis for maintaining the current data;
>
> 3.2. Provide the response within 90 calendar days of receipt unless a longer time period is agreed upon by the notifying Planning Coordinator or Transmission Planner.

Requirement R3 provides some oversight for the data submitted to ensure that the model data and information is of sufficient quality and fidelity. In some cases, data may be submitted that includes unintended errors or inaccuracies. These could range from data entry errors, poor verification testing results, or inaccurate estimation techniques. Regardless, these errors should be corrected in a timely manner. The PC or TP can provide a written notification to the GO that there are technical concerns with the model. These technical concerns may include, but are not limited to, the following:

- **Initialization:** The model does not initialize properly when entered into the interconnection-wide (or larger model) base case. Modeling data errors are created that prohibit proper usage or software tools report initialization errors or warnings.
- **No-Disturbance Flat Run:** When a dynamic disturbance is run with no disturbance, the simulation should produce no significant transients. Models that cause any transients upon a flat run may have suspect data that needs to be inspected more closely.
- **Unstable Performance:** For an otherwise stable simulation, the model should exhibit positive damping. Any models that are contributory to unstable performance may have a modeling error. This is often assumed when an otherwise stable system begins to exhibit unstable conditions.[7]
- **Physically Impossible Parameters:** Some parameter values directly relate to physical characteristics of electrical machines or control components. These parameter values must meet certain criteria to be physically possible or reasonable for a model to function properly. A number of these types of model checks are included in the annual *NERC Case Quality Metrics Assessment*[8] and have been included in the MOD-032 Designee case building processes.
- **Suspect Model Parameters:** Parameter values should typically fall within certain ranges for specific types of equipment and controls. The TP or PC should carefully evaluate values outside these ranges of reasonability, and the GO should verify the values as well. For example, machine saturation values outside of reasonable ranges may be questionable or suspect data. Similarly, bypassed control loops, abnormal gains or time constants, and default parameter values are all considered suspect data by the PC and TP in most cases.
- **Poor Model Fidelity:** If disturbance-based model verification[9] proves that the modeled response does not match the actual response of the machine for multiple instances, this gives ground for technical concerns with the model data provided.

[7] This is often based on engineering expertise and experience working with particular systems.

[8] NERC Case Quality Metrics Assessments: https://www.nerc.com/pa/RAPA/ModelAssessment/Pages/default.aspx

[9] The NERC reliability guideline on power plant dynamic model verification using PMUs can be found here: http://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability%20Guideline%20-%20Power%20Plant%20Model%20Verification%20using%20PMUs%20-%20Resp.pdf.

Requirement R4

Requirement R4 states the following:

> R4. Each Planning Coordinator shall make available models for its planning area reflecting data provided to it under Requirement R2 to the Electric Reliability Organization (ERO) or its designee to support creation of the Interconnection-wide case(s) that includes the Planning Coordinator's planning area. *[Violation Risk Factor: Lower] [Time Horizon: Long-Term Planning]*

The overall goal of the MOD-032 standard is to ensure that modeling data is obtained to support the development of interconnection-wide models used in the long-term planning horizon. These models are provided by the PC to the ERO or its designee (referred to as the "MOD-032 Designee"[10]). Each MOD-032 Designee has signed an agreement with NERC (as the ERO) to meet specific functions and attributes in the interconnection-wide case building process. NERC continues to work closely with the MOD-032 Designees to improve these case building processes as well as improve the overall quality and fidelity of the cases created.

Data Requests Associated with TPL-007-1

MOD-032 can and does relate to other modeling and simulation efforts that the PC and TP may need to perform. These may include more localized transient stability studies, electromagnetic transient simulations, GMD analysis, and other detailed simulations. Specifically, data to perform the GMD studies for TPL-007-1 should be requested from the equipment owners as part of the MOD-032 data requests by the PCs and TPs. Rather than add an additional data collection requirement in TPL-007-1, the TPL-007-1 standard drafting team recommended that this data should be provided and addressed under the data collection process of MOD-032. The Consideration of Comments for Project 2013-03, posted August 27, 2015, stated the following:[11]

> "Data requirements. Commenters stated that the standard needed a requirement for entities to provide data to the PC and TP for development of the required models, including specific time requirements such as 'within 90 days'. Some commenters recommended assigning responsibility for maintaining system models to the ERO or its designee. The SDT believes that requirements for providing modeling data to PCs and TPs are addressed in MOD-032-1 and that an additional requirement in TPL-007 would be redundant. MOD-032 establishes consistent modeling data requirements and reporting procedures for the planning horizon and includes PC, TP, GO, and TO among the applicable entities. MOD-032 also addresses requirements for establishing reporting timelines and for making models available to the ERO or its designee."

[10] The MOD-032 Designees are WECC in the Western Interconnection, Texas RE in the Texas Interconnection, and the Eastern Interconnection Reliability Assessment Group (ERAG) in the Eastern Interconnection. These are all individual or groups of NERC Regional Entities.

[11] See the Consideration of Comments for Project 2013-03 Geomagnetic Disturbance Mitigation, Posted 27 August 2015, Docket No. RM15-11-0. Available: http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/TPL-007-1%20Petition.pdf http://www.nerc.com/FilingsOrders/us/Pages/NERCFilings2015.aspx?Paged=TRUE&p_Order_x0020_Date=20150121%2005%3a00%3a00&p_ID=834&PageFirstRow=91&&View={78AA3CFA-96AC-4499-B535-BDB681B4B0B8}

Chapter 2: Recommended Modeling Data for MOD-032

MOD-032 requires each PC and each of its respective TPs to develop modeling data requirements jointly. These requirements must cover steady-state (powerflow), dynamics and short circuit models (and modeling data) that will be submitted by the equipment owners. Attachment 1 of MOD-032 describes the data that is required to model the interconnected BPS effectively, and each PC may specify more detailed requirements to ensure the necessary data is collected to perform reliability studies. Each column of the table also includes a specification for "other information requested by the [PC] or [TP] necessary for modeling purposes." The intent of this requirement is to allow PCs and TPs to request sufficient data for modeling and system studies rather than to allow unnecessary data reporting requirements from data or equipment owners (DEOs). This may include additional data not captured in the table in Attachment 1 required for modeling and system analysis purposes.

It is not reasonable for the MOD-032 standard to prescribe every data parameter required. The amount of data necessary is dependent on the types of studies to be performed, the types of system phenomena to be studied, and the simulation tools being used. The standard affords a reasonable level of flexibility to the TP and PC to request data for modeling purposes necessary to ensure BPS reliability.

Appendix A–E describe the level of detail related to the models and model parameters PCs or TPs may request from DEOs. **Chapter 4** offers details for how a synchronous generator may be modeled. This document is not intended to be exhaustive, and the TP or PC may request additional information so that a detailed study model can be created in some situations.

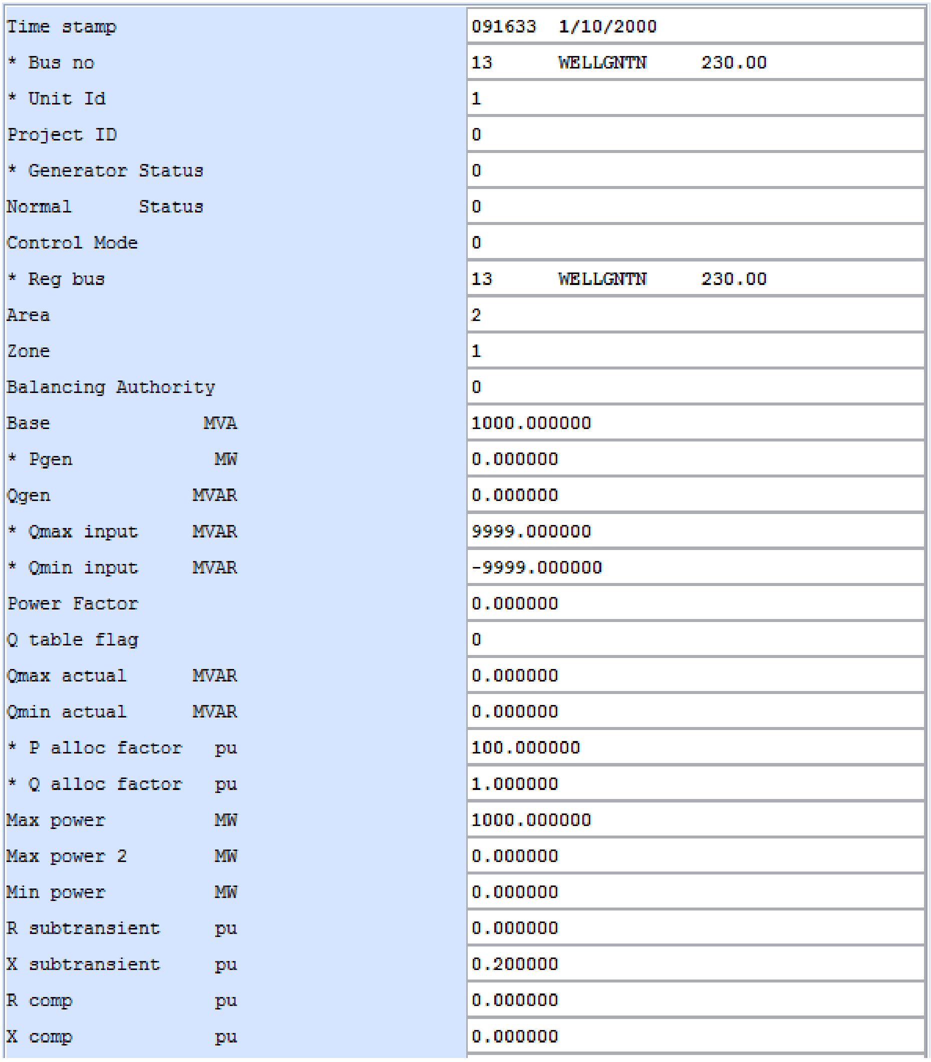
Specified Data Formats

MOD-032 requires each PC and TP to specify the format that equipment owners must submit their model information. PCs and TPs use different model building tools, simulation platforms, data archives, and internal case creation processes. Therefore, it is unreasonable for all PCs or TPs to use a standardized data format. Rather, each PC and TP should attempt to use a format that is comprehensive enough to support the creation of interconnection-wide cases but is also easy to use for data entry and submittal. Data requests should be in a format that relates to how and what data is typically retained by the DEO. For example, data for each modeled condition (e.g., summer peak, spring light load) should be requested such that the DEO understands the assumptions and operating conditions requested (e.g., ambient temperature, pressure). The TP or PC may request data converted by the DEO, data and graphics necessary to convert the requested data to modeled conditions (e.g., ambient temperature-power curves), or both. It is most important that data requests are clear and complete so as not to require multiple requests. While it should not be necessary, the DEO should request clarification from the TP or PC if data requirements are not clear.

Requests for powerflow or dynamics data with a required data format as dictated by a software platform (e.g., *.raw, *.sav, *.dyr, *.dyd) should include a data template. If applicable (typically for dynamics models) and possible, the TP or PC should supply the DEO with the associated data entry template and block diagram. The TP and PC should understand that many DEOs are not users of the applicable power system modeling software and are therefore unfamiliar with the data formats and requirements. It is the responsibility of the TP and PC to fully understand the data requirements and provide data requests to DEOs in a format that respects the needs and limitations of the DEOs.

Recommended Level of Detail

MOD-032-1 Requirement R1.2.2 requires that the "level of detail to which equipment shall be modeled" must be specified as part of the data requirements and reporting procedures. This is generally understood to mean that each component may require a model that includes multiple model parameters. The PC and TP should clearly articulate in their data requirements which model parameters need to be completed. For example, when a generating resource is to be modeled in a steady-state powerflow program, there are multiple parameters that are modeled. **Figure 2.1** shows an example of the data fields that may need to be completed for that component model. The data required from the GO should be clearly specified in the MOD-032 data requirement document maintained by the PC and TP.



Time stamp	091633 1/10/2000
* Bus no	13 WELLGNTN 230.00
* Unit Id	1
Project ID	0
* Generator Status	0
Normal Status	0
Control Mode	0
* Reg bus	13 WELLGNTN 230.00
Area	2
Zone	1
Balancing Authority	0
Base MVA	1000.000000
* Pgen MW	0.000000
Qgen MVAR	0.000000
* Qmax input MVAR	9999.000000
* Qmin input MVAR	-9999.000000
Power Factor	0.000000
Q table flag	0
Qmax actual MVAR	0.000000
Qmin actual MVAR	0.000000
* P alloc factor pu	100.000000
* Q alloc factor pu	1.000000
Max power MW	1000.000000
Max power 2 MW	0.000000
Min power MW	0.000000
R subtransient pu	0.000000
X subtransient pu	0.200000
R comp pu	0.000000
X comp pu	0.000000

Figure 2.1: Example Steady-State Generator Model Parameters

In addition to specifying the parameter values that should be required by the DEOs, the "level of detail" should also include recommendations or specifications for the accuracy of the data requested. The following are recommendations regarding the accuracy level:

- Data should be of the highest quality and accuracy available to the GO.
- Data should have a documented source (e.g., original equipment manufacturer (OEM)-supplied specification sheet, factory test report, nameplate rating, commissioning test report, verification test report, measured, estimated) to support coordination between the DEO and the OEM as well as between the DEO and the TP and PC.
- Data from the OEM is the best source of information for many model parameter values. If this type of information is available (e.g., equipment specification sheets, factory test reports), it should be considered the most trusted data source in general.
- If parameter values have been verified by test (e.g., MOD-026-1 and MOD-027-1), these values should be trusted with a relatively high level of confidence.

- For older equipment or where information is not available for specific model parameters, the DEO should make every attempt to obtain this information (e.g., contact the OEM, seek guidance on accurate/reasonable estimation techniques).
- If data is unavailable and cannot be tested or verified, then some form of estimation should be used. The DEO should consult with the PC and TP to agree upon a suitable estimation technique to be used for that specific model parameter value.

List of Acceptable Models

The NERC Modeling Working Group (MWG) developed the *NERC Libraries of Standardized Powerflow Parameters and Standardized Dynamics Models*[12] in October 2015. The NERC MWG was disbanded in 2016 and its efforts were consolidated into the NERC System Analysis and Modeling Subcommittee (SAMS) activities until the dissolution of SAMS in September 2020. NERC Staff now develops and maintains the *NERC List of Acceptable Models for Interconnection-wide Modeling*,[13] which is a simplified and more explicit version of the original model list. This list is expected to be implemented by the MOD-032 Designees per the Designee Agreement, Attachment A. The attribute states the following:

> “Designees shall direct the Planning Coordinators to use NERC standardized interconnection-wide dynamics models for equipment when made available through the NERC Standardized Powerflow Parameters and the NERC Standardized Dynamics Model List. Temporary “unapproved” models may be allowed if an approved model is not yet available or is under development. Each [PC] may be more restrictive if they desire.”

PCs and TPs then must submit models to the MOD-032 Designee that meet the list of acceptable models. To do this, the TPs (and PCs) are therefore required to also have a list of acceptable models or to reference the NERC (or MOD-032 Designee) list. In addition, Requirement R1 of MOD-026-1 and MOD-027-1 states that each TP is required to provide information to the GO within 90 calendar days, which includes “instructions on how to obtain the list of…models that are acceptable to the [TP] for use in dynamic simulations.” GOs are recommended to reach out to their TPs to identify where their list of acceptable models resides and ensure that the models being submitted meet the requirements of the TP.

Following this process (see **Figure 2.2**), GOs are required to provide models that meet these lists of acceptable models, and it is the responsibility of the TP and PC to provide a list to the GO.

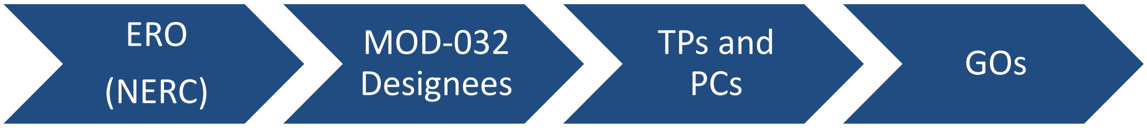


Figure 2.2: Flow of List of Acceptable Models to GOs

[12] NERC Libraries of Standardized Powerflow Parameters and Standardized Dynamics Models: http://www.nerc.com/comm/PC/Model%20Validation%20Working%20Group%20MVWG%202013/NERC%20Standardized%20Component%20Model%20Manual.pdf

[13] https://www.nerc.com/pa/RAPA/ModelAssessment/Pages/default.aspx

Chapter 3: Recommended Data Exchange

MOD-032 requires information and model data to flow between the PC, TP, and DEOs. This section describes recommended practices and considerations for this information exchange.

Recommended Reporting Procedures Notification

Requirement R1.3 of MOD-032-1 requires the PC and each of its TPs to specify the "distribution or posting of the data requirements and reporting procedures so that they are available to those entities responsible for providing the data." There are multiple mechanisms that the PC and TP can use to distribute or post this information. Some recommended practices related to this notification are provided in this section.

The recommended option for sharing data requirements and reporting procedures is for the PC to post the materials at a central location available for all entities to easily access (see **Figure 3.1**). Each PC is encouraged to have a MOD-032 webpage that each DEO can easily access. This webpage should specify all the information needed to meet the requirements of MOD-032. Having the information publicly posted ensures that the information is available to all DEOs and allows a central location with the required data, format, and specified time lines. DEOs are typically familiar with their corresponding TP or PC and are more likely to have access to the TP or PC website for more information.

Centrally posted information also mitigates potential miscommunication issues where information cannot be provided for some reason.[14] Lastly, it focuses efforts on the results and quality of the data submitted rather than focusing on the process and compliance obligations such as archiving email correspondence.

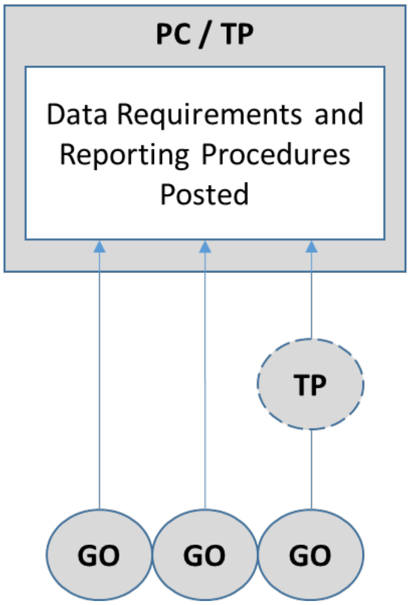


Figure 3.1: Recommended Notification Process

The following information should be included on a website posting for MOD-032 at a minimum:

- Data requirements that include the information described in **Chapter 2**
- Reporting procedures that describe the expected time line for annual data submittal
- Reporting procedures that describe the process and expected time line for providing updates to model information
- Contact information for the PC or TP that does not changes based on internal staffing (example: *mod032planning@pc.com*)

Each PC should notify its stakeholders that this webpage has been established and provide notification if there are any changes in the webpage or to the scheduled data submittal process. Any changes to the posted materials (data requirements or reporting procedures) should be followed by an email notification to those entities so they are aware of the changes. These notifications help ensure that the necessary information is made available to the best possible extent to the equipment owners without hindering the equipment owners from complying with the requirements of MOD-032.

[14] This could include changes in job responsibilities at either the PC/TP or the equipment owner (e.g., TO, GO), personnel retirements, lost email correspondence, etc.

Along with the annual case creation process established and performed by the MOD-032 designee in coordination with the TPs and PCs, the TP or PC may identify technical concerns regarding model quality or fidelity (refer to **Chapter 1** for more details on Requirement R3 of MOD-032-1). This initiates a model review by the DEO and a response to either correct the model or justify its use. The TP and PC should have tools available to perform a technical review of the models received. These tools may range from data quality checks to flag physically impossible data to more advanced disturbance-based model verification.[15] The TP or PC can often work collaboratively with the DEO to understand potential modeling errors, and may have insight as to how to correct those errors. Technical concerns may be expressed to the DEO at any time, and the TP and PC are encourage to express those concerns as soon as they are identified (not only during the annual case creation and data submittal processes). **Figure 3.2** provides an illustrative example of the two different processes.

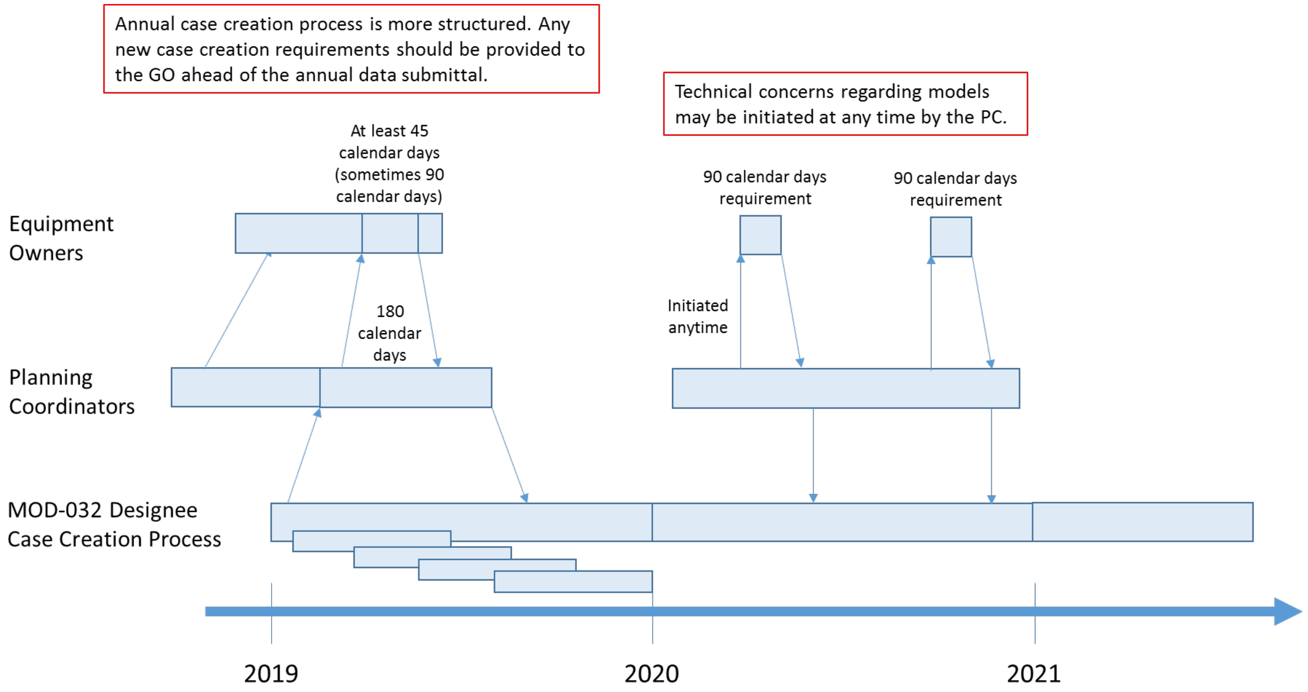

Annual case creation process is more structured. Any new case creation requirements should be provided to the GO ahead of the annual data submittal.
Technical concerns regarding models may be initiated at any time by the PC.
At least 45 calendar days (sometimes 90 calendar days)
90 calendar days requirement
90 calendar days requirement
Equipment Owners
180 calendar days
Initiated anytime
Planning Coordinators
MOD-032 Designee Case Creation Process
2019
2020
2021

Figure 3.2: Relationship between Annual Case Creation Process and Technical Concerns

Model Verification Updates from MOD-026 and MOD-027

The processes outlined in MOD-032 are intended to support the annual (or more frequent) creation of interconnection-wide base cases used for planning the BPS. It is critical that the most up-to-date and accurate data is supplied for these processes and that the TP and PC have clear data requirements and reporting procedures in place to gather that data. The equipment owners (e.g., GOs) then must supply the data following those requirements and procedures such that the TPs and PCs can assemble the planning models for their area. Case creation is a nearly continuous process since many different cases are generated annually to support planning assessments for TPL-001-4, generator interconnection studies, and other related studies.

Concurrently, applicable GOs are required to verify the dynamic models provided to the TP and PC as part of the requirements in MOD-026 and MOD-027. Model verification efforts typically occur much less frequently (on a 10-year window unless changes are made to the facility that could impact the dynamic model). However, those models need to be implemented into the annual case creation process at the most effective and expeditious opportunity.

[15] Refer to the NERC Reliability Guideline: Power Plant Dynamic Model Verification using PMUs. Available: https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability%20Guideline%20-%20Power%20Plant%20Model%20Verification%20using%20PMUs%20-%20Resp.pdf.

The MOD-026 and MOD-027 standards only require the GO to provide the data to the TP once verification is complete. On the other hand, MOD-032 requires data to be submitted according to the reporting procedures outlined jointly by the PC and TP. Therefore, the data reporting requirements developed jointly by the TP and PC should explicitly describe what is expected of the GO in terms of submitting updated or verified models. If this direction is not provided in the reporting requirements, then the GO should consult with the TP and PC to identify what is expected for data submission. In either case, the TP and PC should have a method for tracking the updated models and incorporating them in the next iteration of case creation (or update them in the models under development).

TPs and PCs should request information as to whether the unit(s) have been verified for MOD-026 or MOD-027 (e.g., setting a flag, confirmation of testing date). This may be done either as part of a model submitted or may be tracked externally. This action helps tracking verification activities for the TP, PC, and MOD-032 designee for creation of interconnection-wide cases.

Modeling New Units

The MOD-032 Designees all have preferred or required modeling practices for representing newly interconnecting units into the interconnection-wide base cases. The TPs or PCs may have different practices for localized studies, otherwise they will abide by the practices for interconnection-wide case creation. These recommended practices are not typically prescriptive in nature[16] and may follow any or all of the general guidelines for planned facilities, including the following:

- The facilities are expected be in-service on the scheduled base case posting date
- The facilities are expected to be in-service in the month and year represented in the case
- The facilities are required to support proposed generation facilities that are modeled in-service in the case.
- The facilities have provided all necessary documentation (e.g., environmental permits, financially binding agreements with the TSP, construction agreements)
- The facilities have a signed interconnection service agreements (short-term cases)
- Firm transactions from neighboring BA areas are insufficient to serve native load, and therefore non-firm transactions are needed (longer-term cases)

The data supplied for these planned facilities should be the most accurate data available at the time. Dynamic models verified by equipment testing should be provided if available.[17] If this data is not available, design data should be provided. If design data is not available, generic dynamic data or estimated parameters may be acceptable. In-service equipment should be supported by test data while longer-term planning horizon cases may only have generic data available.

[16] This is due to the fact that there are often widely differing practices among TPs and PCs regarding when a facility starts being modeled in the interconnection-wide cases (and regional and local transmission planning cases).

[17] For new applicable units, documentation and data must be provided to the TP within 365 days after the commissioning date per Attachment 1 in MOD-026-1 and MOD-027-1.

Chapter 4: Power Plant Modeling

Accurate steady state and dynamic power plant modeling in power system simulation tools is critical to BPS reliability. Consistency in power plant modeling, and the data supplied to represent these resources, supports various types of simulations performed: powerflow simulations, contingency analysis, short circuit studies, and dynamic simulations. Accurate representation of all elements of the BPS, including power plant components, ensures that the correct investment decisions are made by TPs and PCs and that the grid is effectively operated within SOLs and IROLs.

This section describes several modeling topics that have been discussed at length in the NERC Power Plant Modeling and Verification Task Force (PPMVTF), and are captured here for industry reference.

Modeling Synchronous Generator Capability

On the surface, modeling the active and reactive power limits of a generating resource seems straightforward. However, these limits are some of the most difficult parameters to accurately represent with existing software tools and modeling practices. The overall capability of a machine is dependent on many factors, including ambient temperature conditions, active power output, and terminal and plant voltages. Unless the assumptions and expectations for modeling are made clear, the parameter values received may not accurately model the resource as anticipated.

Terminology is critical with capability curve modeling. The following terms are used:

- **Machine capability curve:** This is the physical capability of the generating resource itself; typically a D-curve or nameplate rating with varying capabilities of active and reactive power for a nominal voltage (1.0 pu).
- **Limits:** This most commonly refers to the machine over- and under-excitation limiters (UELs) but can also include other restrictions on generating resource output such as plant voltage limits, stability limits, or any other type of limit that restricts or controls machine output limits.
- **Composite capability curve:** This term is used to describe the overall capability of the resource while taking into consideration the machine capability curve[18] as well as any limits that may restrict output. See **Figures 4.1–4.4** for examples of such curves. The term “capability curve” is often used to refer to the “composite capability curve” rather than the actual machine capability curve.

Machine capability is defined by the machine manufacturer and is the basis for setting limiter values. The machine capability curve (i.e., the D-curve) is not the most appropriate information for use in models because it does not include systems and settings that restrict active and reactive unit output. Rather, it is the composite curve developed by the engineer(s) setting the limiters and protection. Limiter values and protection settings are created and coordinated as part of NERC Reliability Standard PRC-019. Often, test reports or data collected for PRC-019 contain the most suitable machine capability information to provide for the purposes of NERC MOD-032.

All commonly used software platforms allow the planning engineers to enter in a simplified (i.e., linearized) representation of a capability curve for each generator that typically consists of a table of data points to represent reactive limits for one or several active outputs. It is advisable for the TP and PC to request the composite capability curve and use that information for modeling to the best possible extent. If a table of values is provided, the software can automatically set the reactive limits based on the active power dispatch for each individual unit. It is advisable for the TC and PC to ensure as many units are modeled with the proper composite capability curve as possible. This ensures voltage profiles are accurate based on the dispatch assumed in the base cases.

[18] The top of the capability curve (dictated by the rotor winding temperature) or the bottom of the curve (dictated by the end-iron heating or minimum excitation limit) are protected by limiters that should be coordinated with the determined capability.

To visualize how a capability curve can be entered into a software platform, consider a generator with the simplified composite capability curve shown in Figure 4.1 (left). Note that this example only includes the over-excitation limiter (OEL) and UEL by the red and blue curves, respectively, and the generator capability by the black semi-circle. The black vertical lines represent where data is extracted to generate the linearized curve in Figure 4.1 (right) as well as the information in Table 4.1. The linearized representation should be a relatively close match to the actual composite capability curve, and the number of points selected should be based on engineering judgement. The data points are then provided in the necessary format for each specific software platform to represent the composite capability curve for the generating resource.

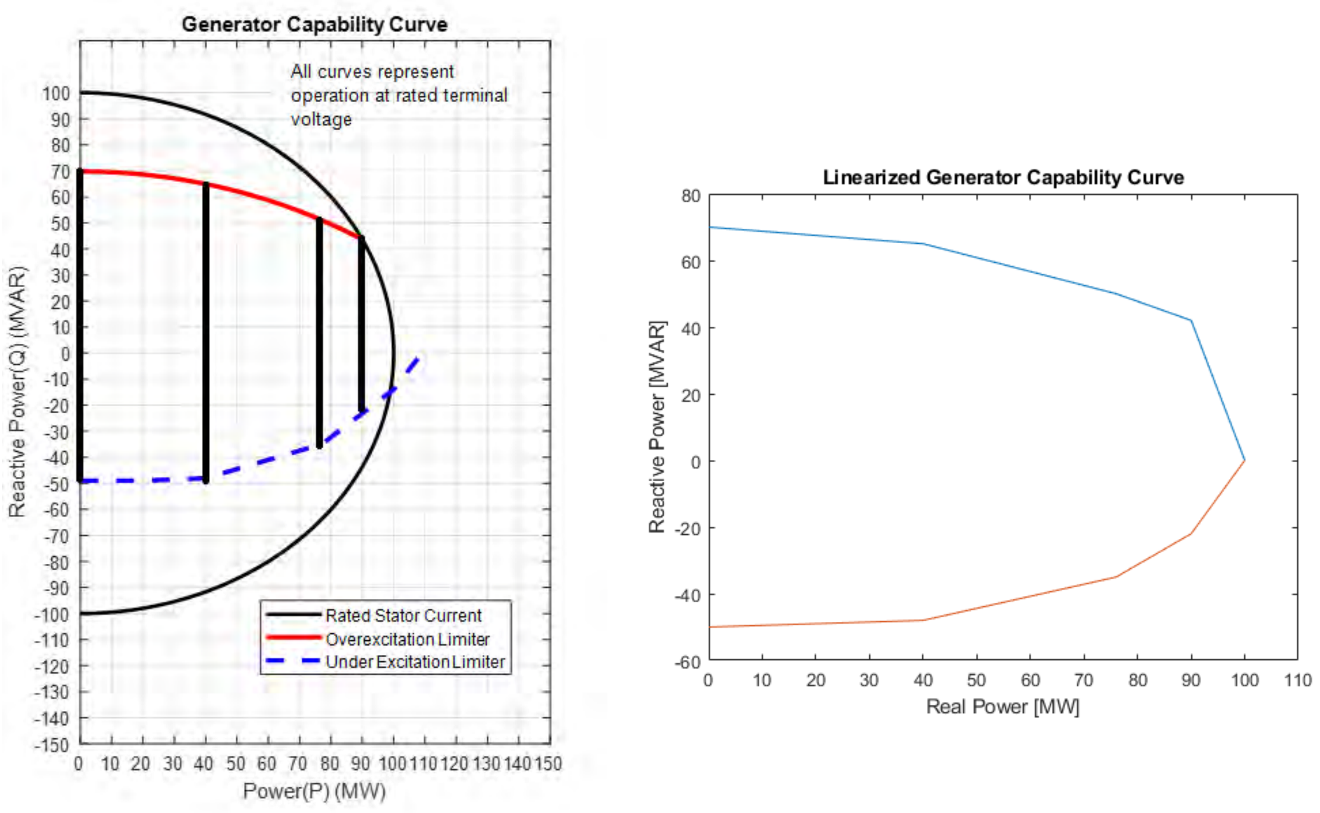


Figure 4.1: Composite Capability Curve and Linearized Curve for Modeling

Table 4.1: Active and Reactive Power Points on Composite Capability Curve

Real Power [MW]	Maximum Reactive Power [MVAR]	Minimum Reactive Power [MVAR]
0	70	-50
40	65	-48
76	50	-35
90	42	-22
100	0	0

The inclusion of a composite capability curve representation is particularly important for units dispatched across a wide range of active powers since the reactive power limits are different for each dispatch. On the other hand, units that are consistently base-loaded may suffice with just a Qmax and Qmin value provided.

Ambient temperature assumptions may also be important for some types of generating resources versus other types. Figure 4.2 shows an example curve for an air-cooled synchronous generator, demonstrating the relationship between inlet air temperature and power output from the generator. Figure 4.3 shows a capability curve at different inlet temperature conditions. Compare these curves to the singular capability curve for the hydro unit in Figure 4.1 since ambient temperature is not a factor for hydro units. The steam unit in Figure 4.4 is different from both the natural gas unit and the hydro unit. To this point, it is advisable for the TP and PC to specify the ambient temperature assumptions required to develop a complete model set. It is advisable to the TP and PC to develop an ambient temperature requirement for each season that is represented (e.g., six temperatures in the Eastern Interconnect to coincide with the light load, spring peak, summer peak, summer shoulder, fall peak, and winter peak cases). This is particularly important for summer or winter peak cases where limits may be restricted from or relaxed to their absolute limits.

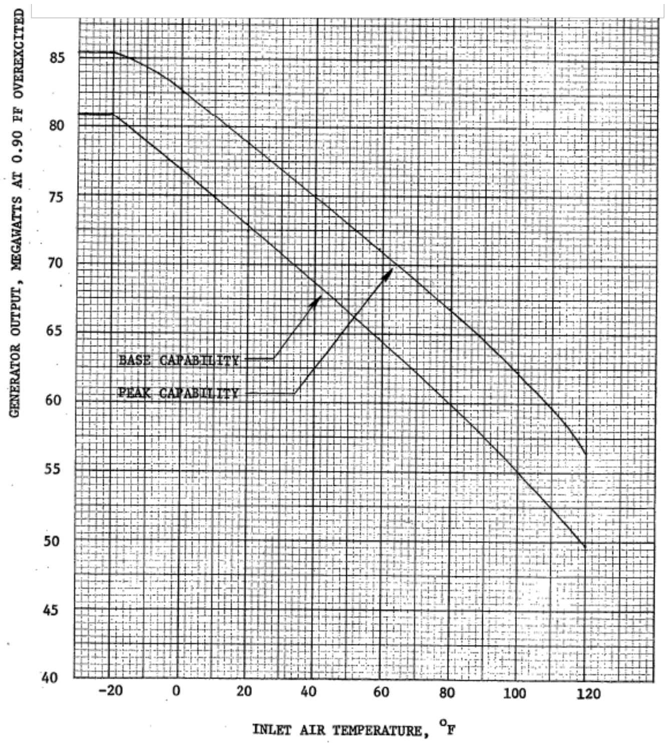


Figure 4.2: Air-Cooled Synchronous Generator Output vs. Inlet Air Temperature Curve [Source: Evergy]

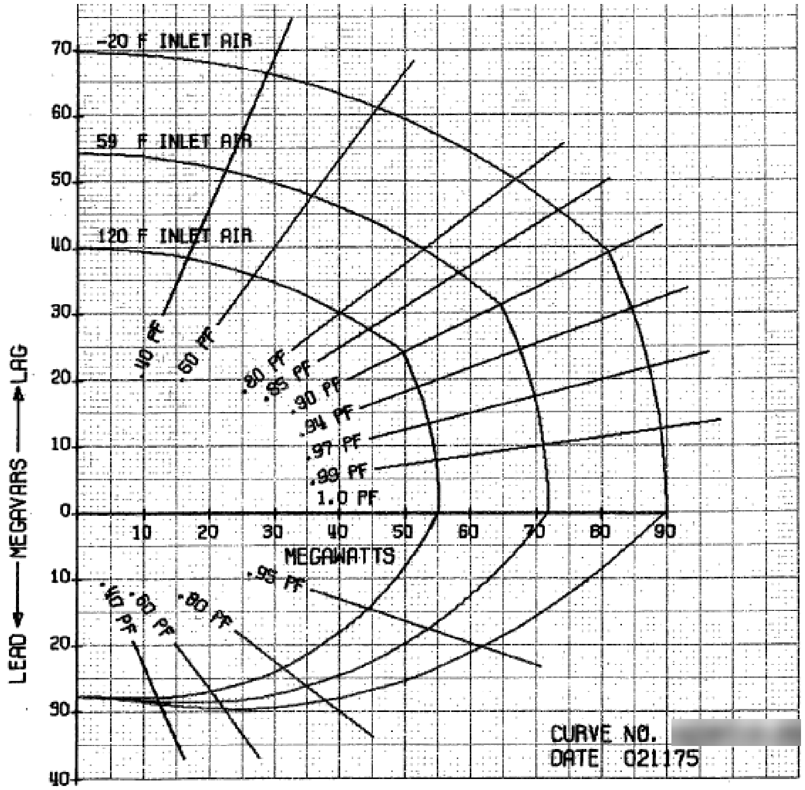


Figure 4.3: Composite Capability Curve for Ambient Cooled Natural Gas Turbine Generator [Source: Evergy]

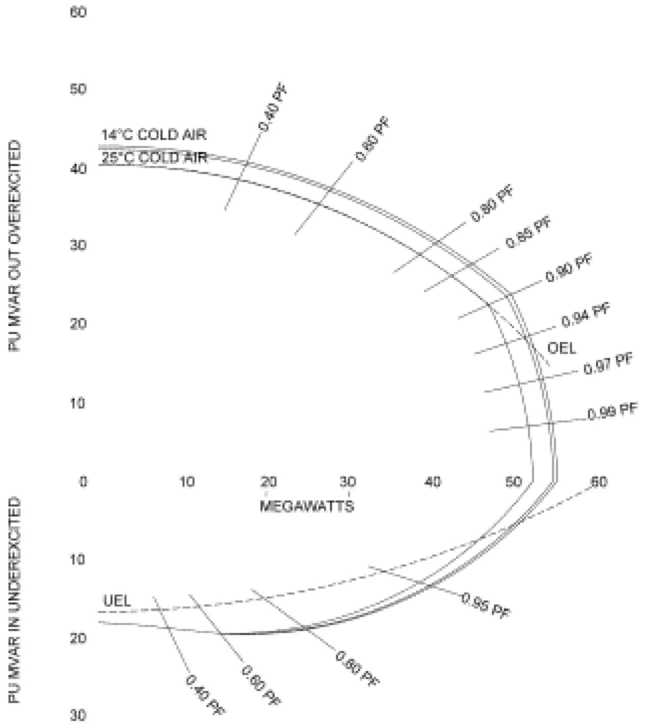


Figure 4.4: Composite Capability Curve for 54.6 MW Steam[19] Turbine [Source: PSE]

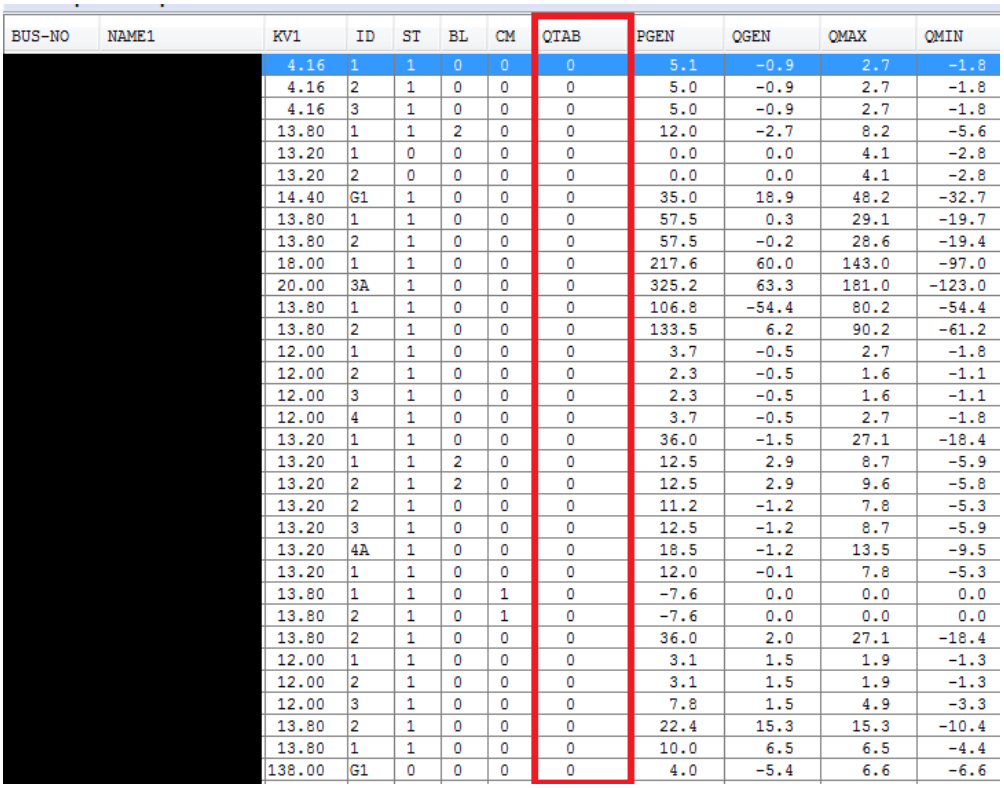
[19] Totally Enclosed Water to Air Cooled (TWAC)

Accurately modeling the composite capability curve for generating resources is directly related to the accuracy of the studies performed, particularly for any studies where voltage-related issues (either voltage instability or large post-contingency voltage changes) are a concern. Overestimation of reactive capability may put the system in a vulnerable state during normal operations during peak conditions. Similarly, underestimation of reactive capability may lead to unnecessary transmission reinforcements.

Industry continues to consider including dynamic excitation limiter models to represent the actual machine capability during dynamic simulations more accurately. This will likely begin occurring in the near future with this data readily available as part of NERC PRC-019-2 efforts. To be successful in including these models, the steady-state representation of machine capability also needs to be accurate to ensure there are no initialization issues result from mismatched data between the powerflow and dynamics databases. This will require significant model improvements beyond the capabilities and practices used today.

Capability Curve Modeling Example using PSLF

In PSLF, each generator record has a qtab flag (see Figure 4.5) that dictates whether a record exists in the qtable for the corresponding generator. If qtab = 1, then the reactive limits are determined by a piecewise linear function dictated by the data in the qtable rather than by the Qmax and Qmin parameters entered in the generator record. The powerflow solution uses the table of limits in lieu of those two parameters. Using the qtab table, up to 20 tuples of data (P, Qmx, Qmn) in ascending order of P are allowed, and the program will recreate the capability curve by using linear interpolation between adjacent points. In the qtable, the data entry for the bus number and ID (assuming bus number 100 and ID “1”) would look like the entry in Figure 4.6.



BUS-NO	NAME1	KV1	ID	ST	BL	CM	QTAB	PGEN	QGEN	QMAX	QMIN
[redacted]	[redacted]	4.16	1	1	0	0	0	5.1	-0.9	2.7	-1.8
[redacted]	[redacted]	4.16	2	1	0	0	0	5.0	-0.9	2.7	-1.8
[redacted]	[redacted]	4.16	3	1	0	0	0	5.0	-0.9	2.7	-1.8
[redacted]	[redacted]	13.80	1	1	2	0	0	12.0	-2.7	8.2	-5.6
[redacted]	[redacted]	13.20	1	0	0	0	0	0.0	0.0	4.1	-2.8
[redacted]	[redacted]	13.20	2	0	0	0	0	0.0	0.0	4.1	-2.8
[redacted]	[redacted]	14.40	G1	1	0	0	0	35.0	18.9	48.2	-32.7
[redacted]	[redacted]	13.80	1	1	0	0	0	57.5	0.3	29.1	-19.7
[redacted]	[redacted]	13.80	2	1	0	0	0	57.5	-0.2	28.6	-19.4
[redacted]	[redacted]	18.00	1	1	0	0	0	217.6	60.0	143.0	-97.0
[redacted]	[redacted]	20.00	3A	1	0	0	0	325.2	63.3	181.0	-123.0
[redacted]	[redacted]	13.80	1	1	0	0	0	106.8	-54.4	80.2	-54.4
[redacted]	[redacted]	13.80	2	1	0	0	0	133.5	6.2	90.2	-61.2
[redacted]	[redacted]	12.00	1	1	0	0	0	3.7	-0.5	2.7	-1.8
[redacted]	[redacted]	12.00	2	1	0	0	0	2.3	-0.5	1.6	-1.1
[redacted]	[redacted]	12.00	3	1	0	0	0	2.3	-0.5	1.6	-1.1
[redacted]	[redacted]	12.00	4	1	0	0	0	3.7	-0.5	2.7	-1.8
[redacted]	[redacted]	13.20	1	1	0	0	0	36.0	-1.5	27.1	-18.4
[redacted]	[redacted]	13.20	1	1	2	0	0	12.5	2.9	8.7	-5.9
[redacted]	[redacted]	13.20	2	1	2	0	0	12.5	2.9	9.6	-5.8
[redacted]	[redacted]	13.20	2	1	0	0	0	11.2	-1.2	7.8	-5.3
[redacted]	[redacted]	13.20	3	1	0	0	0	12.5	-1.2	8.7	-5.9
[redacted]	[redacted]	13.20	4A	1	0	0	0	18.5	-1.2	13.5	-9.5
[redacted]	[redacted]	13.20	1	1	0	0	0	12.0	-0.1	7.8	-5.3
[redacted]	[redacted]	13.80	1	1	0	1	0	-7.6	0.0	0.0	0.0
[redacted]	[redacted]	13.80	2	1	0	1	0	-7.6	0.0	0.0	0.0
[redacted]	[redacted]	13.80	2	1	0	0	0	36.0	2.0	27.1	-18.4
[redacted]	[redacted]	12.00	1	1	0	0	0	3.1	1.5	1.9	-1.3
[redacted]	[redacted]	12.00	2	1	0	0	0	3.1	1.5	1.9	-1.3
[redacted]	[redacted]	12.00	3	1	0	0	0	7.8	1.5	4.9	-3.3
[redacted]	[redacted]	13.80	2	1	0	0	0	22.4	15.3	15.3	-10.4
[redacted]	[redacted]	13.80	1	1	0	0	0	10.0	6.5	6.5	-4.4
[redacted]	[redacted]	138.00	G1	0	0	0	0	4.0	-5.4	6.6	-6.6

Figure 4.5: qtab Flag Representation in GE PSLF [Source: PSLF]

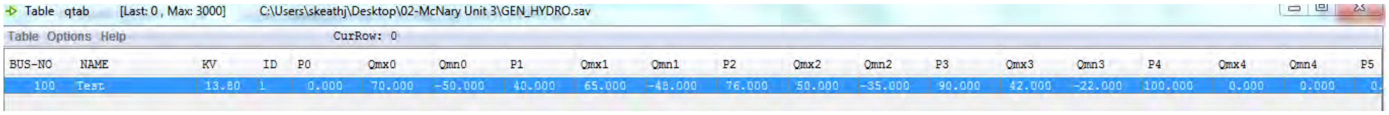


Table qtab [Last: 0 , Max: 3000] C:\Users\skeathj\Desktop\02-McNary Unit 3\GEN_HYDRO.sav

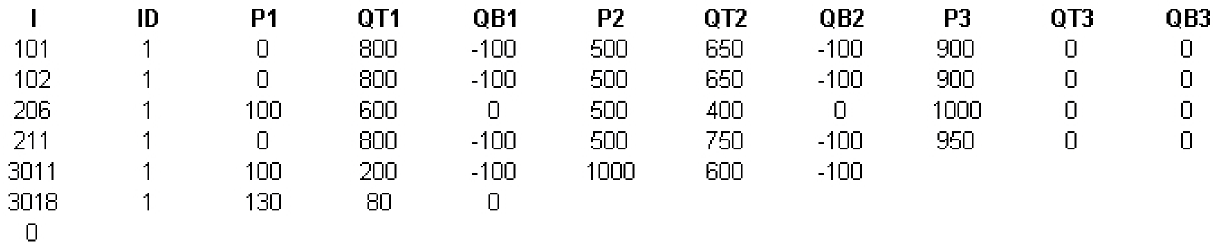
CurRow: 0

BUS-NO	NAME	KV	ID	P0	Qmx0	Qmn0	P1	Qmx1	Qmn1	P2	Qmx2	Qmn2	P3	Qmx3	Qmn3	P4	Qmx4	Qmn4	P5
100	Test	13.80	1	0.000	70.000	-50.000	40.000	65.000	-48.000	76.000	50.000	-35.000	90.000	42.000	-22.000	100.000	0.000	0.000	0.

Figure 4.6: Qtable Depicting Generator Capability Curve [Source: PSLF]

Capability Curve Modeling Example Using PSS®E

In Siemens PTI's PSS®E, the composite capability curve data is stored in a separate file with the extension .gcp (see Figure 4.7). The file itself is a space delimited file that can be edited with any text editor and must end with a new line character for each entry. The last line in the file must be terminated with a single 0, indicating to GCAP that the file is terminated.



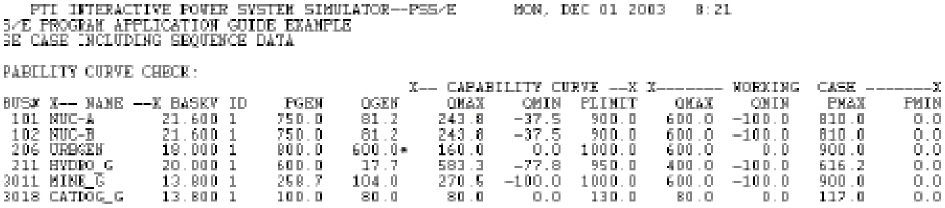
I	ID	P1	QT1	QB1	P2	QT2	QB2	P3	QT3	QB3
101	1	0	800	-100	500	650	-100	900	0	0
102	1	0	800	-100	500	650	-100	900	0	0
206	1	100	600	0	500	400	0	1000	0	0
211	1	0	800	-100	500	750	-100	950	0	0
3011	1	100	200	-100	1000	600	-100			
3018	1	130	80	0						
0										

Figure 4.7: Sample .gcp file required for the GCAP routine [Source: PTI]

Knowing the format, the .gcp file provided to the TP in the above example for the data in Table 4.1 would look like the following (still assuming a bus number of 100 and an ID of "1"):

- 100 1 0 70 -50 40 65 -48 76 50 -35 90 42 -22 100 0 0 0

The GCAP function reads the information in the .gcp files and modulates the Qmin and Qmax associated with the current Pgen in the working case. The exact details are documented in the PSS®E Program Operating Manual and the process of adjusting the generator record values is irreversible. A sample report from the PSS®E Program Operating Manual is detailed in Figure 4.8.



```
   PTI INTERACTIVE POWER SYSTEM SIMULATOR--PSS/E      MON, DEC 01 2003    8:21
3/E PROGRAM APPLICATION GUIDE EXAMPLE
SE CASE INCLUDING SEQUENCE DATA

PABILITY CURVE CHECK:
                                         X-- CAPABILITY CURVE --X X------- WORKING  CASE -------X
BUS# X-- NAME --X BASKV ID    PGEN    QGEN    QMAX    QMIN  PLIMIT    QMAX    QMIN    PMAX    PMIN
 101 NUC-A        21.600 1   750.0    81.2   243.8   -37.5   900.0   600.0  -100.0   810.0     0.0
 102 NUC-B        21.600 1   750.0    81.2   243.8   -37.5   900.0   600.0  -100.0   810.0     0.0
 206 URBGEN       18.000 1   800.0   600.0*  160.0     0.0  1000.0   600.0     0.0   900.0     0.0
 211 HYDRO_G      20.000 1   600.0    17.7   583.3   -77.8   950.0   400.0  -100.0   616.2     0.0
3011 MINE_G       13.800 1   258.7   104.0   270.5  -100.0  1000.0   600.0  -100.0   900.0     0.0
3018 CATDOG_G     13.800 1   100.0    80.0    80.0     0.0   130.0    80.0     0.0   117.0     0.0
```

Figure 4.8: Report Output for Reactive Power Checking with Capability Curve [Source: PTI]

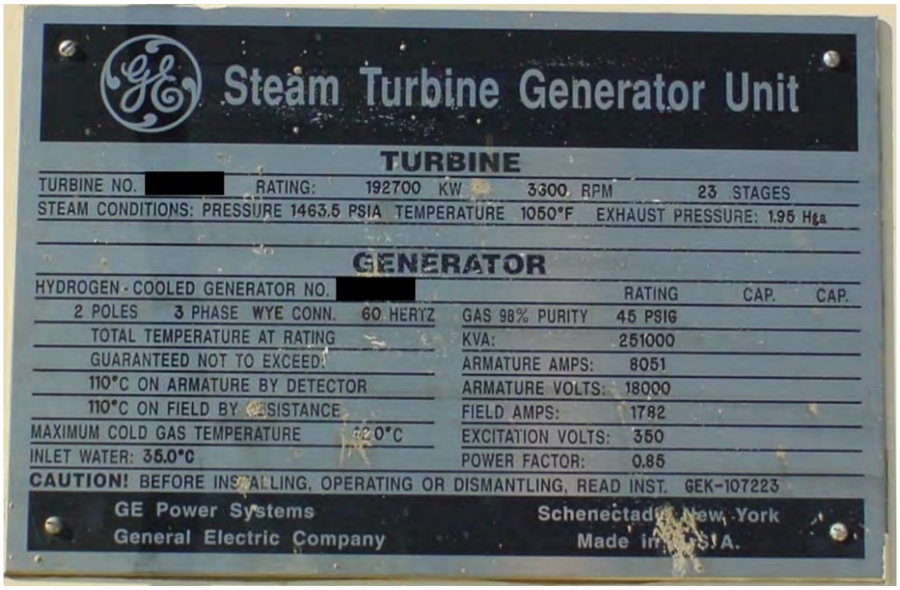
Interaction between MOD-032 and MOD-025

The generator capability data supplied for MOD-032 purposes and the data collected during capability testing for MOD-025-2 should be clearly differentiated. MOD-025 requires testing the gross maximum and minimum real power capability and the maximum and minimum reactive power capability at those real power extremes. Attachment 1 of MOD-032 also requires that these capabilities be provided to the TP and PC for modeling purposes. However, unless the full capability is reached during test (or calculated after-the-fact, something not required per MOD-025), it is expected that these values will differ from each other. Refer to the NERC *Reliability Guideline: Power Plant Model*

Verification and Testing for Synchronous Machines,[20] specifically the Chapter 3 section "MOD-032 Data and MOD-025 Testing" for more information on why these two data points are likely to differ from one another.

Nameplate Pictures and Drawings

TPs and PCs typically use a "trust but verify" approach to data collection. While it is assumed that accurate and updated information about the equipment installed in the field is provided, errors often do exist in the data. There are many reasons why the data supplied may not match reality, ranging from simple data entry errors to misinterpretation of the data requirements. For these reasons, it is often suggested (or required by the TP and PC) to provide nameplate pictures and drawings of the actual equipment whenever possible. Having the actual nameplate information can help the TP and PC identify and fix some modeling issues that may arise. **Figure 4.9** shows an example of a picture of a generator nameplate. **Figure 4.10** shows a picture of a physical GSU nameplate, the nameplate drawing (typically separate from the GSU test report), and a physical inspection of the GSU tap position. Incorrect GSU tap position is a very common source of model error in interconnection-wide models that can lead to highly inaccurate simulation results. Refer to **Appendix E** for more information about GSU modeling.



Steam Turbine Generator Unit

TURBINE

TURBINE NO. [redacted] RATING: 192700 KW 3300 RPM 23 STAGES

STEAM CONDITIONS: PRESSURE 1463.5 PSIA TEMPERATURE 1050°F EXHAUST PRESSURE: 1.95 Hga

GENERATOR

HYDROGEN - COOLED GENERATOR NO. [redacted]

		RATING	CAP.	CAP.
2 POLES 3 PHASE WYE CONN. 60 HERTZ	GAS 98% PURITY	45 PSIG		
TOTAL TEMPERATURE AT RATING	KVA:	251000		
GUARANTEED NOT TO EXCEED:	ARMATURE AMPS:	8051		
110°C ON ARMATURE BY DETECTOR	ARMATURE VOLTS:	18000		
110°C ON FIELD BY RESISTANCE	FIELD AMPS:	1782		
MAXIMUM COLD GAS TEMPERATURE 4[illegible]0°C	EXCITATION VOLTS:	350		
INLET WATER: 35.0°C	POWER FACTOR:	0.85		

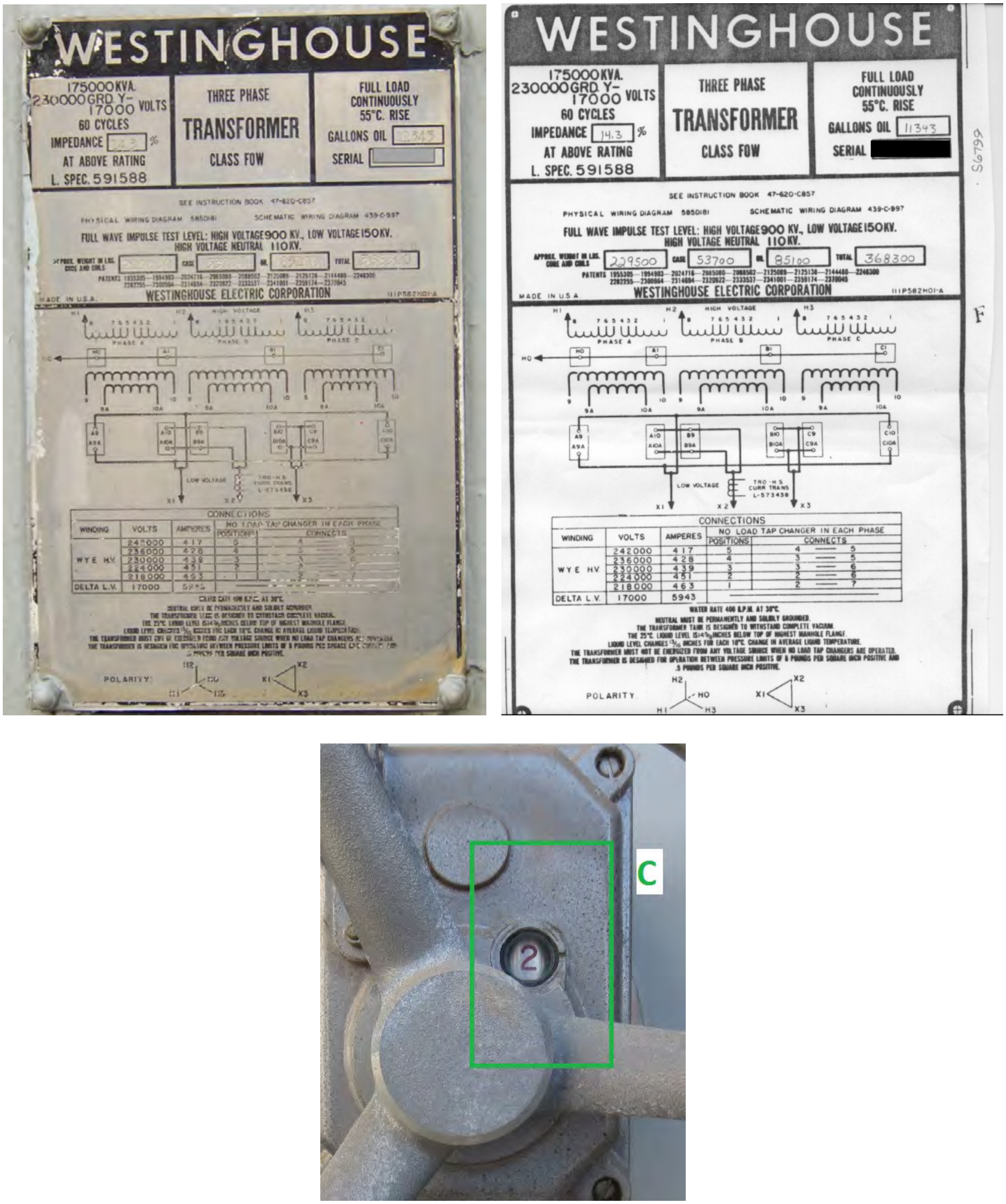
CAUTION! BEFORE INSTALLING, OPERATING OR DISMANTLING, READ INST. GEK-107223

GE Power Systems
General Electric Company

Schenectady, New York
Made in U.S.A.

Figure 4.9: Example of Generator Nameplate Picture

[20] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_-_PPMV_for_Synchronous_Machines_-_2018-06-29.pdf



WESTINGHOUSE

175000 KVA.
230000 GRD. Y– 17000 VOLTS
60 CYCLES
IMPEDANCE 14.3 %
AT ABOVE RATING
L. SPEC. 591588

THREE PHASE
TRANSFORMER
CLASS FOW

FULL LOAD
CONTINUOUSLY
55°C. RISE
GALLONS OIL 11343
SERIAL [redacted]

SEE INSTRUCTION BOOK 47-620-C857

PHYSICAL WIRING DIAGRAM 585D181 SCHEMATIC WIRING DIAGRAM 439-C-997

FULL WAVE IMPULSE TEST LEVEL: HIGH VOLTAGE 900 KV., LOW VOLTAGE 150 KV.
HIGH VOLTAGE NEUTRAL 110 KV.

APPROX. WEIGHT IN LBS. CORE AND COILS 229500 CASE 53700 OIL 85100 TOTAL 368300

PATENTS 1955305—1994903—2024716—2085080—2088502—2125089—2125138—2144480—2246300
2282255—2300964—2314694—2320922—2333537—2341001—2359174—2370045

MADE IN U.S.A. WESTINGHOUSE ELECTRIC CORPORATION 111P582H01-A

S6799

F

CONNECTIONS				
WINDING	VOLTS	AMPERES	NO LOAD TAP CHANGER IN EACH PHASE	
			POSITIONS	CONNECTS
WYE HV	242000	417	5	4 — 5
	236000	428	4	3 — 5
	230000	439	3	3 — 6
	224000	451	2	2 — 6
	218000	463	1	2 — 7
DELTA L.V.	17000	5943		

WATER RATE 400 G.P.M. AT 30°C.
NEUTRAL MUST BE PERMANENTLY AND SOLIDLY GROUNDED.
THE TRANSFORMER TANK IS DESIGNED TO WITHSTAND COMPLETE VACUUM.
THE 25°C. LIQUID LEVEL IS 14 5/8 INCHES BELOW TOP OF HIGHEST MANHOLE FLANGE.
LIQUID LEVEL CHANGES 13/16 INCHES FOR EACH 10°C. CHANGE IN AVERAGE LIQUID TEMPERATURE.
THE TRANSFORMER MUST NOT BE ENERGIZED FROM ANY VOLTAGE SOURCE WHEN NO LOAD TAP CHANGERS ARE OPERATED.
THE TRANSFORMER IS DESIGNED FOR OPERATION BETWEEN PRESSURE LIMITS OF 8 POUNDS PER SQUARE INCH POSITIVE AND .5 POUNDS PER SQUARE INCH POSITIVE.

POLARITY

Figure 4.10: Example of GSU Nameplate Picture (top left), Drawing (top right), and Physical Tap Position (bottom)

Modeling Station Service Load

MOD-032-1 Attachment 1 states that "station service auxiliary load for normal plant configuration" should be provided to the TP and PC in the same manner as that required for aggregate demand under item 2 of Attachment 1. Station service load should be explicitly represented in powerflow and dynamic simulations and should not be netted with the generator(s). Typically, station service load is modeled as an aggregate load in the base case (see left side of Figure 4.11) that represents one or more station service transformers and all the low-side auxiliary equipment. Load may be represented for each generating unit or for the entire plant. More detailed examples of representing station service load in the model are shown on the right side of Figure 4.11 based on the configuration within the plant. The unit auxiliary transformer may be modeled explicitly and the station service load placed on the low side of the unit auxiliary transformer. This creates complexity in the model but does allow the TP and PC to better understand the auxiliary load bus voltages. This is particularly important for studies that examine any potential ride-through issues where prolonged low voltages could cause auxiliary load to trip, leading to potential generating unit (or plant) tripping.

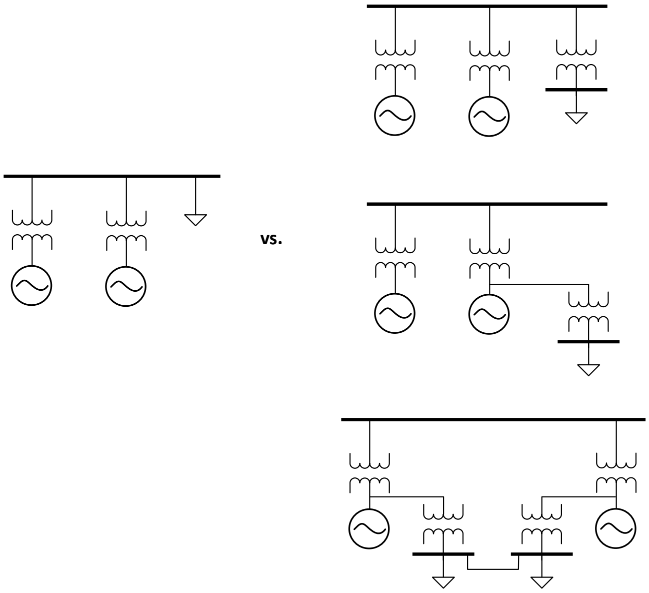


Figure 4.11: Examples of Station Service Load Representation [Source: PSEG]

TPs and PCs should provide guidance as to how they model station service load in the base case. While not specifically listed in Attachment 1 of MOD-032-1, the following information described here is useful for TPs and PCs to request to develop accurate models to represent station service:

- **Types of Station Service Loads:** Information pertaining to the types of loads (e.g., pumps, fans, compressors) should be requested so that an appropriate dynamic load model can be developed for dynamic simulations. The DEO should use engineering judgment to understand the level(s) at which auxiliary load tripping may occur and provide that information to the TP and PC as well. Simplified one-line diagrams of the stations service load (at least the transformers) should be provided as well. Any information pertaining to the transformer impedance and configuration may also be useful if modeled explicitly.

- **Change in Station Service Load Levels:** Often, the auxiliary loading changes based on generating unit(s) output in the plant. Hence, real and reactive station service loading should be provided at maximum and minimum outputs. If multiple units are at the plant, then any changes in station service load level should also be provided for all potential unit configurations (e.g., with one unit on-line versus two units on-line). This way, the TP and PC can set up station service load in the model appropriately.

Unit Breaker Modeling for Short Circuit Studies

MOD-032-1 Attachment 1 does not describe breakers as a necessary component for modeling. However, this data may be required for short-circuit studies in some cases. In particular, the generator breaker data should be provided such that these breakers can be included in breaker duty studies (rated kV, continuous rating in amps, and interrupt rating in kA). Figure 4.12 provides an example system as typically modeled for power flow studies (left, no breaker detail is included) and the explicitly modeled breakers necessary for short circuit studies (right). Station buses that are tied together should be included in the contribution to a BES breaker. DEOs may only study short-circuit at one level (e.g., 40 kA) during construction and may not reassess breaker duty that can change over time with changes in the transmission system. Fault studies at generator terminals should include the unit breaker so that the total contribution from the grid can be correctly observed on that breaker. Therefore, this data should be requested as part of the MOD-032 data requests for short-circuit information.

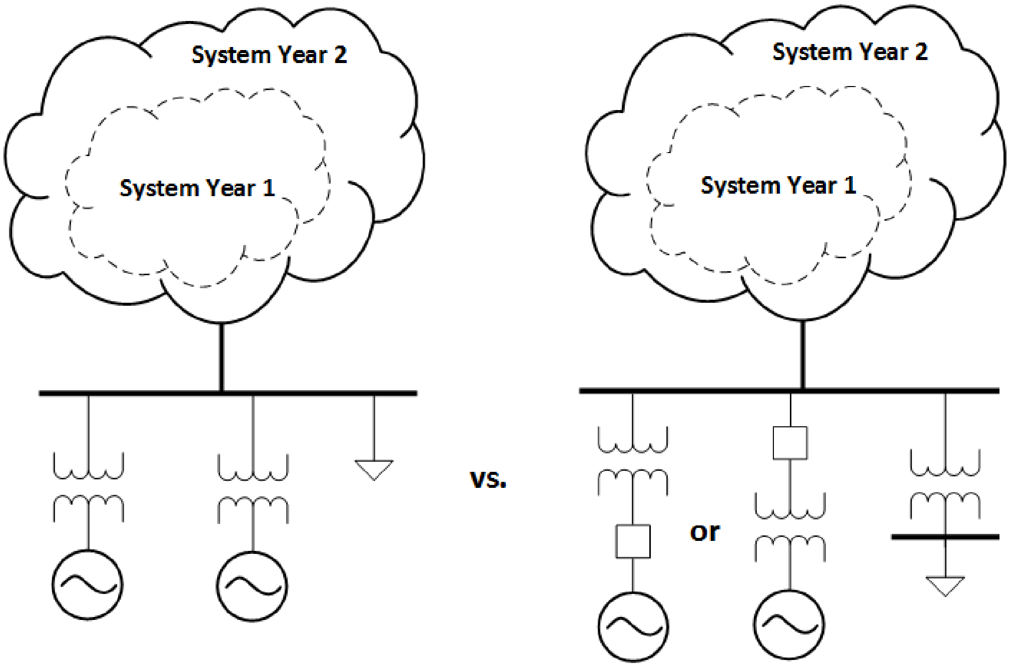


Figure 4.12: No (Left) versus Representation (Right) of Unit Breaker Status

[Source: PSEG]

Contingencies

The TP or PC may request information pertaining to how the unit(s) or plant will operate under contingency situations. For example, the TP or PC may request information for how a steam turbine will behave during a forced outage of a natural gas unit. Similarly, the TP or PC may request information pertaining to any risks associated with entire plant tripping so that these conditions may be studied as part of sensitivity cases or extreme events. Furthermore, any contingency that causes additional units to trip should be well documented for the TP and PC. This includes cross compound units where both generators should be tripped in the model for a contingency of a single unit. Typically there will be individual dynamic models. Steady-state powerflow models may or may not represent the units separately. Short-circuit models should model them separately.

This contingency information is specifically useful for the TP and PC to understand what may happen within the plant that they otherwise are not able to determine with high voltage one-line diagrams that are typically available for the TP and PC.

Modeling Synchronous Condensing or Pumping Capability

Synchronous condensers are typically modeled as a generating resource in the steady-state base case with a Pmax value of zero and associated dynamics models. These practices are fairly consistent across entities since the modeling is typically straightforward. However, some generating units have the ability to also operate as a synchronous condenser or as a pump (e.g., pumped storage). The modeling practices for these capabilities are not consistent across entities and have led to modeling challenges. The TP and PC should know whether a unit has either capability, and the DEO should inform the TP and PC accordingly. This may require the TP and PC to provide additional data or information to the DEO. The TP and PC likely have an understanding of how these capabilities are used for correct dispatching in the base case setup.

For units with pumping capability, the TP and PC will have specific data requirements and reporting procedures to ensure sufficient data is provided to model the two modes correctly. This typically involves distinct parameter values for Pmax, Pmin, Qmax, Qmin, and Pgen for each mode. The dynamic models may also need to be changed when switching modes. Some TPs and PCs may use the same model and have scripts for updating parameter while others may use different model records and change the unit statuses accordingly.

The GO should request information to help facilitate accurate data submission if any data requirements or reporting procedures set by the TP and PC are not clear.

Appendix A: Steady-State Modeling Data

This appendix provides information regarding data that could be requested for steady-state modeling purposes.

Generator Information

Table A. 1 provides the recommended steady state modeling data for the generator and plant auxiliary load to request from GOs for MOD-032. This list is comprehensive but not exhaustive. The PC or TP may request other information necessary for modeling purposes.

Table A.1: Recommended Steady-State Modeling Data for MOD-032 Data Requests

Common Name	Detailed Description	Data Source
3a. Real Power Capability *Real Power Capabilities - Gross Maximum and Minimum Values*		
Gross Maximum Value (P_{max})	For the purposes of a consistent approach, the maximum value of active power (Pmax) output [MW] used in interconnection-wide case shall be as follows: The lesser of the mechanical power of the turbine and the continuous electrical capability of the generator for +/- 0.95 lead/lag power factor, measured at the generator terminals and excluding all supplemental firing capability (and/or any power augmentation) for conditions[21] specified by the TP If the turbine is underrated so therefore generator 0.95 lead/lag reactive capability can always be achieved, then this power factor requirement can always be met (report max gate). OR If the turbine is over-rated such that the turbine can continuously operate beyond the active power level specified by 0.95 lead/lag, then the model should limit Pmax to the point where 0.95 lead/lag power factor can still be met (not max gate).	• Composite capability curve including generator and turbine capability (specification sheets, if available) and excitation limiters curves (OEL and UEL) • PRC-019-2 compliance reports • Power output versus temperature curves, if applicable • Power output versus hydro head level, if applicable (refer to sections of this guideline for discussion on these curves.) • OEM-provided specification sheets and data • Contractual obligations

[21] This should include all factors that may in any way affect machine power capability. This may include, but is not limited to, ambient temperature assumptions and hydro headlevel assumptions. The TP and PC may either require a curve, where applicable, or the specific set of ambient conditions in which data should be provided for including season, time of day, temperature, etc.

Table A.1: Recommended Steady-State Modeling Data for MOD-032 Data Requests

Common Name	Detailed Description	Data Source
Gross Minimum Value (P_{min})	The minimum generator output [MW], measured at the generator terminals, to ensure the generating unit does not become unstable or violate any emissions regulations [MW] *Note that special consideration needs to be given to pump storage gens.	• Minimum generation limits due to environmental regulations • (NOTE: This value may not match the MOD-025-2 testing data unless engineering calculations were performed.)
3b. Reactive Power Capability *Reactive Power Capabilities - Maximum and Minimum Values at Real Power Capabilities in 3a Above*		
Gross Maximum Value	Maximum sustained overexcited reactive output [MVAR] at the generator terminals, at the real power capability (3a above) These values should be based on the most limiting constraints as shown in PRC-019-2 coordination curves (e.g., OEL, UEL) and based on 1.0 pu terminal voltage.	• Composite capability curve, including generator and turbine capability (specification sheets if available) and excitation limiters curves (OEL and UEL) • PRC-019-2 compliance reports • (NOTE: This value may not match the MOD-025-2 testing data unless engineering calculations were performed.)
Gross Minimum Value	Maximum sustained under-excited reactive output [MVAR] at the generator terminals at the real power capability (3a above) These values should be based on the most limiting constraints as shown in PRC-019-2 coordination curves (e.g., under-excitation limiter, loss of field) and on 1.0 pu terminal voltage.	
3c. Station Service Auxiliary Load for Normal Plant Configuration *Provide data in the same manner as that required for aggregate demand under Item 2, above.* *All loads associated with the generating unit or plant required for operations, including the total aggregate of terminal connected, high side feeds, and separate bus feeds* *A more detailed station service/auxiliary load profile may be provided to show more accurate demands.*		
Station One-line Diagram	Station one-line diagram that shows station auxiliary transformers and loads	• MOD-025-2 test reports • Plant files

Table A.1: Recommended Steady-State Modeling Data for MOD-032 Data Requests

Common Name	Detailed Description	Data Source
Station Service Real Power Load at Generator Gross Maximum Power Output (P_{max})	Aggregate amount [MW] of load for each voltage level in the generator substation	• Historical plant data • MOD-025-2 test reports
Station Service Reactive Power Load at Generator Gross Maximum Power Output (Q_{max})	Aggregate amount [MVAR] of load for each voltage level in the generator substation	
Station Service Real Power Load at Minimum Generator Gross Power Output (P_{min})	Aggregate amount [MW] of load for each voltage level in the generator substation	
Station Service Reactive Power Load at Minimum Generator Gross Power Output (Q_{min})	Aggregate amount [MVAR] of load for each voltage level in the generator substation	
3d. Regulated Bus* and Voltage Set Point *As typically provided by the TOP*		
Regulated Bus	Name and nominal voltage of the bus specified by the TOP to maintain voltage schedule as per VAR-002-4 This is typically at the point of interconnection to the BPS. While required as a data point in MOD-032, the TP/PC typically get this information from the TOP.	• Interconnection requirements • Bus that the exciter voltage transformer is connected to unless any impedance compensation is used (in which case, describe the location of that impedance) • Describe any adjustments in control system if applicable

Table A.1: Recommended Steady-State Modeling Data for MOD-032 Data Requests		
Common Name	**Detailed Description**	**Data Source**
Voltage Set Point	Voltage set point [pu] specified by the TOP as per VAR-001-4 associated with the Regulated Bus. Voltage set points may change based on system conditions (peak load, off-peak load, seasonal, etc.). While required as a data point in MOD-032, the TP/PC typically get this information from the TOP.	• Provided by TOP (typically sent by TOP on annual basis)
3e. Machine MVA Base		
MVA Base	The nameplate MVA base of a generating unit (synchronous generator, synchronous condenser and pump storage) for which the dynamic parameters are per unitized on For dispersed power producing resources (e.g., solar or wind), this data may not be located on the physical nameplate of the turbines or inverters; however, the MVA base of the aggregate resources should still be used for per unitizing dynamics data.	• Generator nameplate
3g. Generator Type		
Generator prime mover type and associated fuel type	Example prime movers: hydraulic turbine, combustion turbine, steam turbine, wind turbine (Type 1 to Type 5), solar photovoltaic (PV) Example fuel types: natural gas, coal, nuclear, wind, solar, geothermal	• N/A
Additional Data		
Composite Capability Curve	Generator D-curve with associated limiting constraints as shown in PRC-019-2 coordination curves (e.g., OEL, UEL, LOF) based on 1.0 pu terminal voltage This may not be the tested capability information supplied for MOD-025-2 testing, particularly if the unit was constrained from hitting its capability limits due to external factors during testing.	• PRC-019-2 reports • Manufacturer information • Generator data sheet(s)

Table A.1: Recommended Steady-State Modeling Data for MOD-032 Data Requests

Common Name	Detailed Description	Data Source
Real Power Output vs. Ambient Conditions Curve[22]	Curves associated with power output compared with ambient conditions that will change power output from nominal (e.g., hydro: head vs. power curve, natural gas: temperature vs. power curve, wind: wind speed vs. power curve)	• Manufacturer datasheets
One-Line Diagram	Simplified electrical one-line diagram up to point of Interconnection TP can generally get this information from the MOD-025-2 submittal, or interconnection service agreements. However, the TP may request this information if needed in some cases.	• Plant datasheets

Synchronous Machine Impedance

Table A.2 provides the recommended steady state impedance data for synchronous machines to request from GOs for MOD-032.

Table A.2: Recommended Steady-State Synchronous Machine Impedance Data for MOD-032 Data Requests

Common Name	Detailed Description	Data Source
DC Armature Resistance	The dc armature resistance (Ra) is a value generally provided by the OEM and should be converted to per-unit on the machine MVA and kV bases [pu]. If no OEM data is available and no adequate estimation technique is available (or practical), a value of 0.0015 pu should be used as an approximation.	• OEM documentation, unit testing
Unsaturated D-axis sub-transient reactance (X’’du)	The unsaturated D-axis sub-transient reactance provided for load flow should match the X’’du value used in the dynamic rotor model [pu] If no OEM data is available and no adequate estimation technique is available (or practical), a value of 0.20 pu should be used as an approximation.	• OEM documentation • MOD-026-1 test report

[22] This curve, in combination with the “composite” capability curve, is used by the TP or PC to modify the real and reactive power capability (P_{max}, Q_{max}, Q_{min}) for various study conditions (e.g., ambient temperature changes based on season, time of day). Some TPs and PCs may alternatively request the separate models of generating resources for each of these conditions that already include these assumptions. In these cases, the TP or PC will need to clearly specify the assumptions for ambient temperature.

Equivalent Type I, II, and III Wind Machine Impedance

Table A.3 provides the recommended steady state impedance values for equivalent wind machines that represent wind turbines that utilize one of the following technologies: direct grid connection (Type I), induction machine with external controlled resistors (Type II), or doubly-fed induction machine (Type III). Generally, Type I, II, and III wind machines are represented in grid-level simulations as one or several equivalent machines rather than including a model for each machine in the plant. The equivalent machine impedance should either utilize OEM data for a single machine or an average of the OEM impedance of all machines included in the equivalent.

Table A.3: Recommended Steady-State Type I, II, or III Wind Machine Impedance Data for MOD-032 Data Requests

Common Name	Detailed Description	Data Source
DC Armature Resistance	The dc armature resistance (Ra) is a value generally provided by the OEM and should be converted to per-unit on the machine MVA and kV bases [pu]. If no OEM data is available and no appropriate/adequate estimation technique is available (or practical), a value of 0.0015 pu should be used as an approximation.	• OEM documentation • MOD-026-1 test report
Unsaturated D-axis transient reactance (X’du)	The unsaturated D-axis transient reactance provided for load flow should match the X’’du value used in the dynamic rotor model [pu]. If no OEM data is available and no appropriate/adequate estimation technique is available (or practical), a value of 0.50 pu should be used as an approximation.	• OEM documentation • MOD-026-1 test report

Equivalent Type IV Wind Machine or Solar PV Impedance

Table A.4 provides the recommended steady state impedance values for equivalent inverter-based resources (IBRs), most commonly Type IV wind machines or solar PV installations. IBRs are typically represented in grid-level simulations as one or several equivalent machines rather than including a model for each inverter in the plant. The source impedance for IBRs should represent the current-clamping capability of the inverter power electronics.

Table A.4: Recommended Steady-State Type IV Wind Machine or Solar PV Impedance Data for MOD-032 Data Requests		
Common Name	**Detailed Description**	**Data Source**
Reactive Component	$XSource = ZSource\ [pu]$ $ZSource = \frac{V_{rated[\,pu]}}{I_{rated,[pu]}}\ [pu]$ $V_{rated} = 1.0\ [pu]\ (assumed)$ $I_{rated} = Maximum\ Rated\ Current\ [pu]\ (supplied\ by\ GO)$ I_{rated} [pu] is typically included in the dynamic model and represents the transient current rating. For second-generation renewable models, it is part of the electrical control model and should be verified by the GO.	• OEM documentation • MOD-026-1 test report

Generator Step-Up and Station Transformer Information

Table A.5 provides the recommended data for steady-state modeling data for the GSU or GO-owned station transformer(s) that should be requested from GOs for MOD-032. This list is comprehensive but not exhaustive. The PC or TP may request any other information necessary for modeling purposes.

Table A.5: Recommended Steady-State Transformer Data for MOD-032 Data Requests

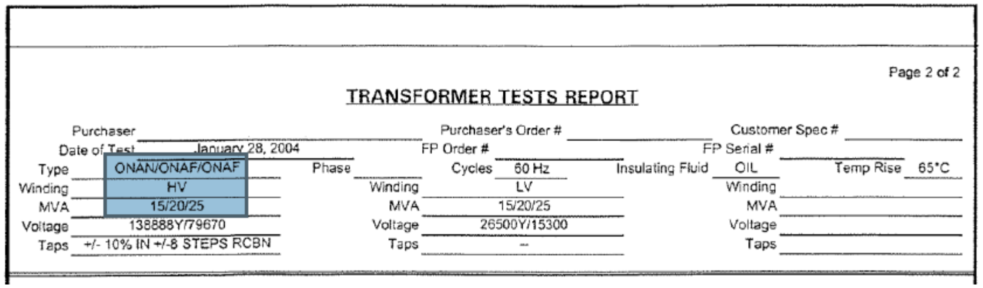
Common Name	Detailed Description	Data Source
GSU transformer name	Descriptive name of the GSU It should ideally match any name agreed upon between the GO, GOP, and TOP.	• Plant one-line diagrams • Other plant documentation
MVA base (usually self-cooled rating)	The MVA base for which the impedance is provided; usually the lowest MVA rating (for transformers with multiple MVA ratings); MVA base, impedance, and tap position should all be matching.  Page 2 of 2 TRANSFORMER TESTS REPORT Purchaser ____ Purchaser's Order # ____ Customer Spec # ____ Date of Test January 28, 2004 FP Order # ____ FP Serial # ____ Type ONAN/ONAF/ONAF Phase ____ Cycles 60 Hz Insulating Fluid OIL Temp Rise 65°C Winding HV Winding LV Winding ____ MVA 15/20/25 MVA 15/20/25 MVA ____ Voltage 138888Y/79670 Voltage 26500Y/15300 Voltage ____ Taps +/- 10% IN +/-8 STEPS RCBN Taps -- Taps ____	• Transformer nameplate • Transformer factory test report
Winding connection configuration	Winding connection configuration for each winding (e.g., grounded-wye, wye, delta)	• Transformer nameplate • Transformer factory test report

Table A.5: Recommended Steady-State Transformer Data for MOD-032 Data Requests		
Common Name	**Detailed Description**	**Data Source**
All transformer positive sequence impedances from nameplate (% and MVA base) or from factory test report (load-losses [W] and impedance %)	The positive sequence impedance model parameters can be calculated by using the load-loss values given in the test report (should be losses in watts and % impedance). If multiple results for the same test are given, use the results for the nominal taps or the tap setting which the transformer will be set if known and available. For a two-winding transformer, the per-unit values are computed as follows: $$R_{1,pu} = \frac{P_c}{S_n}[pu]$$ $$X_{1,pu} = \sqrt{Z_{1,pu}^2 - R_{1,pu}^2}\,[pu]$$ Where: - $R_{1,pu}$ is the positive sequence resistance [pu] - $X_{1,pu}$ is the positive sequence reactance [pu] - $Z_{1,pu}$ is the positive sequence impedance [pu] - P_c are the full load copper losses [W]; corrected to 85°C, if available - S_n is the MVA base at which the load loss test was performed [MVA] For a three-winding transformer, this calculation should be performed for the H-X, H-Y, and X-Y windings. The report should also include values for losses for these windings.	• Transformer nameplate • Transformer factory test report

Table A.5: Recommended Steady-State Transformer Data for MOD-032 Data Requests		
Common Name	**Detailed Description**	**Data Source**
Magnetization admittance (i.e., No-Load Losses [W] and Exciting Current [%])	The magnetizing admittance accounts for the losses of the transformer incurred to magnetize the core. This is also called no-load loss because it corresponds to the power lost if the high-side of the transformer is energized but no load is connected. Modeling software requires this parameter to be entered in per-unit on the system MVA base (i.e., 100 MVA). $$G_{pu} = \frac{P_{NL[W]}}{MVA_{System} * 10^6} [pu]$$ $$B_{pu} = (-1) * \sqrt{\left(\frac{I_{exc}}{100} * \frac{MVA_{NL[MVA]}}{MVA_{System}}\right)^2 - G_{pu}{}^2} [pu]$$ Where: - G_{pu} is the magnetizing conductance (real part of the magnetizing admittance) [pu] - $P_{NL[W]}$ is the No-Load losses [W] - $MVA_{NL[MVA]}$ is the MVA base at which the No-Load test was performed [MVA] - MVA_{System} is the system MVA base (typically 100 MVA) [MVA]. - B_{pu} is the magnetizing susceptance (imaginary part of the magnetizing admittance) [pu]. - I_{exc} is the magnetizing current [%]	• Transformer factory test report
Nominal winding voltage	Nominal voltage of the primary, secondary, and tertiary (if applicable) windings [kV]	• Transformer nameplate

Table A.5: Recommended Steady-State Transformer Data for MOD-032 Data Requests

Common Name	Detailed Description	Data Source
Tap ratio	This value is the ratio of the winding voltage at the present tap setting divided by the nominal winding voltage For instance, if the nominal winding voltage is 345 kV (but the tap is presently set to 353.625 kV), the tap ratio is 1.025 (353.625 / 345 = 1.025). Any winding with a tap changer may have a tap ratio other than 1.0. If a winding does not have a tap changer, the tap ratio must be 1.0. This data may be supplied as part of MOD-025 testing.	• Historical plant data

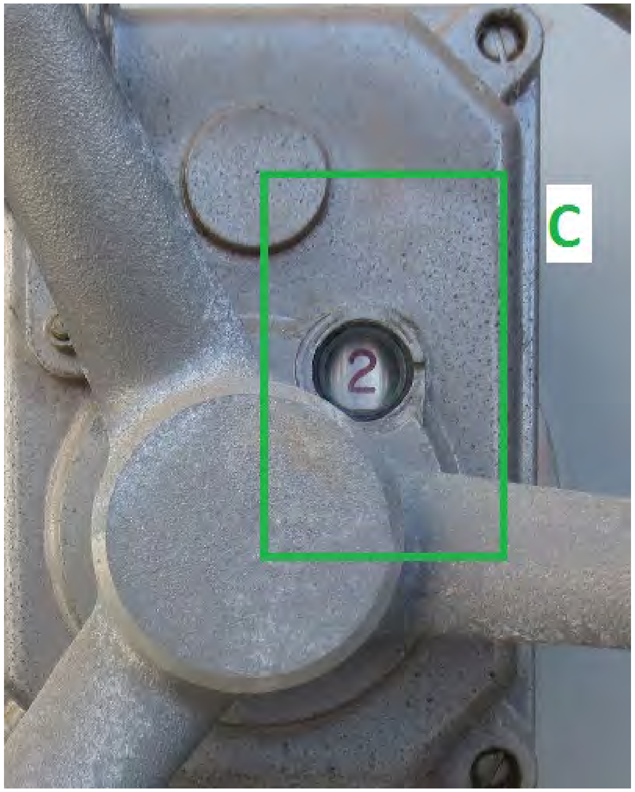
Table A.5: Recommended Steady-State Transformer Data for MOD-032 Data Requests		
Common Name	**Detailed Description**	**Data Source**
Fixed tap position	Tap position to which the no-load tap is set for normal system operation; this must be verified by inspecting the transformer and generally does not change. 	• Physical tap position from in-service (usually a dial with a padlock)
No Load Tap Changer (NLTC) and Under Load Tap Changer (ULTC) minimum and Maximum tap position limits	Most transformers have a tap NLTC range of ±5% (10% total range) Most GSUs do not have a ULTC; however, when a ULTC is present, common limits are ±10% from nominal (20% total range).	• Transformer nameplate • Transformer factory test report

Table A.5: Recommended Steady-State Transformer Data for MOD-032 Data Requests		
Common Name	**Detailed Description**	**Data Source**
Number of tap positions (for both ULTC and NLTC)	The number of physically available tap positions that can be used to regulate or change the tap ratio Both NLTCs and ULTCs have at least two tap positions. Generally, NLTCs have five steps: one nominal, two above-nominal, and two below-nominal. Generally, ULTCs have 33 steps: one nominal, 16 above-nominal, and 16 below-nominal.	• Transformer nameplate • Transformer factory test report
ULTC mode of operation	If a GSU has a ULTC, the TP should be made aware of how the ULTC is used: as a fixed tap or if it is operated manually or automatically to regulate power system quantities. ULTC operation is considered automatic when it is used to dynamically regulate power system quantities (e.g., voltage, VARs) through an automated process. In this scenario, the control mode of the ULTC is set to "Automatic." ULTC operation is considered manual when a system operator uses it to regulate power system quantities through remote adjustment capability. In this scenario, the control mode of the ULTC is set to "Manual." ULTC operation is considered fixed when it is not used to dynamically regulate power system quantities, cannot be adjusted remotely, and must be manually changed by field personnel.	• SCADA data • Protection and control engineering
ULTC regulated quantity	ULTCs may be set to automatically regulate electrical quantities, such as voltage or MVAR flow. If an automatically regulating ULTC is present on the GSU, the TP should be made aware of what electrical quantity is being regulated (e.g., voltage).	• SCADA data • Protection and control engineering

Table A.5: Recommended Steady-State Transformer Data for MOD-032 Data Requests

Common Name	Detailed Description	Data Source
ULTC set point and regulation band	To allow correct operation of automatically adjusted ULTCs in power flow simulations, it is necessary for the TP to understand the bounds at which the ULTC will operate. ULTC operation can be broadly captured by using a desired quantity setpoint and a regulation bandwidth. This consists of the following three data points: 1. Desired regulated quantity set point (e.g., voltage of 1.0375 PU) 2. Desired regulation bandwidth maximum (e.g., voltage of 1.04375 PU 3. Desired regulation bandwidth minimum (e.g., voltage of 1.03125 PU)	• SCADA data • Protection and control engineering
In-service status (in or out)	Specify whether the GSU is in service or should be set out of service. Typically, this will be specified as in service unless out for an extended period during the conditions being studied in the base case.	• Maintenance schedule
MVA ratings (normal and emergency)	This is the normal and emergency MVA rating of the most limiting element of the GSU and/or any series components in line with the GSU.	• Transformer nameplate • Facility ratings documentation
Picture of GSU transformer nameplate	The GO should provide a picture of the GSU nameplate for future reference and any calculation	• N/A
Copy of GSU factory test report	If available, a physical or digital copy of the transformer factory test report, including the following items for reference and parameter verification: 1. MVA ratings 2. Winding resistances 3. No-load losses [W] and exciting current [%] 4. Load losses [W] and impedance [%] 5. Zero-sequence impedances	• GSU manufacturer

Plant Interconnection Transmission Line(s) or Distributed Sub-Transmission Line Equivalent(s)

Table A.6 provides the recommended data for steady-state modeling data for the GSU or GO-owned station transformer(s) that should be requested from GOs for MOD-032. This list is comprehensive but not exhaustive. The PC or TP may request other information necessary for modeling purposes.

Table A.6: Recommended Power Flow Modeling Data for Interconnection or Equivalent Plant Transmission Line MOD-032 Data Requests

Common Name	Detailed Description	Data Source
Plant Tie Line(s) Data		
R_l	Positive Sequence Line Resistance [pu on 100 MVA base]	• Calculated
X_l	Positive Sequence Line Reactance [pu on 100 MVA base]	• Calculated
B_l	Positive sequence line charging susceptance [pu on 100 MVA base]	• Calculated
MVA Ratings (normal and emergency)	The most limiting rating [MVA], both normal and emergency, of the phase conductor and any series equipment.	• Line design specifications • Substation design specifications
Line Length	Line length [miles] of the line. For equivalent lines, this should be the total amount of line represented in the equivalent.	• Calculated
Additional Data *This data is only required for overhead transmission lines. This information is generally not available or relevant to the sub-transmission collector circuits present in large renewable facilities.*		

Table A.6: Recommended Power Flow Modeling Data for Interconnection or Equivalent Plant Transmission Line MOD-032 Data Requests

Common Name	Detailed Description	Data Source
Line Configuration	Line configuration (i.e., X- and Y-coordinates [ft.] where center of line right-of-way is 0 in the horizontal (or X) direction and the ground is 0 in the vertical (or Y) direction) and spacing [in.] information for plant tie lines or equivalent plant sub-transmission liens (typically for distributed resources like wind or solar farms) This includes the following: - Average pole height - Average span sag - X- and Y-coordinates for all phase conductors and static conductors (f applicable) [ft.] - Phase conductor type (e.g., 1192 Bunting ACSR) - Number of phase conductors per bundle (e.g., 2) - Spacing between conductors in bundle [in.] - Separation angle of conductors in bundle [°] (e.g., 0° for perfectly horizontal, 90° for perfectly vertical) - Type(s) of static conductor (e.g., 3/8EHS) o Possible to have multiple types per line (e.g., Fiber Optic and 3/8EHS) - Length of line [mi.]	• Line design specifications • Line engineering drawings

Appendix B: Dynamics Modeling Data

This appendix provides information regarding data that could be requested for dynamics modeling purposes.

Synchronous Machines

Table B.1 provides the recommended data for dynamics modeling of synchronous generators that should be requested from GOs for MOD-032. This list is comprehensive but not exhaustive. The PC or TP may request other information necessary for modeling purposes. Most data in this section should be provided as verified through the MOD-026 or MOD-027 processes as applicable. If those verification activities have not been performed, the GO should provide the best available data (e.g., OEM data, commissioning testing, type testing reports).

Table B.1: Recommended Dynamics Modeling Data for Synchronous Machine MOD-032 Data Requests

MOD-032 Reference	Common Name	Detailed Description	Data Source
Overview *Under MOD-026 and MOD-027, each TP is required to provide a list of acceptable dynamic models to the GO upon request. Each GO should request this list of acceptable dynamic models when verifying models and when submitting models for MOD-032. Further, each MOD-032 designee that coordinates the creation of the interconnection-wide base cases is required to maintain a list of models that is required to be the same or more restrictive than the NERC List of Acceptable Models.* [23] *This list is enforced during the creation of the interconnection-wide models, and data should be supplied that aligns with this list. Since there are many dynamic models, some with a significant number of parameters, this table provides important considerations and guidance for submitting data for each type of dynamic model.*			
Generator	Generator Dynamic Model	The dynamic models for generators are standardized throughout software platforms. Refer to the *NERC List of Acceptable Models* for recommended models. If the generator parameters in per-unit are based on a different machine MVA base provided in the power flow model, the machine MVA base used for those per-unit values should be submitted.	• Manufacturer-provided data • Commissioning reports • Factory test reports

[23] https://www.nerc.com/pa/RAPA/ModelAssessment/Pages/default.aspx

Table B.1: Recommended Dynamics Modeling Data for Synchronous Machine MOD-032 Data Requests

MOD-032 Reference	Common Name	Detailed Description	Data Source
Excitation System	Excitation System Dynamic Model	In 2005, IEEE approved IEEE Std. 421.5-2005 *IEEE Recommended Practice for Excitation System Models for Power System Stability Studies*. In 2017, IEEE approved IEEE Std. 421.5-2016 as a major revision to the 2005 standard.[24] These models serve as the de facto standard for the vast majority of excitation systems in use today and should be made available in the software platforms. Refer to the *NERC List of Acceptable Models* for recommended models.	• MOD-026 or MOD-027 test reports • Manufacturer-provided data • Commissioning reports • Factory test reports • MOD-026 or MOD-027 test reports
Power System Stabilizer	Power System Stabilizer Model	Units that have a PSS installed and operational must be modeled accordingly. PSS models are standardized in IEEE Std. 421.5-2016. Digital PSSs should have a direct correlation (mapping) of controller values and model parameters.	
Excitation Limiters	Overexcitation and Underexcitation Limiter Dynamic Models	Excitation limiter (UEL and OEL) models should be provided if the UEL or OEL affects excitation controls and reactive power output within approximately 60 seconds following a disturbance. These models are defined in IEEE 421.5-2016 and should be implemented in all software applications. It should be ensured that the excitation limiter model is compatible with the excitation system model.	
Governor	Turbine-Governor Dynamic Model	There is no IEEE standard for modeling turbine-governor systems in power system stability studies. However, IEEE published a technical report[25] on *Dynamic Models for Turbine-Governors in Power System Studies*. This report also serves as the current industry best practice and guidance document for modeling turbine-governors and is generally followed by software vendors. Refer to the *NERC List of Acceptable Models* for recommended models. Data should be carefully per unitized on either the turbine rating (*trate*/*mwcap*) or machine base (MBASE) appropriately.	
Governor Load Controller	Turbine-Governor Load Control Model	Units that have plant-level or outer-loop controls that affect the response of the turbine-governor within approximately 60 seconds following a disturbance should be modeled accordingly. These functions are incorporated into some turbine-governor models or can be added with an additional model.	

[24] https://standards.ieee.org/findstds/standard/421.5-2016.html

[25] http://sites.ieee.org/fw-pes/files/2013/01/PES_TR1.pdf

Table B.1: Recommended Dynamics Modeling Data for Synchronous Machine MOD-032 Data Requests

MOD-032 Reference	Common Name	Detailed Description	Data Source
Current Compensati on	Compensator Dynamic Model	Depending on software implementation, generator reactive current compensation is accomplished either in a separate model or included in the generator model. Cross current compensation between multiple units requires a separate model. Refer to the *NERC List of Acceptable Models* for recommended models.	
Other Dynamic Models *Upon request by the TP or PC, to support system stability and reliability studies*			
Protection	Generator Protection Models	Some stability studies, particularly specialized studies, may require more detailed information regarding generator protection settings. Examples of protection models include V/Hz, reverse power, out of step, loss of excitation, voltage ride-through (low voltage and high voltage), frequency ride-through (low frequency and high frequency), and other forms of protection schemes for the generator.	• Manufacturer-provided data • Verification test reports • PRC-019 study reports
Other Information *TPs and PCs should track which dynamic models have been verified by the GO as per MOD-026-1 and MOD-027-1. They may ask information related to the last date of verification testing. The goal is to minimize duplication of information and tracking of latest information in the interconnection-wide cases.*			
Verification	Verification Flag and Date	The TP or PC may request information regarding the last date of model verification as per MOD-026-1 and MOD-027-1. If this testing has not been performed, provide the next testing date (if available), and there should be an option to specify this accordingly.	• Verification testing schedule

Plant-Level Equivalent Machines

Table B.2 provides the recommended data for dynamics modeling of plant-level equivalent generators that should be requested from GOs for MOD-032. It is very common for plant-level equivalent generator models to use one or several machine models to represent multiple, distributed generator resources, such as wind or solar farms. This list is comprehensive but not exhaustive. Other information may be requested by the PC or TP necessary for modeling purposes.

Most data in this section should be provided as verified through the MOD-026 or MOD-027 processes (as applicable). If those verification activities have not been performed, the GO should provide the best available data (e.g., OEM data, commissioning testing, type testing reports).

Table B. 2: Recommended Dynamics Modeling Data for Plant-Level Equivalent Machine MOD-032 Data Requests

MOD-032 Reference	Common Name	Detailed Description	Data Source
Overview *Each TP is required under MOD-026-1 and MOD-027-1 to provide a list of acceptable dynamic models to the GO upon request. Each GO should request this list of acceptable dynamic models when verifying models, and when submitting models for MOD-032. Further, each MOD-032 Designee that coordinates the creation of the interconnection-wide base cases is required to maintain a list of models that is required to be the same or more restrictive than the NERC List of Acceptable Models.*[26] *This list is enforced during the creation of the interconnection-wide models, and data should be supplied that aligns with this list. Since there are many dynamic models, some with a significant number of parameters, this table provides important considerations and guidance for submitting data for each type of dynamic model.*			
Generator/ Convertor Model	Converter Dynamic Model	Inverter-based resources have a generator/converter model that models the dynamic interaction between the physical generator and the electrical converter. The inverter manufacturer provides most of the parameters in this model.	• Manufacturer-provided data • Commissioning reports • Factory test reports • MOD-026 or MOD-027-1 test reports • Inverter-level settings • Plant-level control settings
Electrical Control Model	Electrical Control Dynamic Model	Inverter-based resources have an electrical control model. These control-based parameters represent the aggregate dynamic response of inverters within the plant. This dynamic model includes the active and reactive power controls, large disturbance behavior characteristics, control flags, and other parameters.	
Power Plant Controller Model	Plant-Level Controller Dynamic Model	Many inverter-based resources are equipped with a plant-level controller that interacts with the individual inverter controls. This dynamic model represents the control interactions between the plant-level control and the individual inverter controls. It is imperative that this system (and the associated model) are coordinated with the electrical control model. The parameters in this model often come from the plant-level controller itself.	

[26] https://www.nerc.com/pa/RAPA/ModelAssessment/Pages/default.aspx

Table B. 2: Recommended Dynamics Modeling Data for Plant-Level Equivalent Machine MOD-032 Data Requests

MOD-032 Reference	Common Name	Detailed Description	Data Source
Mechanical Model	Wind Turbine Mechanical Dynamic Model OR Solar PV Panel Output Curve	Wind resources directly connected (Type 1 and Type 2) or partially connected (Type 3) to the synchronous grid may include a turbine control model that represents the aggregate physical/mechanical response of the plant. This includes the wind turbine inertia constant and other mechanical turbine parameters. Solar PV resources may include a model that represents the linearized, aggregate model of the solar PV panel output curve (otherwise known as the PV panel I-P characteristic curve).	
Pitch Controls Model	Wind Turbine Pitch Controls Dynamic Model OR Solar PV Irradiance Model	Wind resources that are partially connected to the synchronous grid (i.e., Type 3) are equipped with blade pitch controls with modeling requirements of aggregate regulator controls, time constants, and angle limits. Solar PV resources may include an irradiance profile that may need to be modeled.	
Aerodynamic Control Model	Wind Turbine Aerodynamic Control Model	Wind resources that are directly connected (Type 1 and Type 2) or partially connected (Type 3) to the synchronous grid may have controls that help regulate the pitch controls that may need to be modeled.	
Torque Control Model	Wind Turbine Torque Controller Model	Wind resources that are directly connected to the synchronous grid (i.e., Type 3) may have turbine torque controllers that may need to be modeled.	

Other Dynamic Models *Upon request by the TP or PC, to support system stability and reliability studies*			
Protection	Generator Protection Models	Some stability studies, particularly specialized studies, may require more detailed information regarding generator protection settings. Examples of protection models include V/Hz, reverse power, out of step, loss of excitation, voltage ride-through (low voltage and high voltage), frequency ride-through (low frequency and high frequency), and other forms of protection schemes for the generator.	• Manufacturer-provided data • MOD-026 or MOD-027 test reports • PRC-019 study reports
Other Information *TPs and PCs should track which dynamic models have been verified by the GO as per MOD-026-1 and MOD-027-1. They may ask information related to the last date of verification testing. The goal is to minimize duplication of information and tracking of latest information in the interconnection-wide cases.*			
Verification	Verification Flag and Date	The TP or PC may request information regarding the last date of model verification as per MOD-026-1 and MOD-027-1. If this testing has not been performed, provide the next testing date if available, and there should be an option to specify this accordingly.	• Verification testing schedule

Appendix C: Short Circuit Modeling Data

This appendix provides information regarding data that could be requested for short-circuit modeling purposes.

Synchronous Machines

Table C.1 provides the recommended data for synchronous machine short circuit modeling that should be requested from GOs for MOD-032. This list is comprehensive but not exhaustive. Other information may be requested by the PC or TP necessary for modeling purposes.

Table C.1: Recommended Short Circuit Modeling Data for Synchronous Machine MOD-032 Data Requests

Common Name	Detailed Description	Data Source
Bus Voltage Data		
PU Base Voltage	Generator terminal base voltage [kV]	• Generator nameplate
Generator Data		
MVA Rating (MVA Base)	Generator MVA Rating (Generator MVA Base) [MVA][27]	• Generator nameplate
Generator Rated Voltage	Rated Stator Voltage [kV]	• Generator nameplate
X_{dsat}[28]	Saturated synchronous reactance, direct axis [pu]	• Saturation curve in generator test report • OEM calculations
X'_{dsat}	Saturated transient synchronous reactance, direct axis [pu]	• Test report • Calculations from manufacturer
X''_{dsat}	Saturated subtransient synchronous reactance, direct axis [pu]	• Test report • Calculations from manufacturer

[27] Should be used as per unit base for impedance values.

[28] Regarding saturated values in general, it is understood that lower values of impedance may be desirable for conservative fault current calculations. Some of these three values are often included in manufacturer/test data. However, they are not all always measured, calculated, or included in test reports. If not available, they cannot be reliably derived by the GO, who should not be held accountable for accuracy of their estimation. All values are defined by tests as detailed in IEEE Std. 115-2009.

Table C.1: Recommended Short Circuit Modeling Data for Synchronous Machine MOD-032 Data Requests

Common Name	Detailed Description	Data Source
X_2	Saturated Negative Sequence Reactance [pu]	• Test report • Calculations from manufacturer
X_0	Zero Sequence Reactance [pu]	• Test report • Calculations from manufacturer
R_1	Positive sequence stator resistance [pu]	• Test report • Calculations from manufacturer
R_2	Negative sequence stator resistance [pu]	• Test report • Calculations from manufacturer
R_0	Zero sequence stator resistance [pu]	• Test report • Calculations from manufacturer
R_{g0}	Zero Sequence Grounding Resistance [pu] (should include devices such as grounding resistors for transformers)	• Calculated from neutral grounding equipment information
X_{g0}	Zero Sequence Grounding Reactance [pu] (should include devices such as grounding resistors for transformers)	• Calculated from neutral grounding equipment information

Equivalent Type I and Type II Wind Machines

Table C.2 provides the recommended short-circuit data for equivalent, directly connected wind machines (Type I) or induction wind machines with externally controlled resistor (Type II) that should be requested from GOs for MOD-032. It is very common that these generator models are not machine-level representations where each turbine or inverter is individually modeled. Instead, one or several equivalent machine(s) is/are used to represent the aggregate output and dynamic response of the plant. This list is comprehensive but not exhaustive. The PC or TP may request other information necessary for modeling purposes.

Table C.2: Recommended Short Circuit Modeling Data for Inverter-Based Machine MOD-032 Data Requests		
Common Name	**Detailed Description**	**Data Source**
Bus Voltage Data		
PU Base Voltage	Generator terminal base voltage [kV]	- Generator nameplate
Generator Data		
MVA Rating (MVA Base) [MVA]	Aggregate MVA rating for the plant Typically, this is the MVA rating of a single generator or inverter times the number of generators or inverters represented by the equivalent. [MVA]	- Generator nameplate
Generator Rated Voltage	Rated stator voltage [kV]	- Generator nameplate
X_{dsat}[29]	Saturated synchronous reactance, direct axis [pu]	- Saturation curve in generator test report - OEM calculations
X'_{dsat}	Saturated transient synchronous reactance, direct axis [pu]	- Test report - OEM calculations
X''_{dsat}	Saturated subtransient synchronous reactance, direct axis [pu]	- Test report - OEM calculations
X_2	Saturated negative sequence reactance [pu]	- Test report - OEM calculations
X_0	Zero sequence reactance [pu]	- Test report - OEM calculations

[29] Regarding saturated values in general, it is understood that lower values of impedance may be desirable for conservative fault current calculations. Some of these three values are often included in manufacturer/test data. However, they are not all always measured, calculated, or included in test reports. If not available, they cannot be reliably derived by the GO, who should not be held accountable for accuracy of their estimation. All values are defined by tests as detailed in IEEE Std. 115-2009.

Table C.2: Recommended Short Circuit Modeling Data for Inverter-Based Machine MOD-032 Data Requests		
Common Name	**Detailed Description**	**Data Source**
R_1	Positive sequence resistance [pu]	• Test report • OEM calculations
R_2	Negative sequence resistance [pu]	• Test report • OEM calculations
R_0	Zero sequence resistance [pu]	• Test report • OEM calculations

Other Inverter-Based Resources

The IEEE PSRC C24 Working Group report published in June 2020 specifies the recommended short-circuit data for inverter-based resources.[30] This report outlines a voltage-dependent current injection table format that is now adopted by the major commercial simulation tool platforms. TPs and PCs should establish modeling requirements that align with this work, particularly to capture the current injection for different fault types and different fault periods. GOs should provide information in the specified data formats per the requirements established.

Generator Step-Up or Station Transformers

Table C.3 provides the recommended data for GSU or GO-owned station transformer short-circuit modeling that should be requested from GOs for MOD-032. This list is comprehensive but not exhaustive. The PC or TP may request other information necessary for modeling purposes.

Table C.3: Recommended Short Circuit Modeling Data for Transformer MOD-032 Data Requests		
Common Name	**Detailed Description**	**Data Source**
Two-Winding Generator Step Up Transformer Data		
R_{01}	Positive Sequence Resistance primary to secondary [pu]	• Transformer test report
X_{01}	Positive Sequence Reactance primary to secondary [pu]	• Transformer test report
R_{png1}	Positive Sequence Resistance primary neutral to ground [pu]	• Transformer test report

[30] https://www.pes-psrc.org/kb/published/reports/C24_WG_Report_Jun_2020_Final.pdf

Table C.3: Recommended Short Circuit Modeling Data for Transformer MOD-032 Data Requests		
Common Name	**Detailed Description**	**Data Source**
X_{png1}	Positive Sequence Reactance primary neutral to ground [pu]	- Transformer test report
R_{sng1}	Positive Sequence Resistance secondary neutral to ground [pu]	- Transformer test report
X_{sng1}	Positive Sequence Reactance secondary neutral to ground [pu]	- Transformer test report
R_{ps0}	Zero Sequence Resistance primary to secondary [pu]	- Transformer test report
X_{ps0}	Zero Sequence Reactance primary to secondary [pu]	- Transformer test report
R_{png0}	Zero Sequence Resistance primary neutral to ground [pu]	- Neutral grounding equipment information
X_{png0}	Zero Sequence Reactance primary neutral to ground [pu]	- Neutral grounding equipment information
R_{sng0}	Zero Sequence Resistance secondary neutral to ground [pu]	- Neutral grounding equipment information
X_{sng0}	Zero Sequence Reactance secondary neutral to ground [pu]	- Neutral grounding equipment information
Three-Winding Generator Step Up Transformer Data *For each three-winding transformer, the following data should be provided in addition to the parameters for two-winding transformers.*		
GSU MVA Rating $(\text{Base})_{P\text{-}T}$	GSU MVA Rating (Base) Primary-Tertiary (typically self-cooled) [MVA]	- Transformer nameplate or test report
GSU MVA Rating $(\text{Base})_{T\text{-}S}$	GSU MVA Rating (Base) Tertiary-Secondary (typically self-cooled) [MVA]	- Transformer nameplate or test report
Tertiary Rated Voltage	Operating Tap Voltage (or measured voltage from GSU test report)	- Transformer nameplate or test report

Table C.3: Recommended Short Circuit Modeling Data for Transformer MOD-032 Data Requests

Common Name	Detailed Description	Data Source
$Config_{tertiary}$	Tertiary winding configuration (e.g., delta, wye, wye-grounded)	• Transformer nameplate or test report
R_{pt1}	Positive Sequence Resistance primary to tertiary [pu]	• Transformer test report
X_{pt1}	Positive Sequence Reactance primary to tertiary [pu]	• Transformer test report
R_{ts1}	Positive Sequence Resistance tertiary to secondary [pu]	• Transformer test report
X_{ts1}	Positive Sequence Reactance tertiary to secondary [pu]	• Transformer test report
R_{tng1}	Positive Sequence Resistance tertiary neutral to ground [pu]	• Transformer test report
X_{tng1}	Positive Sequence Reactance tertiary neutral to ground [pu]	• Transformer test report
R_{pt0}	Positive Sequence Resistance primary to tertiary [pu]	• Transformer test report
X_{pt0}	Positive Sequence Reactance primary to tertiary [pu]	• Transformer test report
R_{ts0}	Positive Sequence Resistance tertiary to secondary [pu]	• Transformer test report
X_{ts0}	Positive Sequence Reactance tertiary to secondary [pu]	• Transformer test report
R_{tng0}	Zero Sequence Resistance tertiary neutral to ground [pu]	• Transformer test report
X_{tng0}	Zero Sequence Reactance tertiary neutral to ground [pu]	• Transformer test report

Plant Interconnection Transmission Line(s) or Collector Circuit Equivalent Line(s)

Table C.4 provides the recommended data for GO-owned transmission or collector circuit equivalent line short-circuit modeling that should be requested from GOs for MOD-032. This list is comprehensive but not exhaustive. The PC or TP may request other information necessary for modeling purposes.

Table C.4: Recommended Short Circuit Modeling Data for Lines MOD-032- Data Requests

Common Name	Detailed Description	Data Source
R_{l0}	Zero Sequence Line Resistance [pu on 100 MVA base]	• Calculated
X_{l0}	Zero Sequence Line Reactance [pu on 100 MVA base]	• Calculated
B_{l0}	Zero Sequence Line Shunt Admittance [pu on 100 MVA base]	• Calculated
Additional Data		
MOV Protection Status	If the line is protected by a metal-oxide varistor (MOV), the TP and PC should be informed so that it can be included in models. There are four general types of MOV status: 1. Not MOV protected 2. MOV protection enabled 3. MOV protection disabled (i.e., present but not online) 4. MOV spark-gap protection enabled	• Line design specifications
MOV Rated Current	Rated current [kA] of the MOV protecting a branch.	• MOV design specification/OEM data

Appendix D: Geomagnetic Disturbance Modeling Data

Table D.1 provides the recommended data for GMD modeling that should be requested from GOs. GOs should be prepared to supply modeling data for GMD assessments per the latest version of NERC TPL-007. Applicable facilities include power transformer(s) with a high side, wye-grounded winding with terminal voltage greater than 200 kV although the TP and PC may identify additional facilities needed for modeling and study purposes.

It is assumed that the best source of information for GMD modeling is someone specializing in transformers who is aware of the data records. The secondary source would be substation or plant design group or equivalent. Some entities maintain a central data source that includes transformer data. Test reports refer to the standard factory test report provided as part of the delivery of a transformer. For blocking devices, the answer will almost always be “no” since the normal delta connection for GSUs blocks geomagnetically-induced current (GIC). If it is necessary to seek records from the manufacturer or subsequent company with the manufacturer assets, the nameplate will provide the serial number and other information needed to start the inquiry.

Table D.1: Recommended GMD Modeling Data for TPL-007-1 Data Requests

Common Name	Detailed Description	Data Source
General Data		
GPS Coordinates	GPS coordinates (i.e., latitude and longitude) for the power plant substation [degrees]	• Facility management
Two-Winding Transformer Data		
Core Construction	If the unit is a single-phase bank, a three-phase shell-type, or a three-phase core-type (with 3, 5, or 7 legs), this info may be needed to determine certain GIC calculations depending on other transformer construction factors. If this information is unknown, report as "unknown." Options: Unknown, Single-Phase, Shell-Type, Core-Type (3 legged), Core-Type (5 legged), Core-Type (7 legged)	• Substation design • OEM data
H-Winding has GIC Blocking Device?	Yes or No If the unit has a GIC blocking device installed, it will affect GIC currents.	• Substation design • By inspection
X-Winding has GIC Blocking Device?	Yes or No If the unit has a GIC blocking device installed, it will affect GIC currents.	

Table D.1: Recommended GMD Modeling Data for TPL-007-1 Data Requests

Common Name	Detailed Description	Data Source
H-Winding DC Resistance	Used to create a dc model of the transformer for GIC studies (typically from GSU commissioning test report) [ohms]	• Transformer factory test report
X-Winding DC Resistance	Used to create a dc model of the transformer for GIC studies (typically from GSU commissioning test report) [ohms]	• Transformer factory test report
DC Winding Resistance Temperature	Used to convert dc winding resistances to the desired temperature.	• Transformer factory test report
Core Winding Material	Generally, copper or aluminum This information helps better convert the dc resistances to the desired temperature. This information is not always available, if unknown material, assume copper.	• Transformer factory test report
Vector Group	The vector group indicates the phase difference between the primary and secondary sides caused by the particular configuration of the transformer windings connection. This information is used to determine how the transformer is grounded and how fault currents should be calculated. The manufacturer typically indicates this information on the nameplate of the transformer.	• Substation design • Transformer nameplate
Is Autotransformer?	Yes or No Needed to determine how short circuit and GIC currents should be calculated.	• Substation design • Transformer nameplate
DC Resistance Measurement Type	Refers to how the dc winding resistance information is presented in the test report Generally, winding resistances are measured in the following one of two ways: 1. Per-phase 2. All phases in series This information is important because the dc transformer model needed for GIC analysis requires dc winding resistances to be in ohms/phase.	• Transformer factory test report

Table D.1: Recommended GMD Modeling Data for TPL-007-1 Data Requests

Common Name	Detailed Description	Data Source
Three-Winding Transformer Data *For each three-winding transformer, the following data should be provided in addition to the parameters for two-winding transformers.*		
Y-Winding has GIC Blocking Device?	Yes or No If the unit has a GIC blocking device installed, it will affect GIC currents.	• Substation design • By inspection
Y-Winding DC Resistance	Used to create a dc model of the transformer for GIC studies (typically from GSU commissioning test report) [ohms]	• Transformer factory test report
Which Windings are Auto?	H-X, X-Y, or H-Y Needed to determine how short circuit and GIC currents should be calculated.	• Substation design • Transformer nameplate

Appendix E: Details of Generator Step Up Transformer Data

This appendix describes data entry for GSU transformers to provide clear guidance on how the model data is requested and used. Alberta Electric System Operator has produced a useful transformer modeling guide that also serves as a useful reference.[31]

Power transformers can have different configurations and configurable taps that can lead to different data requirements for positive sequence simulations. These configurations are as follows:

- Three-phase, two-winding transformer
- Three single-phase, two-winding transformers
- Three-phase, three-winding transformer
- Three single-phase, three-winding transformers

Each winding could have one of the following:

- No load tap changer
- Under load tap changer
- No tap changer

The software tools used by the TP and PC use the same model for GSUs as used for other transformers on the BPS. The transformer model can represent a number of different transformer types, such as GSUs, autotransformers, voltage regulating transformers, phase shifters, and load station transformers. As such, software vendors have made the transformer model flexible such that the configurations and tap options can be modeled. In simplest terms, powerflow implementation of a two- and three-winding transformers are shown in **Figure E.1** and **Figure E.2**.

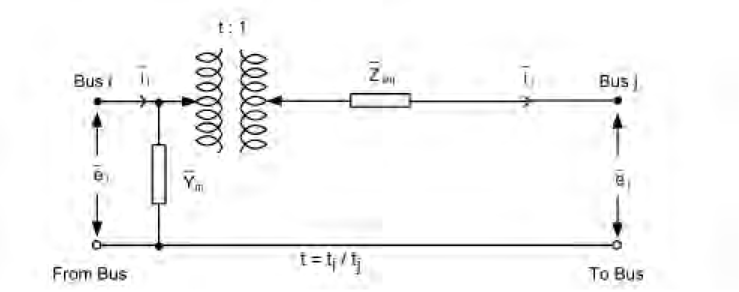


Figure E.1: Two-Winding Transformer Representation

[31] https://www.aeso.ca/assets/linkfiles/4040.002-Rev02-Transformer-Modelling-Guide.pdf

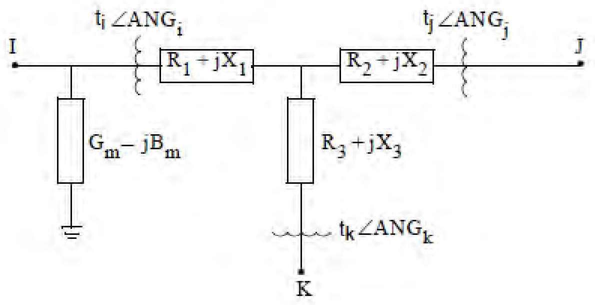
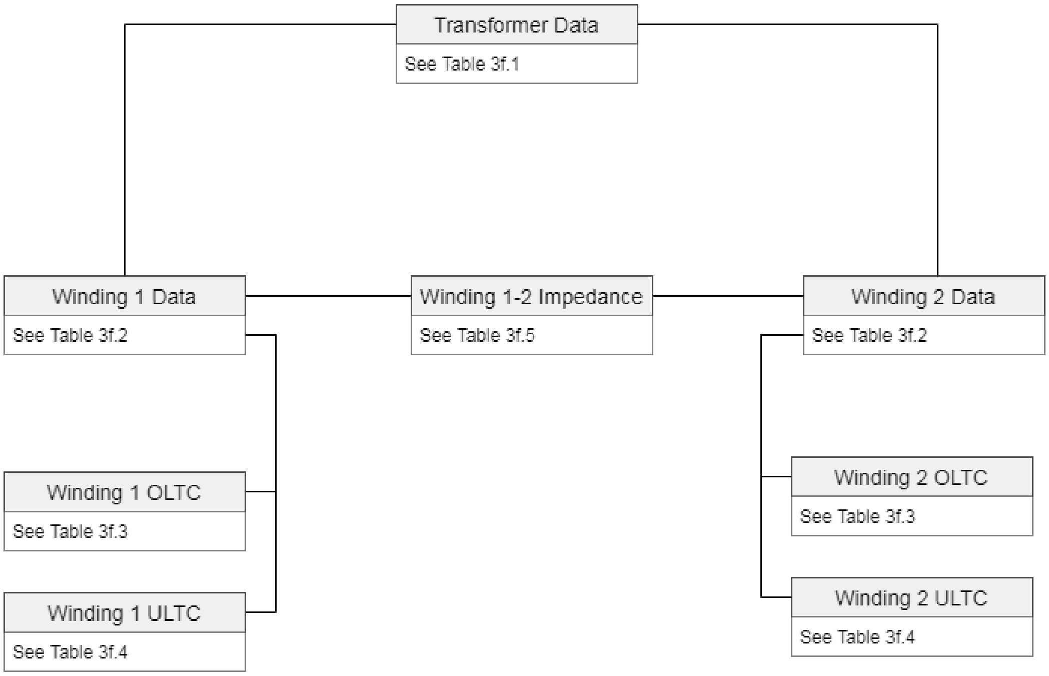


Figure E.2: Three-Winding Transformer Representation

From the simplified diagram above, the modeler must get two parts of the model correct: tap ratio(s) and impedance(s). Modeling these incorrectly has a significant effect on voltage and reactive power flow.

Transformer data is split into the structure shown in Figure E.3 using a number of tables to allow for flexibility. This structure states that transformers have windings (under-load tap changer (ULTC) or on-load tap changer (OLTC)) and have impedances between windings. Each table is described below, and this information can be mapped to the data explained in Appendix A. Examples of gathering this data following the tables to help understand how to obtain this data. Note that not all nameplates are identical in the way information is presented here, but these examples should provide useful reference information.

Most transformer data is available from the transformer nameplate, with supplemental information available in the transformer test report. Additional data may require reviewing engineering drawings and physical settings and positions.


Transformer Data
See Table 3f.1

Winding 1 Data
See Table 3f.2

Winding 1-2 Impedance
See Table 3f.5

Winding 2 Data
See Table 3f.2

Winding 1 OLTC
See Table 3f.3

Winding 1 ULTC
See Table 3f.4

Winding 2 OLTC
See Table 3f.3

Winding 2 ULTC
See Table 3f.4

Figure E.3: Breakdown of Transformer Data

The following data is specified:

- **General Transformer Data:** General data used to account for each unique transformer in the model
- **Winding Data:** Winding data describes the windings and provides the rating and nominal voltage value
- **Winding OLTC Data:** GSUs typically have off-load tap positions on at least one winding. This must be captured in the loadflow by correctly entering the tap position in the winding ratio field for the correct winding by using the correct units as per the winding I/O code. The GO should communicate all values in kV and leave the conversion of the proper I/O code to the TP as this will eliminate any possibility of errors.
- **Winding ULTC Data:** Typically GSUs did not have ULTC and they only had OLTCs; however, this feature does exist on many wind and solar installations that control the HV bus with inverter resources. The ULTC is used to control the LV bus (e.g., 34.5 kV). One must be careful when modeling this as this may cause issues with voltage control in the load flow as many software tools do not have steady state droop feature available. This must be captured in the load flow by correctly entering the tap position in the winding ratio field for the correct winding by using the correct units as per the winding I/O code. The GO should communicate all values in kV and leave the conversion to the proper I/O code to the TP as this will eliminate any possibility of errors.
- **Impedance Pair Data:** GSU transformers have measured impedances between pairs of windings that is usually the average of the three-phase readings as each phase is slightly different. For a two-winding transformer, there is one positive sequence impedance; for a three-winding, there are three values. The impedance is often measured at the lowest MVA rating of the windings (self-cooled) and may only be measured for one set of taps. For transformers with multiple taps, the impedance changes as a result of changing the turns ratio (adding more or less turns and material); however, this is not measured at all taps. This is usually measured at nominal tap and stamped on the nameplate. Measurements at minimum and maximum tap may also be presented in the transformer test report.

TPs should understand the effect of modeling the changes in impedance for off-nominal windings before asking the GO to retrieve these.

Example Transformer Data Entry

Most transformer ratings are 60/80/100% of the full-cooled rating with the impedances listed on the self-cooled rating. Application of engineering principals should be able to tell one the effect of modeling the different transformer impedances in detail with respect to reactive power loss and voltage drop. First, one can simplify the equations by assuming that the resistance value is 0 and the generator winding is 1 pu voltage. Given that both the reactive power loss and voltage drop are highest at full loading, the LV winding is set to 1 pu loading or (1/0.6 pu). Therefore, the losses on nominal tap can be estimated by the following equation:

$$Qloss_{tap\,n} = I^2 * X_{tap\,n} \ * MVA_{base}$$

The losses on Tap 1 can be estimated by the following equation:

$$Qloss_{tap\,1} = I^2 * X_{tap\,1} * MVA_{base}$$

Subtracting one from the other will give the estimate of the difference in losses, shown in the following equation:

$$Qloss_{diff} = I^2 * (X_{tap\,n} - X_{tap\,1}) * MVA_{base}$$
$$Qloss_{diff} = (1/0.6)^2 * (X_{tap\,n} - X_{tap\,1}) * MVA_{base}$$
$$Qloss_{diff} = 2.77 * (X_{tap\,n} - X_{tap\,1}) * MVA_{base}$$

Here are some impedance values measured at the self-cooled rating for Taps 1, 9 (nominal), and Tap 17 for a 66/88/110 MVA transformer (see Table E.1 and Figure E.4). The difference between Tap 9 (nominal) and Tap 17 is 0.0015 pu, and the difference between Tap 9 (nominal) and Tap 1 is 0.0044 pu.

Table E.1: Example Impedance Values

Impedance	Tap 1	Tap 9 (Nominal)	Tap 17
%IX	8.04	7.60	7.45

If the worst case is used, the equation above shows the difference in Q_{loss} is 0.8 Mvar. When the transformer is modeled in detail and a simulation is performed, the simulation software calculates a 0.84 Mvar difference in losses. Note that powerflow software that uses numerical techniques like Newton-Raphson have user-settable mismatch tolerances. Typical values are 1 MW and 1 Mvar. It is expected that the difference in impedance from nominal winding is similar to the numbers above (e.g., 0.0015 to 0.0044 pu). Therefore, reactive power losses can range rather substantially as shown in Table E.2.

Table E.2: Example of Transformer Loss Data

Self-Cooled Rating	Qloss diff (X diff = 0.0044pu)	Qloss diff (X diff = 0.0015pu)
100	1.2188	0.4155
300	3.6564	1.2465
500	6.094	2.0775
700	8.5316	2.9085
900	10.9692	3.7395
1100	13.4068	4.5705

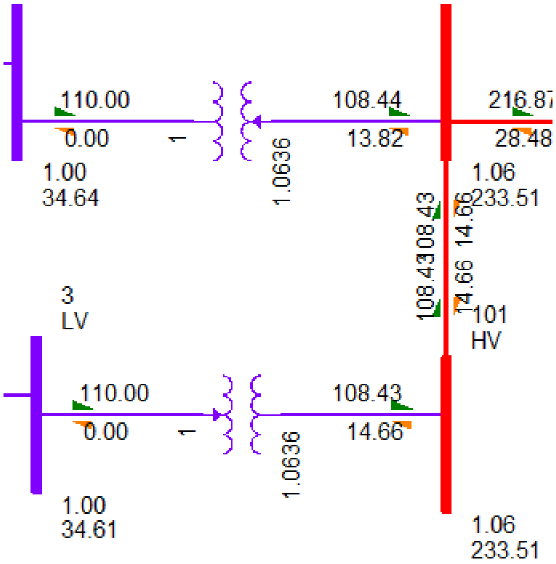


Figure E.4: Transformer Model Representation

All voltages should be in line-to-line unless otherwise stated. When I/O codes are circled, this does not mean use that code in the example; rather, pay close attention to the code and select the correct code that matches the units given or convert the data as necessary. The following tables provide a description of the various data fields that need to be provided for GSU data and a mapping of how that data relates to the modeling parameters and where to gather this data from drawings, physical equipment, etc.

GSU Transformer Data

Table E.3 describes the data that should be requested related to GSU transformer data.

Table E.3: GSU Transformer Data

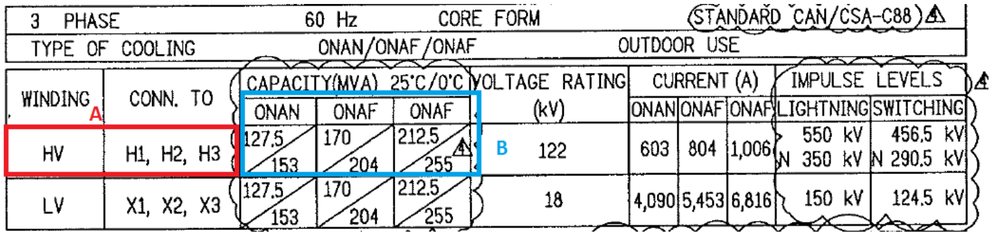
Data	Description	Data Source	Model Parameter
3f.1 Generator Step Up Transformer Data *Provide Same Data as that Required for Transformer under Item 6*			
GSU transformer name	Name given by TOP or GOP to GSU	TOP of GO One-lines	GSU Name
Three phase or three single phase transformer	It is important to establish the whether or not the transformer is three phase or three single phase as the MVA ratings (see below) and the MVA bases are per transformer. Simulation software requires three phase values of MVA. This must be effectively communicated so the TP can appropriately enter the values in software. See winding and winding pair impedance tables.	One-line diagram and transformer nameplate	Not used explicitly in model but useful information for TP/PC to have to confirm model data
One-line diagram	The one-line diagram should clearly show the bus configurations and which buses the transformer windings are connected to	One-line diagram	Useful for GSU mapping to correct bus locations in model

GSU Transformer Winding Data

Table E.4 describes the data that should be requested related to GSU transformer winding data.

Table E.4: GSU Transformer Winding Data

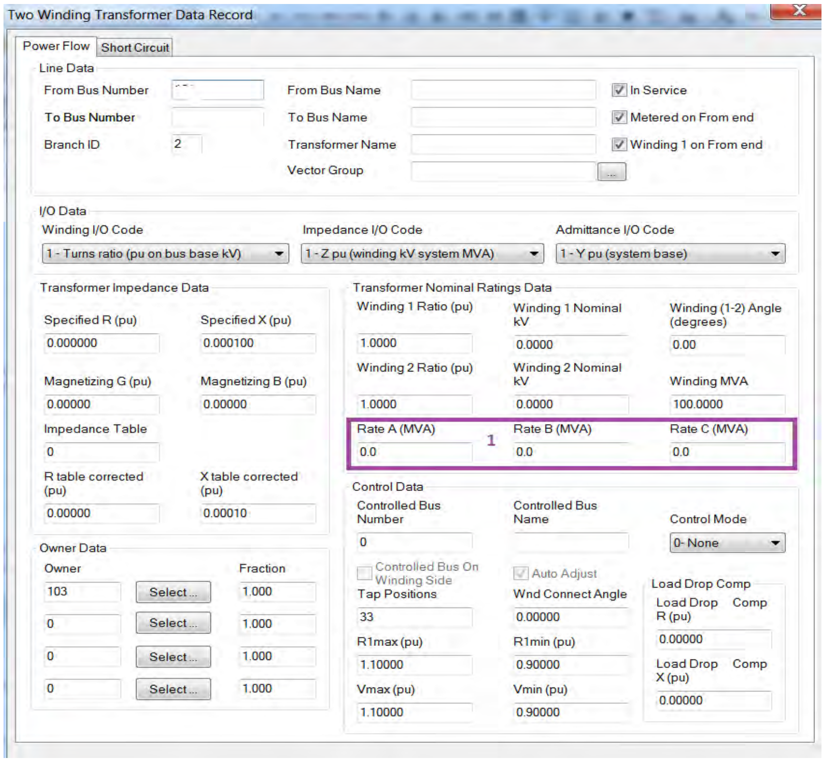
Data	Description	Data Source	Model Parameter
3f.2 Generator Step Up Transformer Winding Data *Provide same data as that required for transformer under Item 6.* *This table is to be duplicated for each winding.*			
Winding Name (H,X,Y,T)	The winding name to provide a reference for all data below (i.e., which winding is all of the data below referring to?) Each transformer winding is designated with an identification.	GSU Nameplate See “A” in **Figure E.5**	Used to select winding (winding 1 or 2). TP uses for mapping windings.
Winding Nominal Voltage	The winding voltage to help provide a reference for all data below (i.e., which winding is all of the data below referring to?)	GSU Nameplate See “A” in **Figure E.5**	Used to select winding (winding 1 or 2) TP uses for mapping windings.
OLTC Present	Does the winding have off load tap changer windings? If yes, populate OLTC table.	GSU Nameplate	See OLTC Table
ULTC Present	Does the winding have under load tap changer windings? If yes, populate the ULTC table.	GSU Nameplate	See ULTC Table
MVA Rating	Highest MVA rating for GSU continuous operation Note that some transformers specify ratings at different ambient temperatures. Check with the TP/PC if questions regarding which temperature. If three single-phase transformers are being represented, the MVA value should be multiplied by three to reflect the three-phase MVA base.	GSU Nameplate and engineering diagrams for any limiting series components See “B” in **Figure E.5**	See “1” in **Figure E.6**.
Emergency Ratings	Limited-time emergency ratings (e.g., two-hour rating). More common in autotransformers and load station transformers where the loading is not fixed. For GSUs, the continuous loading is determined by the generator output and emergency ratings may not provide any value (and often may be the same as the continuous nameplate rating).	Engineering study	See “1” in **Figure E.6**



3 PHASE	60 Hz	CORE FORM	(STANDARD CAN/CSA-C88) △
TYPE OF COOLING	ONAN/ONAF/ONAF		OUTDOOR USE

WINDING	CONN. TO	CAPACITY(MVA) 25°C/0°C			VOLTAGE RATING (kV)	CURRENT (A)			IMPULSE LEVELS △	
		ONAN	ONAF	ONAF		ONAN	ONAF	ONAF	LIGHTNING	SWITCHING
HV	H1, H2, H3	127.5/153	170/204	212.5/255 △	122	603	804	1,006	550 kV N 350 kV	456.5 kV N 290.5 kV
LV	X1, X2, X3	127.5/153	170/204	212.5/255	18	4,090	5,453	6,816	150 kV	124.5 kV

Figure E.5: GSU Transformer Winding Data from Specification Sheet



Two Winding Transformer Data Record

Power Flow | Short Circuit

Line Data

From Bus Number:

From Bus Name:

☑ In Service

To Bus Number:

To Bus Name:

☑ Metered on From end

Branch ID: 2

Transformer Name:

☑ Winding 1 on From end

Vector Group: ...

I/O Data

Winding I/O Code: 1 - Turns ratio (pu on bus base kV)

Impedance I/O Code: 1 - Z pu (winding kV system MVA)

Admittance I/O Code: 1 - Y pu (system base)

Transformer Impedance Data

Specified R (pu): 0.000000

Specified X (pu): 0.000100

Magnetizing G (pu): 0.00000

Magnetizing B (pu): 0.00000

Impedance Table: 0

R table corrected (pu): 0.00000

X table corrected (pu): 0.00010

Transformer Nominal Ratings Data

Winding 1 Ratio (pu): 1.0000

Winding 1 Nominal kV: 0.0000

Winding (1-2) Angle (degrees): 0.00

Winding 2 Ratio (pu): 1.0000

Winding 2 Nominal kV: 0.0000

Winding MVA: 100.0000

Rate A (MVA): 0.0

Rate B (MVA): 0.0

Rate C (MVA): 0.0

Control Data

Controlled Bus Number: 0

Controlled Bus Name:

Control Mode: 0- None

□ Controlled Bus On Winding Side

☑ Auto Adjust

Tap Positions: 33

Wnd Connect Angle: 0.00000

R1max (pu): 1.10000

R1min (pu): 0.90000

Vmax (pu): 1.10000

Vmin (pu): 0.90000

Load Drop Comp

Load Drop Comp R (pu): 0.00000

Load Drop Comp X (pu): 0.00000

Owner Data

Owner		Fraction
103	Select ...	1.000
0	Select ...	1.000
0	Select ...	1.000
0	Select ...	1.000

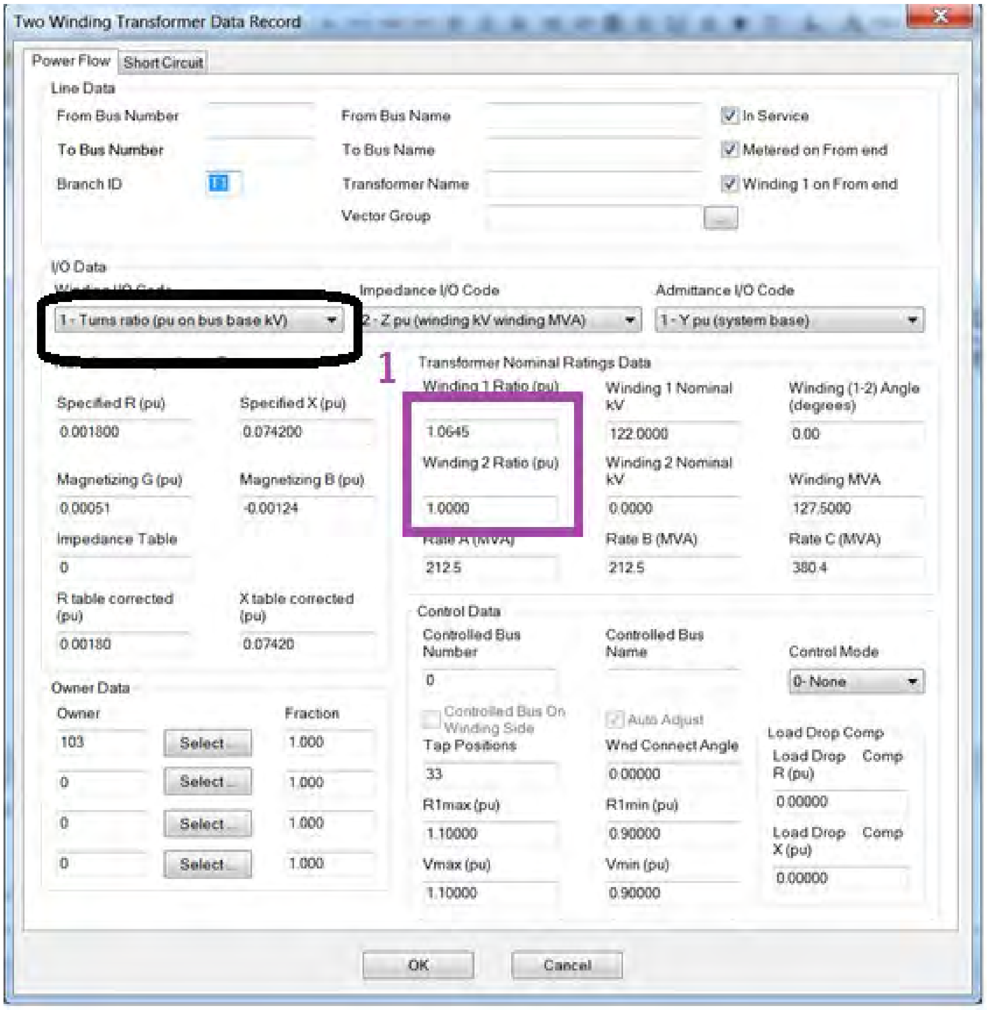
Figure E.6: GSU Ratings in Powerflow Data

GSU Transformer OLTC Data

Table E.5 describes the data that should be requested related to GSU OLTC data.

Table E.5: GSU Transformer OLTC Data

Data	Description	Location of data.	Model Parameter
3f.3 Generator Step Up Transformer OLTC data *Provide same data as that required for transformer under Item 6.* *This table is to be duplicated for each winding that has OLTC.*			
Winding Name (H,X,Y,T)	The winding name to provide a reference for all data below (i.e., which winding is all of the data below referring to?)	This is obtained from the nameplate; all transformer windings are designated with identification. See "A" in Figure E.8.	This data is used to select the correct winding, (i.e. winding 1 or 2). The TP uses this data to map to correct winding. The correct I/O code must be used.
Winding Nominal Voltage	The winding voltage to help provide a reference for all data below (i.e., which winding is all of the data below referring to?)	This is obtained from the Nameplate, all transformer windings are designated with identification. See "A" in Figure E.8.	
OLTC Tap Positions	Does the winding have Off Load Tap Changer Windings? If yes, populate OLTC Table.	This is obtained from the Nameplate See "B" in Figure E.8.	
In-Service Tap Position	The tap position that the tap is in most of the time (in kV).	This is obtained from field verification of the OLTC position indicator. See "C" in Figure E.9.	See "1" in Figure E.7.



Two Winding Transformer Data Record

Power Flow | Short Circuit

Line Data

From Bus Number:

To Bus Number:

Branch ID: 1

From Bus Name:

To Bus Name:

Transformer Name:

Vector Group:

☑ In Service

☑ Metered on From end

☑ Winding 1 on From end

I/O Data

Winding I/O Code: 1 - Turns ratio (pu on bus base kV)

Impedance I/O Code: 2 - Z pu (winding kV winding MVA)

Admittance I/O Code: 1 - Y pu (system base)

1

Transformer Nominal Ratings Data

Specified R (pu): 0.001800

Specified X (pu): 0.074200

Winding 1 Ratio (pu): 1.0645

Winding 1 Nominal kV: 122.0000

Winding (1-2) Angle (degrees): 0.00

Magnetizing G (pu): 0.00051

Magnetizing B (pu): -0.00124

Winding 2 Ratio (pu): 1.0000

Winding 2 Nominal kV: 0.0000

Winding MVA: 127.5000

Impedance Table: 0

Rate A (MVA): 212.5

Rate B (MVA): 212.5

Rate C (MVA): 380.4

R table corrected (pu): 0.00180

X table corrected (pu): 0.07420

Control Data

Controlled Bus Number: 0

Controlled Bus Name:

Control Mode: 0 - None

☐ Controlled Bus On Winding Side

☑ Auto Adjust

Tap Positions: 33

Wnd Connect Angle: 0.00000

R1max (pu): 1.10000

R1min (pu): 0.90000

Vmax (pu): 1.10000

Vmin (pu): 0.90000

Load Drop Comp

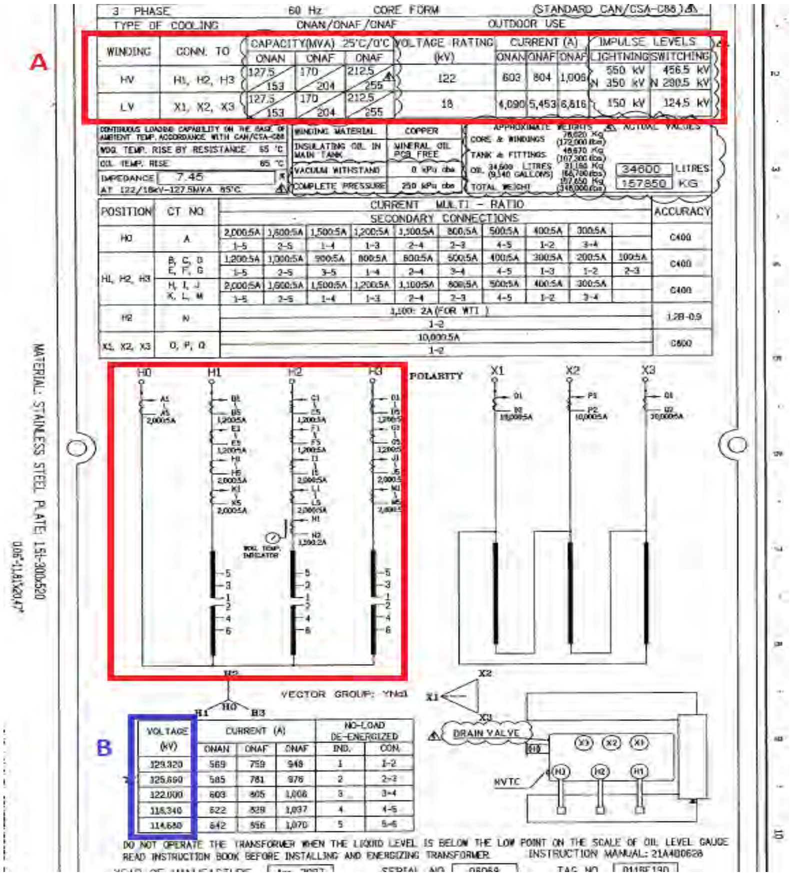
Load Drop Comp R (pu): 0.00000

Load Drop Comp X (pu): 0.00000

Owner Data

Owner		Fraction
103	Select...	1.000
0	Select...	1.000
0	Select...	1.000
0	Select...	1.000

Figure E.7: GSU Winding Ratio in Powerflow Data



3 PHASE 60 Hz CORE FORM (STANDARD CAN/CSA-C88)
TYPE OF COOLING ONAN/ONAF/ONAF OUTDOOR USE

WINDING	CONN. TO	CAPACITY(MVA) 25°C/0°C			VOLTAGE RATING (kV)	CURRENT (A)			IMPULSE LEVELS	
		ONAN	ONAF	ONAF		ONAN	ONAF	ONAF	LIGHTNING	SWITCHING
HV	H1, H2, H3	127.5 / 153	170 / 204	212.5 / 255	122	603	804	1,006	550 kV N 350 kV	456.5 kV N 290.5 kV
LV	X1, X2, X3	127.5 / 153	170 / 204	212.5 / 255	18	4,090	5,453	6,816	150 kV	124.5 kV

CONTINUOUS LOADING CAPABILITY ON THE BASE OF AMBIENT TEMP. ACCORDANCE WITH CAN/CSA-C88	
WDG. TEMP. RISE BY RESISTANCE	65 °C
OIL TEMP. RISE	65 °C
IMPEDANCE AT 122/18kV-127.5MVA 85°C	7.45 %

WINDING MATERIAL	COPPER
INSULATING OIL IN MAIN TANK	MINERAL OIL PCB FREE
VACUUM WITHSTAND	0 kPa abs
COMPLETE PRESSURE	250 kPa abs

APPROXIMATE WEIGHTS		ACTUAL VALUES	
CORE & WINDINGS	78,020 Kg (172,000 lbs)		
TANK & FITTINGS	48,670 Kg (107,300 lbs)		
OIL 34,600 LITRES (9,140 GALLONS)	31,160 Kg (68,700 lbs)	34600	LITRES
TOTAL WEIGHT	157,650 Kg (348,000 lbs)	157850	KG

POSITION	CT NO.	CURRENT MULTI - RATIO SECONDARY CONNECTIONS										ACCURACY
H0	A	2,000:5A	1,600:5A	1,500:5A	1,200:5A	1,100:5A	800:5A	500:5A	400:5A	300:5A		C400
		1-5	2-5	1-4	1-3	2-4	2-3	4-5	1-2	3-4		
H1, H2, H3	B, C, D E, F, G	1,200:5A	1,000:5A	900:5A	800:5A	600:5A	500:5A	400:5A	300:5A	200:5A	100:5A	C400
		1-5	2-5	3-5	1-4	2-4	3-4	4-5	1-3	1-2	2-3	
	H, I, J K, L, M	2,000:5A	1,600:5A	1,500:5A	1,200:5A	1,100:5A	800:5A	500:5A	400:5A	300:5A		C400
		1-5	2-5	1-4	1-3	2-4	2-3	4-5	1-2	3-4		
H2	N	1,100: 2A (FOR WTI)										1.2B-0.9
		1-2										
X1, X2, X3	O, P, Q	10,000:5A										C800
		1-2										

VECTOR GROUP: YNd1

VOLTAGE (kV)	CURRENT (A)			NO-LOAD DE-ENERGIZED	
	ONAN	ONAF	ONAF	IND.	CON.
129,320	569	759	948	1	1-2
125,660	585	781	976	2	2-3
122,000	603	805	1,006	3	3-4
118,340	622	829	1,037	4	4-5
114,680	642	856	1,070	5	5-6

DO NOT OPERATE THE TRANSFORMER WHEN THE LIQUID LEVEL IS BELOW THE LOW POINT ON THE SCALE OF OIL LEVEL GAUGE
READ INSTRUCTION BOOK BEFORE INSTALLING AND ENERGIZING TRANSFORMER. INSTRUCTION MANUAL: 21A400628

Figure E. 8: Transformer Diagram

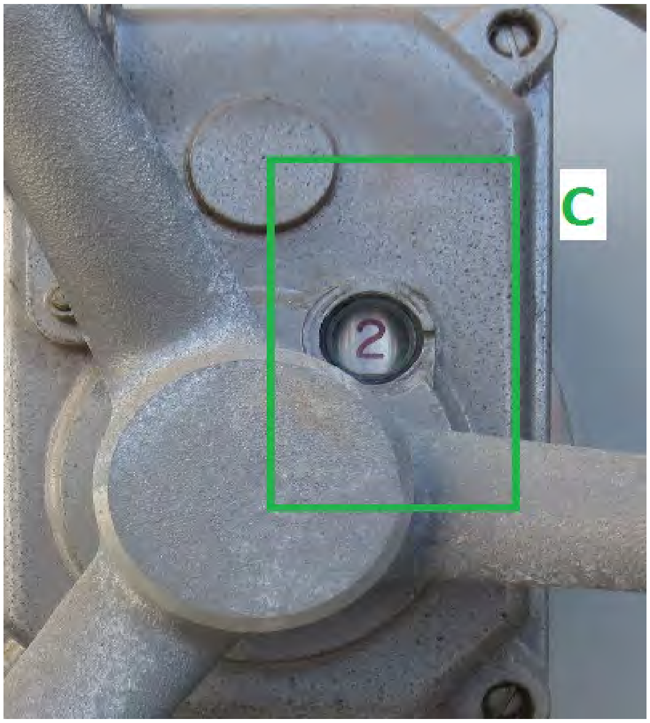


Figure E.9: Example of Physical Inspection of GSU Fixed Tap Position

GSU Transformer ULTC Data

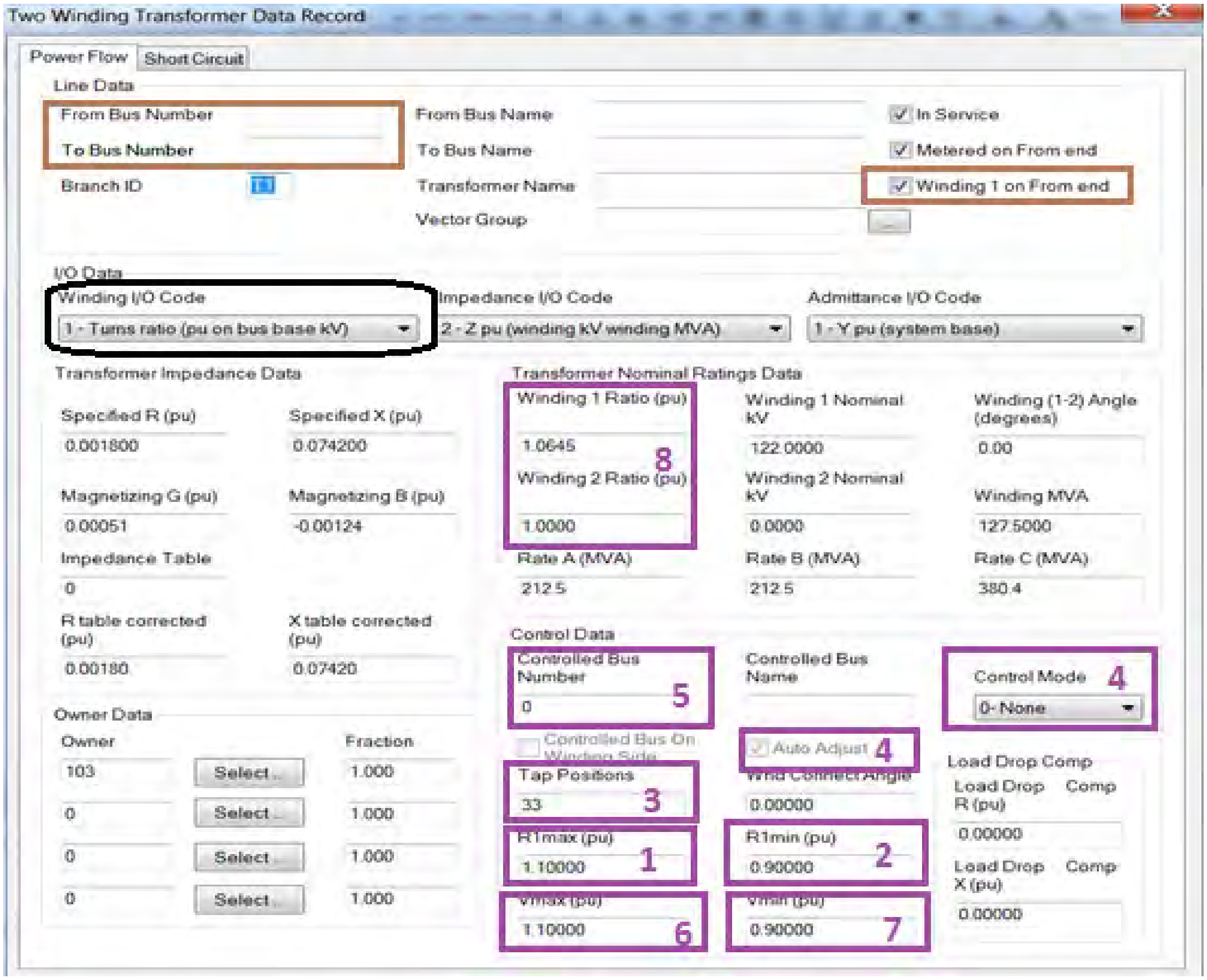
Table E.6 describes the data that should be requested related to GSU ULTC data.

Table E.6: GSU Transformer UTLC Data

Data	Description	Source of Data	Model Parameter
3f.4 Generator Step Up Transformer ULTC data *Provide the same data as that required for transformer under Item 6* *This table is to be duplicated for each winding that has a ULTC.*			
Winding Name (H,X,Y,T)	The winding name provides a reference for all data below (i.e., which winding is all of the data below referring to?). All transformer windings are designated with an identification.	GSU Nameplate See "A" in Figure E. 11.	Used by TP to select and map to correct winding (i.e., Winding 1 or 2).[32] The correct I/O code must be used.
Winding Nominal Voltage	The winding voltage provides a reference for all data below (i.e., which winding is all of the data below referring to?)	GSU Nameplate See "A" in Figure E. 11.	
Minimum ULTC Tap Voltage	The lowest kV value of the transformer ULTC selector switch device	GSU Nameplate See "B" in Figure E.12.	See "1" in Figure E.10
Maximum ULTC tap Voltage	The highest kV value of the transformer ULTC selector switch device	GSU Nameplate. See "C" in Figure E.12.	See "2" in Figure E.10
Number of ULTC Taps	The number of under load tap changer positions, not including neutral tap switchover positions (i.e., 17a and 17c for a 33 tap position ULTC) Example: if GSU has 16 raise and 16 lower, plus three neutral positions, then number of steps is 33.	GSU Nameplate See "D" in Figure E.12.	See "3" in Figure E.10
ULTC in Auto or Manual	Does the ULTC change position automatically? If Auto, populate the remaining fields with exception of in-service tap. If manual, populate only in-service tap position.	Elementary wiring diagram and tap changer control settings See "E" in Figure E.12.	See "4" in Figure E.10
ULTC voltage control bus (for automatic control)	A bus that has the potential measurement that feeds the tap changer control Communicate the winding name and voltage level (e.g., x-winding, 34.5 kV).	Elementary wiring diagram and tap changer control settings See "E" in Figure E.12.	See "5" in Figure E.10

[32] Note PSS®E only allows the user to place the ULTC on Winding 1, so the TP must coordinate this via the bus numbers and Winding 1 on from end option.

Table E.6: GSU Transformer UTLC Data			
Data	**Description**	**Source of Data**	**Model Parameter**
ULTC control central voltage (for automatic control)	The voltage that the tap changer bandwidth is centered around.	Tap changer control settings See "F" in Figure E.12.	Not used in model; used to validate data submitted
ULTC control upper voltage (for automatic control)	See attached diagram, this is the upper voltage limit that causes the tap changer control to issue a change tap command.	Tap changer control settings See Figure E.12.	See "6" in Figure E.10
ULTC control lower voltage (for automatic control)	See attached diagram, this is the lower voltage limit that causes the tap changer control to issue a change tap command.	Tap changer control settings See Figure E.12.	See "7" in Figure E.10
In-service tap (for manual control)	Tap position that the tap is in most of the time, expressed as kV.	Operational data	See "8" in Figure E.10



Two Winding Transformer Data Record

Power Flow | Short Circuit

Line Data

From Bus Number

To Bus Number

Branch ID 1

From Bus Name

To Bus Name

Transformer Name

Vector Group

☑ In Service

☑ Metered on From end

☑ Winding 1 on From end

I/O Data

Winding I/O Code: 1 - Turns ratio (pu on bus base kV)

Impedance I/O Code: 2 - Z pu (winding kV winding MVA)

Admittance I/O Code: 1 - Y pu (system base)

Transformer Impedance Data

Specified R (pu): 0.001800

Specified X (pu): 0.074200

Magnetizing G (pu): 0.00051

Magnetizing B (pu): -0.00124

Impedance Table: 0

R table corrected (pu): 0.00180

X table corrected (pu): 0.07420

Transformer Nominal Ratings Data

Winding 1 Ratio (pu): 1.0645

Winding 2 Ratio (pu): 1.0000

Winding 1 Nominal kV: 122.0000

Winding 2 Nominal kV: 0.0000

Winding (1-2) Angle (degrees): 0.00

Winding MVA: 127.5000

Rate A (MVA): 212.5

Rate B (MVA): 212.5

Rate C (MVA): 380.4

Control Data

Controlled Bus Number: 0

Controlled Bus Name

Control Mode: 0- None

□ Controlled Bus On Winding Side

☑ Auto Adjust

Tap Positions: 33

Wnd Connect Angle: 0.00000

R1max (pu): 1.10000

R1min (pu): 0.90000

Vmax (pu): 1.10000

Vmin (pu): 0.90000

Load Drop Comp

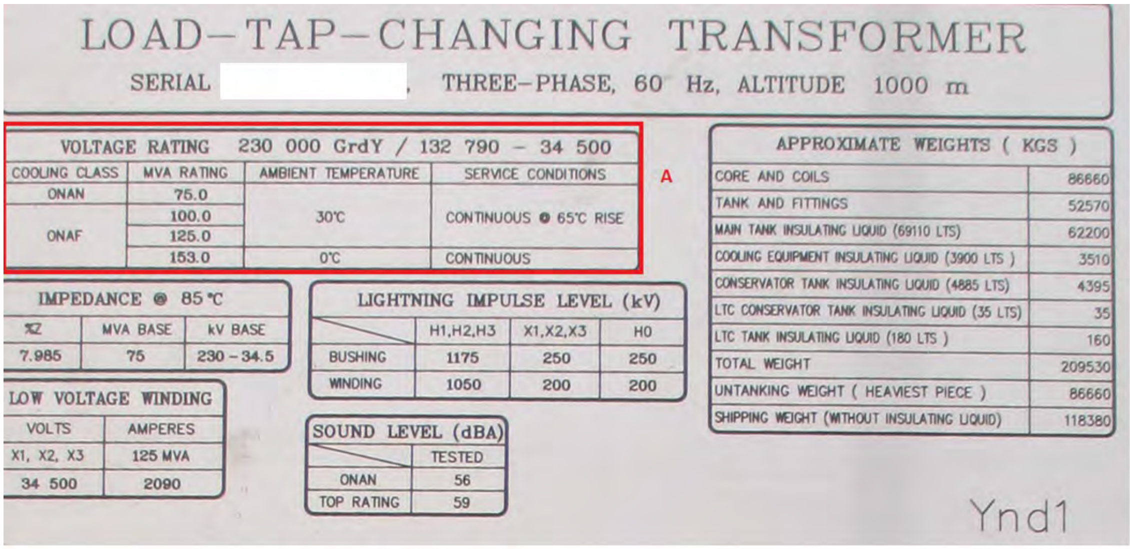
Load Drop Comp R (pu): 0.00000

Load Drop Comp X (pu): 0.00000

Owner Data

Owner		Fraction
103	Select...	1.000
0	Select...	1.000
0	Select...	1.000
0	Select...	1.000

Figure E.10: GSU ULTC Model Parameters in Powerflow Data



LOAD–TAP–CHANGING TRANSFORMER

SERIAL [redacted], THREE–PHASE, 60 Hz, ALTITUDE 1000 m

VOLTAGE RATING 230 000 GrdY / 132 790 – 34 500

COOLING CLASS	MVA RATING	AMBIENT TEMPERATURE	SERVICE CONDITIONS
ONAN	75.0	30°C	CONTINUOUS @ 65°C RISE
ONAF	100.0		
	125.0		
	153.0	0°C	CONTINUOUS

A

IMPEDANCE @ 85 °C

%Z	MVA BASE	kV BASE
7.985	75	230 – 34.5

LIGHTNING IMPULSE LEVEL (kV)

	H1,H2,H3	X1,X2,X3	H0
BUSHING	1175	250	250
WINDING	1050	200	200

LOW VOLTAGE WINDING

VOLTS	AMPERES
X1, X2, X3	125 MVA
34 500	2090

SOUND LEVEL (dBA)

	TESTED
ONAN	56
TOP RATING	59

APPROXIMATE WEIGHTS (KGS)

CORE AND COILS	86660
TANK AND FITTINGS	52570
MAIN TANK INSULATING LIQUID (69110 LTS)	62200
COOLING EQUIPMENT INSULATING LIQUID (3900 LTS)	3510
CONSERVATOR TANK INSULATING LIQUID (4885 LTS)	4395
LTC CONSERVATOR TANK INSULATING LIQUID (35 LTS)	35
LTC TANK INSULATING LIQUID (180 LTS)	160
TOTAL WEIGHT	209530
UNTANKING WEIGHT (HEAVIEST PIECE)	86660
SHIPPING WEIGHT (WITHOUT INSULATING LIQUID)	118380

Ynd1

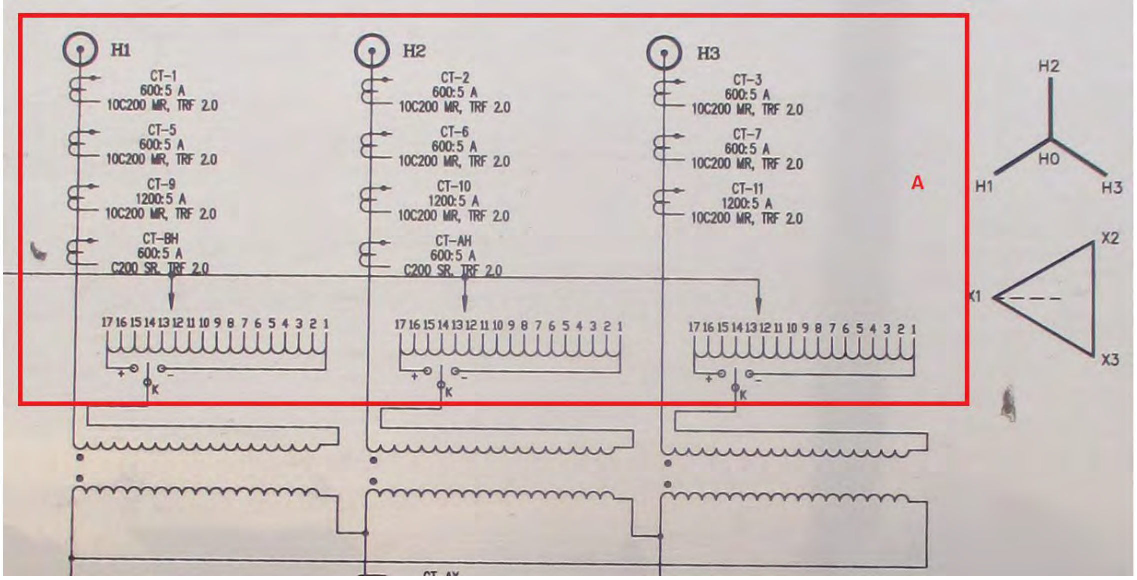
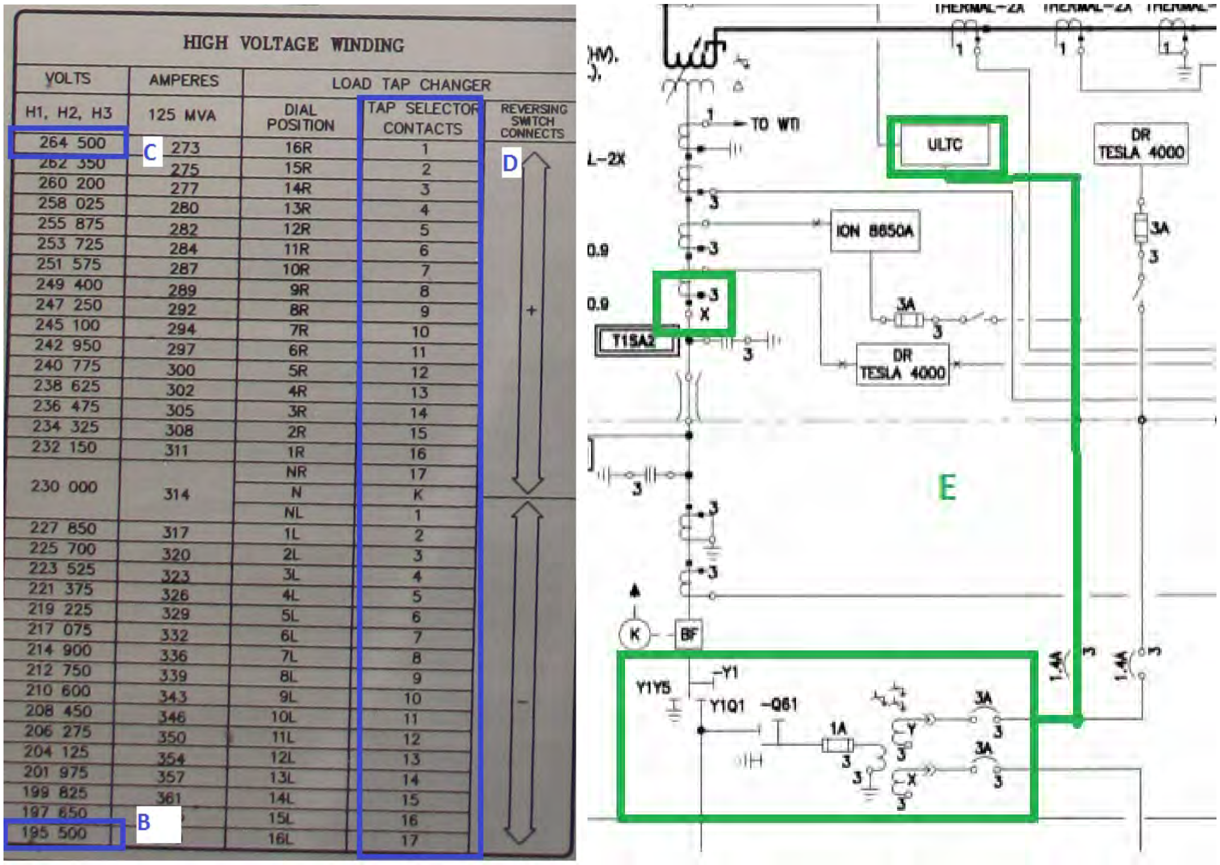


Figure E. 11: GSU ULTC Information from Nameplate



HIGH VOLTAGE WINDING				
VOLTS	AMPERES	LOAD TAP CHANGER		
H1, H2, H3	125 MVA	DIAL POSITION	TAP SELECTOR CONTACTS	REVERSING SWITCH CONNECTS
264 500	273	16R	1	
262 350	275	15R	2	
260 200	277	14R	3	
258 025	280	13R	4	
255 875	282	12R	5	
253 725	284	11R	6	
251 575	287	10R	7	
249 400	289	9R	8	
247 250	292	8R	9	+
245 100	294	7R	10	
242 950	297	6R	11	
240 775	300	5R	12	
238 625	302	4R	13	
236 475	305	3R	14	
234 325	308	2R	15	
232 150	311	1R	16	
230 000	314	NR	17	
		N	K	
		NL	1	
227 850	317	1L	2	
225 700	320	2L	3	
223 525	323	3L	4	
221 375	326	4L	5	
219 225	329	5L	6	
217 075	332	6L	7	
214 900	336	7L	8	
212 750	339	8L	9	
210 600	343	9L	10	−
208 450	346	10L	11	
206 275	350	11L	12	
204 125	354	12L	13	
201 975	357	13L	14	
199 825	361	14L	15	
197 650	[illegible]	15L	16	
195 500	[illegible]	16L	17	

Figure E.12: GSU ULTC Information from Nameplate and Specification Sheet

GSU Transformer Impedance Data

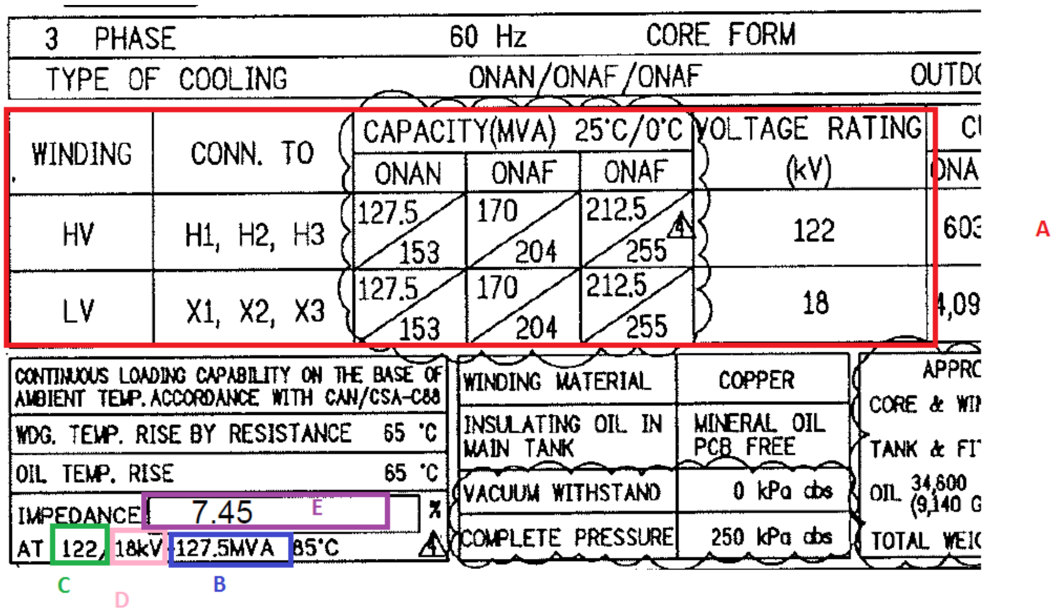
Table E.7 describes the data that should be requested related to GSU impedance data.

Table E.7: GSU Transformer Impedance Data			
Data	**Description**	**Source of Data**	**Model Parameter**
3f.b Generator Step Up Transformer Impedance data *Provide same data as that required for transformer under Item 6* *This table is to be duplicated for each winding pair*			
Winding 1 Name (H,X,Y,T)	The winding name to provide a reference for all data below (i.e., which winding is all of the data below referring to?)	GSU Nameplate See "A" in Figure E.13.	Used by TP to select and map to correct winding pair.[33] The correct I/O code must be used.
Winding 2 Name (H,X,Y,T)	The winding name to provide a reference for all data below (i.e., which winding is all of the data below referring to?)	GSU Nameplate See "A" in Figure E.13.	
MVA base	MVA base at which per unit impedance is measured	GSU Nameplate. See "B" in Figure E.13.	See "1" in Figure E.14.

[33] Note PSS®E allows the user to place winding one on either bus, this must be coordinated with ULTC.

Table E.7: GSU Transformer Impedance Data

Data	Description	Source of Data	Model Parameter
	If this is three single-phase transformers, the MVA value should be multiplied by three to reflect the three-phase MVA base.		
Winding 1 Voltage Base	The voltage base at which the per unit impedance value is measured at for winding 1 When the winding has either OLTC or ULTC, this is usually the nominal tap. If measurements at other taps are available, they may be submitted.	Nominal tap impedances on GSU nameplate; impedances on other taps may only be in the test report. See "C" in Figure E.13.	See "2" in Figure E.14.
Winding 2 Voltage Base	The voltage base at which the per unit impedance value is measured at for winding 2 When the winding has either OLTC or ULTC, this is usually the nominal tap. If measurements at other taps are available, they may be submitted.	Nominal tap impedances on GSU nameplate; impedances on other taps may only be in the test report. See "D" in Figure E.13.	See "3" in Figure E.14.
Positive Sequence X	The measured positive sequence reactance between the designated windings	GSU nameplate and test report See "E" in Figure E.13.	See "4" in Figure E.14.
Positive Sequence R	The measured positive sequence resistance between the designated windings	Test report; may be presented in load loss rather than resistance	See "5" in Figure E.14.



3 PHASE 60 Hz CORE FORM

TYPE OF COOLING ONAN/ONAF/ONAF OUTD

WINDING	CONN. TO	CAPACITY(MVA) 25°C/0°C ONAN	ONAF	ONAF	VOLTAGE RATING (kV)	C ONA
HV	H1, H2, H3	127.5/153	170/204	212.5/255	122	603
LV	X1, X2, X3	127.5/153	170/204	212.5/255	18	4,09

CONTINUOUS LOADING CAPABILITY ON THE BASE OF AMBIENT TEMP. ACCORDANCE WITH CAN/CSA-C88

WDG. TEMP. RISE BY RESISTANCE 65 °C

OIL TEMP. RISE 65 °C

IMPEDANCE 7.45 %

AT 122/18kV 127.5MVA 85°C

WINDING MATERIAL	COPPER
INSULATING OIL IN MAIN TANK	MINERAL OIL PCB FREE
VACUUM WITHSTAND	0 kPa abs
COMPLETE PRESSURE	250 kPa abs

APPR

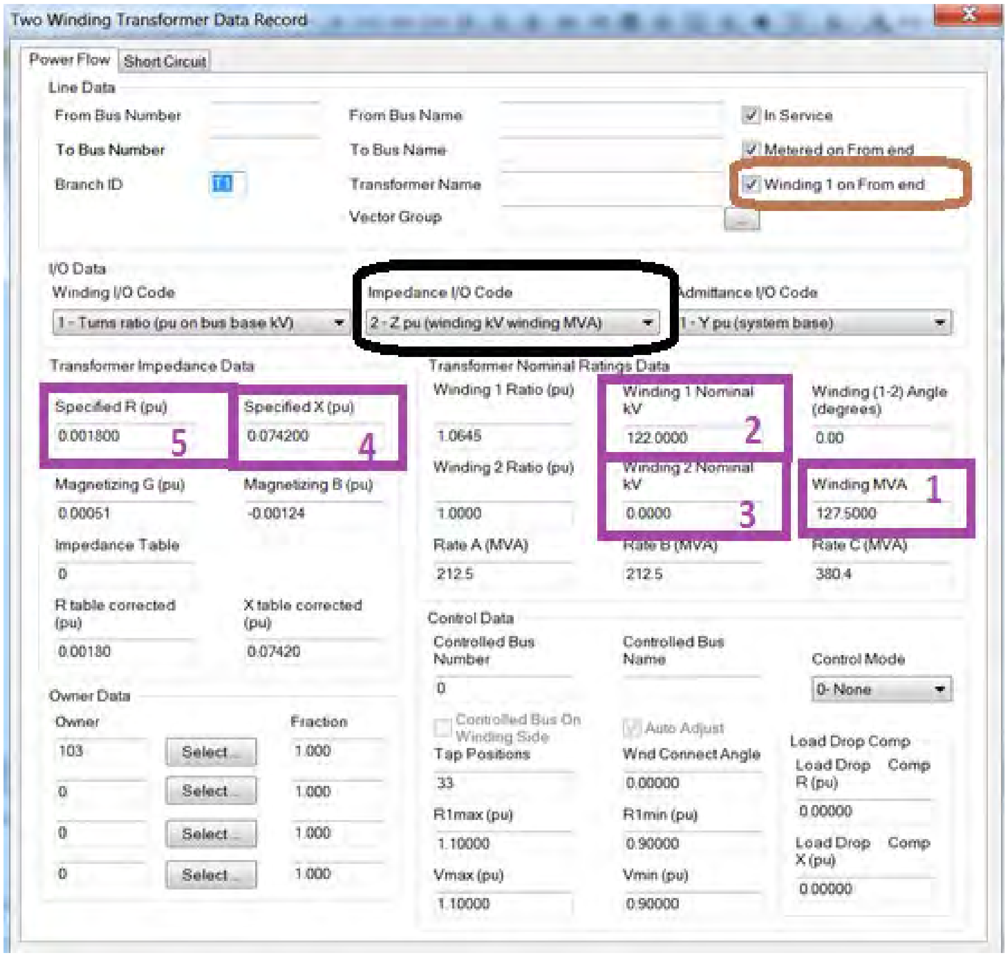
CORE & WI

TANK & FI

OIL 34,600 (9,140 G

TOTAL WEI

Figure E.13: GSU Impedance Information from Specification Sheet



Two Winding Transformer Data Record

Power Flow | Short Circuit

Line Data

From Bus Number

From Bus Name

☑ In Service

To Bus Number

To Bus Name

☑ Metered on From end

Branch ID: T1

Transformer Name

☑ Winding 1 on From end

Vector Group

I/O Data

Winding I/O Code: 1 - Turns ratio (pu on bus base kV)

Impedance I/O Code: 2 - Z pu (winding kV winding MVA)

Admittance I/O Code: 1 - Y pu (system base)

Transformer Impedance Data

Specified R (pu): 0.001800

Specified X (pu): 0.074200

Magnetizing G (pu): 0.00051

Magnetizing B (pu): -0.00124

Impedance Table: 0

R table corrected (pu): 0.00180

X table corrected (pu): 0.07420

Transformer Nominal Ratings Data

Winding 1 Ratio (pu): 1.0645

Winding 1 Nominal kV: 122.0000

Winding (1-2) Angle (degrees): 0.00

Winding 2 Ratio (pu): 1.0000

Winding 2 Nominal kV: 0.0000

Winding MVA: 127.5000

Rate A (MVA): 212.5

Rate B (MVA): 212.5

Rate C (MVA): 380.4

Control Data

Controlled Bus Number: 0

Controlled Bus Name

Control Mode: 0- None

□ Controlled Bus On Winding Side

☑ Auto Adjust

Tap Positions: 33

Wnd Connect Angle: 0.00000

R1max (pu): 1.10000

R1min (pu): 0.90000

Vmax (pu): 1.10000

Vmin (pu): 0.90000

Load Drop Comp

Load Drop Comp R (pu): 0.00000

Load Drop Comp X (pu): 0.00000

Owner Data

Owner		Fraction
103	Select...	1.000
0	Select...	1.000
0	Select...	1.000
0	Select...	1.000

Figure E.14: GSU Impedance Parameters in Powerflow Data

References

1. NERC MOD-032-1 Reliability Standard – Data for Power System Modeling and Analysis: https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx.
2. NERC Acceptable Models List: https://www.nerc.com/pa/RAPA/ModelAssessment/Pages/default.aspx.
3. NATF Modeling Data Request MOD-032 Reference Document: https://www.natf.net/documents.
4. ERCOT Planning Guide: http://www.ercot.com/mktrules/guides/planning/current.
5. WECC Data Preparation Manual: https://www.wecc.biz/Reliability/WECC-Data-Preparation-Manual-Rev-7-Approved.pdf.
6. Multiregional Modeling Working Group Procedural Manual: https://rfirst.org/ProgramAreas/ESP/ERAG/MMWG.
7. Transformer Modeling Guide, Alberta Electric System Operator, Version 2, July 2014: https://www.aeso.ca/assets/linkfiles/4040.002-Rev02-Transformer-Modelling-Guide.pdf.

Contributors

NERC gratefully acknowledges the following primary contributors, all members of the NERC PPMVTF, and NAGF in developing this guidance material.

Name	Entity	Status
Hassan Baklou	SDG&E	PPMVTF Member
Kent Bolton	WECC	PPMVTF Member
Tom Carpenter	TVA	PPMVTF Member
Rob Clemence	IESO	PPMVTF Member
Richard Dennis	Emerson PWS	PPMVTF Member
Clint Drescher	Wisconsin Public Service	PPMVTF Member
Josh Grindeland	ITC	PPMVTF Member
Bo Gong	ColumbiaGrid	PPMVTF Member
Casey Harman	Puget Sound Energy	PPMVTF Member
Shih-Min Hsu	Southern Company	PPMVTF Member
Dennis Kane	We Energies	PPMVTF Member
Gordon Kawaley	BPA	PPMVTF Member
Ruth Kloecker	ITC	PPMVTF Member
Bob Krueger	ATC	PPMVTF Member
David Lemmons	Ethos Energy	PPMVTF Member
Michael Lombardi	NPCC	PPMVTF Member
Tracy MacNicoll	Utility Services, Inc.	PPMVTF Member
Marcus Moor	Evergy	PPMVTF Member
Michael Odom	Southwest Power Pool	PPMVTF Member
John Owen	Powertech Labs	PPMVTF Member
Shawn Patterson	U.S. Bureau of Reclamation	PPMVTF Chair
Randy Rhinier	Duke Energy	PPMVTF Member
David Schooley	Commonwealth Edison	PPMVTF Member
John Schmoker	North American Energy Services	PPMVTF Member
Randhir Singh	PSEG	PPMVTF Member
Stan Sliwa	PJM	PPMVTF Member
Brian Thomas	GE	PPMVTF Member
John Zong	Powertech Labs	PPMVTF Member
Ryan Quint	NERC	NERC Staff – PPMVTF Coordinator
John Skeath	NERC	NERC Staff

Agenda Item 11
Reliability and Security
Technical Committee Meeting
June 8, 2021

Security Integration and Technology Enablement Subcommittee (SITES) Update and Work Plan

Action

Approve

Summary

The SITES has begun implementing and updating their work plan. Chair Naas will provide a status update as well as a revised work plan for approval.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT Security Integration and Technology Enablement Subcommittee 2021 Work Plan

Security Integration and Technology Enablement Subcommittee 2021-2022 Work Plan

NERC Security Integration and Technology Enablement Subcommittee (SITES), in collaboration with industry, has developed a 2021-2022 work plan aligned with the SITES scope[1] document and industry priorities which includes the following focus areas.

SITES 2021-2022 Work Plan

Task	Description	Deliverables	Lead	Estimated Completion
BES Operations in the Cloud	FERC has directed NERC to provide an informational filing regarding use of cloud technologies for bulk electric system (BES) operations. This extends the use of cloud beyond just BES cyber system information to use of cloud for actual BES operations. SITES will support NERC and FERC by developing a white paper that helps provide information and direction related to specific questions and topics contained within the FERC order.	White Paper	TBD	Q4 2021
Security Integration	The integration of security considerations into conventional grid planning, design, and operations is a primary goal of the NERC Reliability and Security Technical Committee (RSTC). SITES will focus on this topic by developing a unified message that considers ongoing industry efforts in addition to developing a reliability/security guideline outlining recommended security integration practices.	Reliability / Security Guideline	TBD	Q1 2022
Zero-Trust Concept	While the concept of “zero-trust” is widely used within the security community, industry would	Security Guideline	TBD	Q4 2021

[1] https://www.nerc.com/comm/RSTC/SITES_/SITES%20Scope.pdf

SITES 2021-2022 Work Plan				
Task	**Description**	**Deliverables**	**Lead**	**Estimated Completion**
	benefit from guidance on the practical use and consideration within the context of the BPS. This effort will explore the concept of zero trust, particularly in the context of the recent SolarWinds compromise, while clarifying related risks and vulnerabilities, practical applications of zero-trust, emerging technologies to apply zero-trust architectures, how to integrate zero-trust with existing NERC CIP standards, and any cost-benefit analyses, etc., in collaboration with other industries and agencies where applicable. (e.g., US DOD, NIST)			
IT/OT Convergence	The concept of "IT/OT convergence" continues to become increasingly relevant, and industry understanding in this area supports the overall security posture of the electric grid. SITES will consider current information technology (IT) and operational technology (OT) security practices and perspectives and develop recommendations to industry that focus on the future state of both the BPS grid and IT/OT security practices. The group will leverage other industries and agencies (e.g., US DOD, NIST)	White Paper	TBD	Q1 2022
Reliability / Resilience / Security Balance	Balancing reliability, resilience, and security necessitates a fundamental understanding of each of these interests. While industry's understanding of reliability is established, and understanding of resilience has advanced, understanding of security continues to develop. SITES will explore the principles for identifying, assessing, and mitigating possible "security issues" to facilitate industry's continued understanding of security. This effort will also focus on terminology clarifications to support collaboration of engineering and security subject-matter experts.	White Paper	TBD	Q1 2022

SITES 2021-2022 Work Plan

Task	Description	Deliverables	Lead	Estimated Completion
Emerging Technologies	Emerging technologies present both opportunities and challenges to the energy sector. This effort will review emerging technologies and potential impacts to security and reliability of the BPS. The team will support industry consideration of emerging technologies, possible implementation of these technologies, and possible risks and opportunities for adoption. The goal in this area is to enable the secure use of these technologies within the industry.	White Paper	TBD	Q1 2022
Risk Identification	Increasing system complexity coupled with decreasing diversity of equipment is increasing the risk of security threats and vulnerabilities. This effort will identify risks and propose mitigations while also considering the potential risks and benefits of increasing system complexity (and attack surface) and decreasing diversity of equipment. SITES will seek to produce useful work product on identified risk areas, coordinated with industry efforts.	White Paper	TBD	Q1 2022
Security Implementation	Implementation of security practices continues to pose challenges for operations technology systems in the context of emerging technologies and a rapidly evolving grid. Opportunities exist to provide guidance for the following: • Device configuration to enhance security, visibility, and monitoring • Identification of secure automated solutions for transient cyber assets • Reference architectures for new systems • Securing applications • Proving use before deployment • Security management for smaller entities	White Paper	TBD	Q1 2022

SITES 2021-2022 Work Plan				
Task	**Description**	**Deliverables**	**Lead**	**Estimated Completion**
	• Secure use of new technology (e.g., technology to defeat the malicious use of drones) • Clarification of terminology. This effort will prioritize and develop guidance for the topics above. These topics will be coordinated closely with NERC Security Working Group (SWG) and any other relevant NERC stakeholder groups.			

NOTE: Any of the aforementioned topics may be combined as the team starts development of work products on each subject.

Agenda Item 12
Reliability and Security
Technical Committee Meeting
June 8, 2021

Inverter-based Resources Performance Working Group (IRPWG) San Fernando Disturbance Follow-Up White Paper

Action

Approve

Summary

This brief white paper was developed by the NERC Inverter-Based Resource Performance Working Group (IRPWG) as a follow-up to the July 2020 San Fernando Disturbance Report published by NERC. That report contained a set of key findings and recommendations. The IRPWG discussed each of the key findings and recommendations in detail, provides a brief technical discussion and basis for each item, and where appropriate recommends follow-up action items. Table 1 shows the key findings and recommendations from the NERC disturbance report on the left-hand column and the IRPWG follow-up and recommendations for each item in the right-hand column.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

San Fernando Disturbance Follow-Up

NERC Inverter-Based Resource Performance Working Group (IRPWG)
White Paper – June 2021

This brief white paper was developed by the NERC Inverter-Based Resource Performance Working Group (IRPWG) as a follow-up to the July 2020 San Fernando Disturbance Report published by NERC.[1] That report contained a set of key findings and recommendations. The IRPWG discussed each of the key findings and recommendations in detail, provides a brief technical discussion and basis for each item, and where appropriate recommends follow-up action items. Table 1 shows the key findings and recommendations from the NERC disturbance report on the left-hand column and the IRPWG follow-up and recommendations for each item in the right-hand column.

The following are the recommended actions from the IRPWG review:

1. FERC should integrate the recommendations from the San Fernando report and the IRPWG guidelines into the pro forma LGIA for all newly interconnecting inverter-based resources. The future PRC-002 Standard Drafting Team should consider P2800 Clause 11 efforts, and ensure that the modifications require disturbance monitoring equipment at inverter-based resource facilities.
2. IRPWG will continue summarizing lessons learned from the events with systematic causes of inverter tripping IRPWG in future publications (white papers, guidelines, SARs etc.). FERC and NERC, in coordination with industry, should develop a coordinated strategy to ensure the effective and widespread adoption of IEEE P2800 once it is approved.
3. IRPWG should draft a SAR to address the outstanding recommendation by NERC to address the issue identified in EOP-004-4 regarding the generation loss criteria so that it is applicable for inverter-based resources as well synchronous generation.
4. Modeling and study standards (e.g., MOD and TPL) should be reviewed by IRPWG to consider the inclusion of EMT models for study purposes by the TP and PC. Currently these studies that would be used to identify possible tripping or abnormal performance from inverter-based resources are not required and are performed only in certain occasions where the TP or PC has identified issues with other modeling tools. However, the issues identified in these disturbances have not been identified or highlighted by the TPs or PCs in their

[1] https://www.nerc.com/pa/rrm/ea/Pages/July_2020_San_Fernando_Disturbance_Report.aspx

respective area. IRPWG is working on an EMT modeling reliability guideline; however, this does not ensure any one entity actually executes EMT studies, when needed.

5. Future industry efforts may consider assessing the extent to which industry has adopted the recommendations in the NERC guidelines regarding interconnection requirements improvements. This would help understand the extent to which these risks are being addressed by industry.

Table 1: Review of Disturbance Report Findings and Recommendations

#	Key Findings/Recommendation	IRPWG Follow-Up
	• **Poor Solar PV Data Resolution:** Almost all solar PV facilities involved in this disturbance were not able to provide adequate information to the analysis team to fully understand the causes of tripping and develop recommended mitigating actions. In many cases, the archived data had resolutions of one-minute or even five-minutes; this serves no useful purpose for post-mortem disturbance analysis. Data resolutions should be on the order of one-second, and other forms of high-speed data recording should be available from the individual inverters within the facility as well as at the plant-level controller. Point-on-wave digital fault recorder data is the most useful data for this type of analysis along with inverter fault codes and inverter oscillography data. ▪ **Recommendation (GO, Generator Operator (GOP)):** All GOs and GOPs should ensure adequate data monitoring within their facilities for inverter-based resources to determine root causes of abnormal performance to BPS disturbances. This includes having access to inverter and plant-level settings, fault codes, oscillography records, digital fault recorder data, and archived plant data (i.e., supervisory control and data acquisition (SCADA) data) with a resolution	IRPWG (formerly IRPTF) submitted a SAR on PRC-002-2 regarding its minimal applicability to inverter-based resources due to the size criteria for dynamic disturbance recording data and the fundamental way in which digital fault recorder data and sequence of events data are specified. Both requirements in PRC-002-2 preclude the selection of locations near or at inverter-based facilities on the bulk power system. IRPWG has published NERC Reliability Guideline: Improvements to Interconnection Requirements for BPS-Connected Inverter-Based Resources, which strongly recommends all BPS-connected inverter-based resources to have sufficient monitoring capability to capture data for event analysis and real-time visibility. However, those recommendations are not mandatory nor appear to be adhered to by BPS-connected inverter-based resource owners since this disturbance further illustrated that nearly no usable data is available from a wide range of owner/operators of these facilities.

Table 1: Review of Disturbance Report Findings and Recommendations		
#	Key Findings/Recommendation	IRPWG Follow-Up
	of one sample per second or faster. NERC Standards should be enhanced to ensure this data is available from all BPS generating facilities, as this continues to be a major issue limiting the ability to perform event analysis. ▪ **Recommendation (TO, FERC):** All TOs should establish or improve data recording requirements for all BPS-connected generating resources, including both synchronous and inverter-based resources, to ensure appropriate data is available for event analysis. FERC may consider adding this capability to the pro forma *Large Generator Interconnection Agreement*.[2] Detailed recommendations are documented in NERC *Reliability Guideline: Improvements to Interconnection Requirements for BPS-Connected Inverter-Based Resources*.[3]	IRPWG is not aware of any activities within FERC to add the recommendations from this NERC guideline to the pro forma LGIA or SGIA; however, as the report highlights this action is recommended. The IEEE P2800 Clause 11 includes requirements for data monitoring, resolution, and retention that will bring future resources to current technology; however, this will only apply to new resources and is likely a few years away in terms of full adoption and effectiveness. **Recommended Action from IRPWG Follow-Up:** FERC should integrate the recommendations from the San Fernando report and the IRPWG guidelines into the pro forma LGIA for all newly interconnecting inverter-based resources. The future PRC-002 Standard Drafting Team should consider P2800 Clause 11 efforts, and ensure that the modifications require disturbance monitoring equipment at inverter-based resource facilities.
	• **Continued and Improved Analyses Needed:** This event, as with past events, involved a significant number of solar PV resources reducing power output (either due to momentary cessation or inverter tripping) as a result of normally-cleared BPS faults. The widespread nature of power reduction across many facilities poses risks to BPS performance and reliability. Many of the issues identified in this disturbance appear systemic and are not being widely addressed by the solar PV fleet.	The NERC Event Analysis Process now includes Category 1i to capture the "non-consequential interruption of inverter type resources aggregated to 500 MW or more not caused by a fault on its inverters, or its ac terminal equipment." The ERO Enterprise will continue to analyze these types of disturbances to identify any possible systemic causes of inverter tripping. Entities are encouraged to do root cause analysis of smaller events that may occur, and GOs should ensure they have

[2] https://www.ferc.gov/industries-data/electric/electric-transmission/generator-interconnection/standard-interconnection
[3] https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_IBR_Interconnection_Requirements_Improvements.pdf

Table 1: Review of Disturbance Report Findings and Recommendations

#	Key Findings/Recommendation	IRPWG Follow-Up
	▪ **Recommendation (RC, GO, GOP):** Analysis of inverter-based resource performance for system faults should be conducted on a regular basis to identify possible abnormal performance. Root cause analysis should be conducted for identified abnormal performance events to develop mitigating measures to improve fleet performance. RCs should be analyzing fleet performance after significant grid disturbances, identifying any abnormal performance, and ensuring affected entities are determining whether improvements to their facilities can be made to eliminate abnormal performance. It does not appear these activities are regularly taking place, and improvements to processes should be developed so that these activities occur more frequently by RCs and affected entities rather than primarily by the ERO Enterprise. Entities are strongly encouraged to share their lessons learned with NERC and its Inverter-Based Resource Performance Working Group (IRPWG) to help industry advance its capabilities moving forward. ▪ **Recommendation (NERC Inverter-Based Resource Performance Working Group (IRPWG), Industry):** NERC and its technical stakeholder groups (i.e., NERC IRPWG) should continue outreach and the development of recommended practices and reliability guidelines to help industry ensure BPS reliability as the penetration of BPS-connected inverter-based resources continues to increase. However, while outreach has been effective in supporting industry in these efforts, it is clear that outreach alone is not an effective	sufficient reporting capabilities to identify these events and determine root causes. NERC and the IRPWG continue to engage in many industry forums (e.g., IEEE, ESIG, CIGRE) and share the lessons learned and recommendations from the published reports, white papers, and guidelines. Further, many IRPWG members are also IEEE P2800 members. **Recommended Action from IRPWG Follow-Up:** NERC IRPWG will continue summarizing lessons learned from the events with systematic causes of inverter tripping IRPWG in future publications (white papers, guidelines, SARs etc.). FERC and NERC, in coordination with industry, should develop a coordinated strategy to ensure the effective and widespread adoption of IEEE P2800 once it is approved.

Table 1: Review of Disturbance Report Findings and Recommendations		
#	Key Findings/Recommendation	IRPWG Follow-Up
	means of minimizing possible abnormal behavior from these resources and developing mitigating measures to eliminate these issues. Additional actions (e.g., standards enhancements, updates to interconnection requirements, engagement in IEEE P2800 activities) are needed by industry to ensure entities are taking appropriate steps to support reliable operation of the BPS.	
	• **Improvements to Identification of Disturbances and Event Reporting:** These events impact many resources across multiple BAs and Reliability Coordinator (RC) footprints. EOP-004-4[4] does not include events of this nature due to the large generation loss criteria contained within EOP-004-4. Therefore, no reporting on these types of events is required and has led to the identification of these events being on an ad hoc basis. CAISO provided a brief report for this event under the voluntary NERC EA Process; however, NERC and WECC needed to perform a more comprehensive analysis to determine any root causes since the brief report did not provide this level of detail or recommend any mitigating actions. ▪ **Recommendation (Industry, NERC, FERC):** Ad hoc reporting of events involving multiple generating resources and possible systemic performance issues should not be considered an acceptable level of reporting. NERC EOP-004-	There is no known action to develop a SAR to address the issues raised by NERC regarding EOP-004-4 and the generation loss requirement it includes. Without addressing this issue, these types of events will not be reported on any uniform basis and will continue to be ad hoc in terms of initiating an analysis. BA and RC reporting helps ensure that the ERO Enterprise is apprised of widespread events and coordinated analyses can occur to support industry address possible reliability risks. NERC Event Analysis Process now includes Category 1i to capture the "non-consequential interruption of inverter type resources aggregated to 500 MW or more not caused by a fault on its inverters, or its ac terminal equipment." The ERO Enterprise will continue to analyze these types of disturbances to identify any possible systemic causes of inverter tripping.

[4] https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=EOP-004-4&title=Event%20Reporting

Table 1: Review of Disturbance Report Findings and Recommendations		
#	Key Findings/Recommendation	IRPWG Follow-Up
	4 should be reviewed in terms of the thresholds used for generator tripping events and should also consider the extent of resources involved in the disturbance. A reasonable threshold for reporting would be around 500 MW of reduction in output (partial or full tripping across all affected resources). Updates to reporting these types of events (not necessarily with quick turnaround times) will help industry improve their situational awareness of abnormal inverter-based resource performance and possible issues needing mitigating action by facility owners to improve their performance.	**Recommended Action from IRPWG Follow-Up:** IRPWG should draft a SAR to address the outstanding recommendation by NERC to address the issue identified in EOP-004-4 regarding the generation loss criteria so that it is applicable for inverter-based resources as well synchronous generation.

Table 1: Review of Disturbance Report Findings and Recommendations

#	Key Findings/Recommendation	IRPWG Follow-Up
	• **Inverter Tripping:** There were three causes of BPS-connected solar PV tripping during this disturbance—ac overcurrent protection, dc low voltage protection, and ac low voltage protection. The vast majority of inverters that tripped were from a single manufacturer that tripped on either ac overcurrent or dc low voltage protection. All inverter tripping was considered abnormal since the BPS fault events were normally-cleared and no resources were disconnected as a consequence of the faulted elements being removed. The primary form of tripping, ac overcurrent protection, is not considered in PRC-024 since it is not related to voltage or frequency protection within the facility. Similar to past disturbances involving tripping due to dc reverse current protection, phase jump protection, and phase lock loop loss of synchronism protection, none of these common trip mechanisms are captured in the latest version of PRC-024. ▪ **Recommendation (GO, GOP, TO, NERC, FERC):** Partial tripping of inverters within a facility is still considered tripping and has an adverse impact on BPS performance. Partial tripping of inverters during normally-cleared faults should not be considered an acceptable level of performance from inverter-based resources. Facility performance should be more closely reviewed for compliance with NERC Reliability Standards and other applicable interconnection requirements. GOs and GOPs should analyze partial tripping events and work with their	Some of the causes of tripping identified in the San Fernando disturbance (as well as the Canyon 2 Fire, Palmdale Roost, Angeles Forest disturbances) are not addressed in NERC Reliability Standards. In particular, NERC PRC-024 only focuses on voltage and frequency protective relaying or controls that could cause momentary cessation or tripping of a generating resource. However, dc reverse current, phase lock loop loss of synchronism, sub-cycle ac overvoltage, and ac overcurrent tripping all are generally not considered in any NERC standards/requirements. This requires TOs to implement and enforce their interconnection requirements for these resources. IEEE P2800 will be addressing these types of tripping or cessation for newly interconnecting inverter-based resources in the future (likely a couple years from widespread adoption); however, existing resources will continue to experience possible tripping and reduction of power output for these reasons. GOs are encouraged to put measures in place to identify partial tripping events and address possible tripping issues. TOPs and RCs should also analyze fault disturbance events and review the performance of inverter-based resources to identify possible partial tripping events and engage the respective GO to address the abnormal performance. These types of tripping are also not generally identifiable using positive sequence dynamic models and require EMT models;

Table 1: Review of Disturbance Report Findings and Recommendations

#	Key Findings/Recommendation	IRPWG Follow-Up
	inverter manufacturers to mitigate inverter tripping to the extent possible. ▪ **Recommendation (GO, GOP, TO, FERC):** Inverters are commonly tripped for reasons other than voltage- or frequency-related tripping, and the PRC-024 curves are often set directly in the inverter solely for compliance with PRC-024 rather than to protect the inverter from physical damage. These other forms of tripping (e.g., ac overcurrent, phase lock loop loss of synchronism) lead to partial tripping of many different solar PV facilities and have an adverse impact on BPS performance. These types of tripping should not be considered acceptable for normally-cleared BPS fault events and enhancements to PRC-024 (or a possibly a new standard focused on ride-through capability) should be made to account for these other forms of tripping. ▪ **Recommendation (TO, Transmission Planner (TP), Planning Coordinator (PC), TOP, RC):** Interconnection requirements should ensure that the models provided during the interconnection study process are able to account for all forms of tripping by inverter-based resources so that sufficiently accurate studies can be conducted by the TP and PC. In most cases, this will require the collection of accurate, plant-specific electromagnetic transient (EMT) models. TPs and PCs should be conducting studies during the interconnection process to ensure adequate fault ride-through while considering all possible forms of inverter tripping. Phase lock loop issues, dc reverse current tripping,	yet EMT modeling is not a widely adopted and used practice for interconnection studies. Therefore, possible tripping will likely go unnoticed for inverter-based resources that are not studied adequately during the interconnection study process. **Recommended Action from IRPWG Follow-Up:** Modeling and study standards (e.g., MOD and TPL) should be reviewed by IRPWG to consider the inclusion of EMT models for study purposes by the TP and PC. Currently these studies that would be used to identify possible tripping or abnormal performance from inverter-based resources are not required and are performed only in certain occasions where the TP or PC has identified issues with other modeling tools. However, the issues identified in these disturbances have not been identified or highlighted by the TPs or PCs in their respective area. IRPWG is working on an EMT modeling reliability guideline; however, this does not ensure any one entity actually executes EMT studies, when needed.

Table 1: Review of Disturbance Report Findings and Recommendations

#	Key Findings/Recommendation	IRPWG Follow-Up
	ac overcurrent tripping, and any other form of tripping beyond simply PRC-024 protection requirements should be accurately modeled and tested by the TP and PC during their interconnection studies. Any unexpected or abnormal performance identified during interconnection studies should be addressed prior to allowing that facility to interconnect to the BPS (per the NERC FAC standards). Furthermore, all models should be updated after plant commissioning and checked to ensure that the model matches the as-built, plant-specific settings, controls, and behavior. Any modeling issues or performance issues identified by the TP and PC should be addressed as quickly as possible, reported to the TOP and RC, and corrective actions put in place in a timely manner.	

Table 1: Review of Disturbance Report Findings and Recommendations

#	Key Findings/Recommendation	IRPWG Follow-Up
	• **Dynamic Behavior of Solar PV during Faults:** Many facilities had a dynamic response to the fault events in this disturbance; however, multiple facilities exhibited dynamic behavior that does not meet the recommended performance specified in previously published NERC reliability guidelines.[5] Some solar PV facilities use legacy inverters that cannot make improvements to performance. Other facilities have relatively newer inverters where changes could be made but were not made prior to the faults, signifying a lack of action being taken by industry to incorporate the recommendations set forth. Some facilities with newer inverter technology were able to use current injection during the fault (eliminating momentary cessation) but required tens of seconds to return to predisturbance output; this is not a preferred behavior. Concerted focus should be made by NERC Compliance Monitoring and Enforcement Program (CMEP) to ensure all BES facilities are meeting the requirements set forth in NERC Reliability Standards including the latest version of PRC-024. ▪ **Recommendation (GO, GOP):** All existing solar PV facilities should review the recommendations in the NERC reliability guidelines and ensure that their equipment is configured to meet the recommendations set forth. Solar PV resources should eliminate the use of momentary cessation to the extent possible. If elimination is not possible, the	The recommendation made by NERC to focus CMEP activities on inverter tripping of BES resources will hopefully help improve the performance of existing resources not meeting the requirements of PRC-024. Further, the NERC reliability guidelines on recommended performance of BPS-connected inverter-based resources and improvements to interconnection requirements for these resources have been widely shared with industry. Hopefully industry is adopting the recommendations contained in these guidelines to address this issue for newly interconnecting resources. **Recommended Action from IRPWG Follow-Up:** No further action is needed by IRPWG; however, future efforts may consider assessing the extent to which industry has adopted the recommendations in the NERC guidelines regarding interconnection requirements improvements. This would help understand the extent to which these risks are being addressed by industry.

[5] https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Inverter-Based_Resource_Performance_Guideline.pdf
https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_IBR_Interconnection_Requirements_Improvements.pdf

Table 1: Review of Disturbance Report Findings and Recommendations

#	Key Findings/Recommendation	IRPWG Follow-Up
	momentary cessation settings should be configured (if possible) to minimize its use (lower voltage threshold) and return to predisturbance output within one second. If elimination is possible, other forms of current injection during fault ride-through (e.g., reactive current injection or some form of active and reactive current injection) should be used. ▪ **Recommendation (GO, GOP):** All existing solar PV facilities should review the recommendations in the NERC reliability guidelines and ensure that their equipment is configured to meet the recommendations set forth. Solar PV resources that use current injection should ensure that the inverter controls and plant-level controls are configured to allow the resource to return to predisturbance output (assuming no current limits are reached) within one second. Resources should not have a prolonged recovery of active power following a dynamic response to a fault event on the BPS. Plant-level ramp rates or other BA-imposed balancing ramp rates should not interfere with the resource returning to predisturbance output levels in a quick and stable manner after a BPS fault event. ▪ **Recommendation (TO):** TOs should ensure their interconnection requirements are clear regarding the dynamic performance requirements and settings for inverter-based resources. TOs are strongly encouraged to ensure resources are complying with these requirements and developing mitigation plans for any requirements that	

Table 1: Review of Disturbance Report Findings and Recommendations

#	Key Findings/Recommendation	IRPWG Follow-Up
	are not being met. In particular, these requirements should ensure clarity and consistency for post-fault recovery of active power following fault events. Furthermore, rise times and settling times should also be specified as well as any reactive current injection (e.g., “K-factor”) settings for large disturbance voltage support.	
	• **Settings Changes:** After coordinating with NERC and WECC on this disturbance analysis, a couple of solar PV facilities stated that they had made changes to equipment settings and performance to improve the dynamic response to fault events. This includes eliminating momentary cessation in favor of reactive current injection and some improvements to momentary cessation or active power recovery rates to be more aligned with the recommendations in the NERC reliability guidelines. ▪ **Recommendation (TO):** All GOs of solar PV facilities, and other BPS-connected inverter-based resources, should review these key findings and recommendations as well as those listed in Chapter 2 [of disturbance report] and ensure their resources are configured to provide the best dynamic response to support BPS reliability. GOs should consult the NERC reliability guidelines as well as their BA, RC, TP, and PC if they have any questions regarding recommended performance.	**Recommended Action from IRPWG Follow-Up:** No further action is needed by IRPWG.

Table 1: Review of Disturbance Report Findings and Recommendations

#	Key Findings/Recommendation	IRPWG Follow-Up
	• **Dynamic Model Accuracy:** NERC and WECC have previously identified[6] modeling issues in the interconnection-wide planning base cases, and modeling challenges continue to be an issue with industry. Discussions with GOs of solar PV facilities during this analysis have highlighted that changes to equipment may take place, but there is little to no emphasis put on getting TP or PC approval of these changes (as a material modification to the facility) prior to making them, nor on ensuring that the TP and PC receive updated dynamic models following those changes. NERC IRPWG has submitted a standard authorization request to modify FAC-002-2 to clarify the use of "material modification" in that standard. ▪ **Recommendation (GO, GOP):** GOs and GOPs should ensure that any changes to plant-level settings, inverter settings, or facility topologies or ratings should be articulated to the TP, PC, BA, and RC. Any applicable interconnection requirements, per FAC-001-3 and FAC-002-2, must be met prior to these changes being made to the facility, including restudy of these changes by the TP and PC. GOs and GOPs should coordinate with their TP and PC to determine if any changes within the facility are considered "material" and require any additional restudy. ▪ **Recommendation (TO, TP, PC, Industry):** TOs should ensure that their interconnection requirements are clear and any	IRPWG submitted a SAR regarding the "material modification" issue identified in the San Fernando disturbance (and other disturbances). The changes to FAC-002 will hopefully address the issues of changes being made to equipment prior to studies being conducted to ensure reliability of the BPS for those changes made. IRPWG has also recommended that interconnection requirements be updated to capture these modeling issues more directly. **Recommended Action from IRPWG Follow-Up:** No further action is needed by IRPWG.

[6] https://www.nerc.com/comm/PC/InverterBased%20Resource%20Performance%20Task%20Force%20IRPT/NERC-WECC_2020_IBR_Modeling_Report.pdf

Table 1: Review of Disturbance Report Findings and Recommendations		
#	Key Findings/Recommendation	IRPWG Follow-Up
	modifications to the facility that can or will change the electrical behavior of the facility (including any settings changes to inverters that affect its electrical output during steady-state or dynamic conditions) should be considered material and should be studied prior to those changes being made. TOs, TPs, and PCs should ensure that their processes for making these changes are timely and effective such that GOs are not discouraged from making these changes to support overall reliability of the BPS.	

Agenda Item 13
Reliability and Security
Technical Committee Meeting
June 8, 2021

IRPWG TPL-001-5 SAR for BPS-Connected Inverter-based Resources

Action

Endorse

Summary

Considering current trends, the NERC IRPWG undertook review of the TPL-001 standard for considering BPS-connected IBRs. This review is captured in the following RSTC-approved white paper:

- IRPTF/IRPWG: IRPTF Review of NERC Reliability Standards – March 2020 (here)
- This SAR proposes to update TPL-001-5.1 to address the issues identified in the white paper. The IRPWG is seeking endorsement of the SAR.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information	
SAR Title:	TPL-001-5.1 Transmission System Planning Performance Requirements
Date Submitted:	_/_/2021

SAR Requester			
Name:	Allen Schriver, NextEra Energy (NERC IRPWG Chair) Julia Matevosyan, ERCOT (NERC IRPWG Vice Chair)		
Organization:	NERC Inverter-Based Resource Performance Working Group (IRPWG)		
Telephone:	Al – 561-904-3234 Julia – 512-994-7914	Email:	Allen.Schriver@fpl.com Julia.Matevosyan@ercot.com

SAR Type (Check as many as apply)	
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)	
☐ Regulatory Initiation ☒ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan	☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified

Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):
Many areas of the North American bulk power system (BPS) continue to experience an increase in BPS-connected inverter-based resources (e.g., wind, solar photovoltaic (PV), battery energy storage systems (BESS), and hybrid power plants). NERC Reliability Standard TPL-001-5.1 is a foundational standard used for “establishing transmission system performance requirements within the planning horizon to develop a bulk electric system (BES) that will operate reliably over a broad spectrum of system conditions and following a wide range of probable contingencies.” Transmission Planners (TPs) and Planning Coordinators (PCs) develop and use models of the electrical grid to perform planning assessments (e.g., steady-state, dynamic, and short-circuit) to develop corrective action plans for future reliability issues identified. Ensuring that the TPL-001 standard is reflective of the evolving nature of the BPS and its resource mix is paramount to ensuring reliable operation and resilience of the BPS moving forward.

Requested information

The NERC Inverter-Based Resource Performance Task Force (IRPTF)[1] undertook a complete review of the NERC Reliability Standards in the context of increasing levels of BPS-connected inverter-based resources and published a white paper on the outcomes and recommendations of this review in March 2020.[2] The review was approved by the NERC Planning Committee and served as the technical justification for future standards revision efforts. The white paper recommended modifications to seven standards, and IRPWG presented four SARs to the NERC Reliability and Security Technical Committee (RSTC) in _____ that addressed the deficiencies identified in six of the seven standards.

Based on the outcome of the review, it was determined that the TPL-001-4/5[3] needed clarifications "to address terminology throughout the standard that is unclear with regards to inverter-based resources" the next time the standard is revised. The language used in the white paper regarding "the next time the standard is revised" was based on the understanding that the NERC System Planning Impacts from Distributed Energy Resources Working Group (SPIDERWG) was developing a SAR and that the recommended modifications to TPL-001-5 from IRPWG could be included in the SPIDERWG SAR. The combined SAR was presented to the NERC RSTC at their March 2021 meeting and was rejected. The overarching comments received were with regards to the DER-related issues and a comment was made that the recommendations pertaining to BPS-connected inverter-based resources were not the primary focus of concern.

Therefore, IRPWG presents this SAR to move the effort forward regarding specifically BPS-connected inverter-based resources. This SAR does not include any modification to TPL-001-5 regarding the inclusion of distributed energy resources (DERs). IRPWG believes that industry needs to be proactive in addressing standards gaps, particularly, where lack of clarity and confusion may lead to studies not adequately capturing possible BPS reliability issues. As the North American BPS continues to experience rising penetration levels of BPS-connected inverter-based resources and is likely to do so into the foreseeable future, these changes are critical for overall BPS reliability and industry efforts to reliably integrate these resources.

Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):

This SAR revises requirements within the TPL-001-5 standard to provide clarity and consistency for how BPS-connected inverter-based resources are considered, modeled, and studied in planning assessments. The proposed revisions to TPL-001-5 will ensure industry is effectively and efficiently conducting planning assessments and that the requirements are equally suitable for inverter-based resources as they are for synchronous generation.

[1] The IRPTF has subsequently become the IRPWG under the NERC Reliability and Security Technical Committee (RSTC).

[2] NERC IRPTF, "IRPTF Review of NERC Reliability Standards," March 2020: https://www.nerc.com/comm/PC/InverterBased%20Resource%20Performance%20Task%20Force%20IRPT/Review_of_NERC_Reliability_Standards_White_Paper.pdf

[3] At the time of review, the TPL-001-5 standard had just recently been approved by FERC and was yet to be subject to enforcement.

Requested information

Project Scope (Define the parameters of the proposed project):

As described in further detail below, the scope of this project includes the following revisions to TPL-001-5.1:

- Modify Requirements 3.3 and 4.3 and their applicable sub-requirements to make the term “GSU transformer” suitable for all generation types since it introduces confusion for BPS-connected inverter-based resources
- Modify Requirements 4.1.1 and 4.1.2 regarding the use of the term “pulls out of synchronism,” which is only applicable for synchronous generator technologies and is not suitable for BPS-connected inverter-based resources
- Modify Requirement 4.3.2 so that the list of devices that impact the study area are inclusive of BPS-connected inverter-based resource technologies
- Modify other Requirements, if necessary as deemed appropriate by the Standard Drafting Team, regarding the aforementioned issues if the IRPTF review missed any other related issues

Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[4] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):

The following detailed description is copied verbatim from the IRPTF white paper that was approved by the NERC PC:

> TPL-001-4 requires Planning Coordinators (PCs) and TPs to assess the reliability of their portion of the BES for various conditions across several specified future years and to plan Corrective Action Plans to address identified performance deficiencies. The requirements and sub-requirements include, among other things, certain simulation assumptions to be used by the planner and performance requirements.
>
> Sub-requirements 3.3 and 4.3 describe simulation assumptions that the planner should use when performing contingency analysis for the steady-state and stability portion of the assessment, respectively. Sub-requirements 3.3.1.1 and 4.3.1.2 each require the planner to include the impact of the “tripping of generators where simulations show generator bus voltages or high side of the [GSU] voltages are less than known or assumed generator” low voltage ride-through capability.
>
> The term GSU transformer can be confusing to GOs of IBR facilities because they will often refer to the transformer that steps the voltage up from the individual inverter (e.g., 600 V) to the collector system voltage (e.g., 34.5 kV). In this case, there is usually another transformer (i.e., the main power transformer (MPT)) to step the voltage up from the collector system voltage to

[4] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
transmission system voltage. It was likely the intent of the TPL-001-2 SDT to be referring to transmission system voltages when drafting the language that refers to known or assumed generator low voltage ride-through capability at the high-side of the GSU. Therefore, the language in these sub-requirements should be modified to provide clarity for inverter-based resources. Sub-requirements 4.1.1 and 4.1.2 provide stability performance criteria when a generator “pulls out of synchronism” in system simulations. Although an inverter-based resource does synchronize with the grid, the phrase “pulls out of synchronism” is typically applicable only to synchronous generators, referring to when a synchronous machine has an angular separation from the rest of the grid. Therefore, these sub-requirements could be clarified by clearly stating that this performance criteria is for synchronous generators. Sub-requirement 4.3.2 specifies that stability studies must “simulate the expected automatic operation of existing and planned devices designed to provide dynamic control of electrical system quantities when such devices impact the study area.” It then contains a list of example devices that have dynamic behavior. Not included in this list are power plant controllers and inverter controls, which often dominate the dynamic response of IBRs. While the sub-requirement does not preclude the simulation of plant-level controllers and inverter controls, it would add clarity if they were added to the list. The suggested clarifications for sub-requirements 3.3, 4.3, 4.1.1, 4.1.2, and 4.3.2 should be considered by a future SDT when editing the standard. However, the IRPTF does not believe the clarifications by themselves warrant changing the standard at this time. It should be noted that the identified issues with TPL-001-4 also apply to the draft TPL-001-5 standard that is awaiting FERC approval as of the publication of this whitepaper.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
The cost impacts for the proposed changes to TPL-001-5 are expected to be minimal. The changes being proposed are clarifications that will bring consistency and effectiveness industry related to how planning assessments are conducted and how planning engineers set up and conduct those assessments.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
None. This SAR will impact Transmission System Planning Assessments, not any specific BES facilities.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission

Requested information

Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):

Planning Coordinators, Transmission Planners, and Generator Owners of inverter-based resources

Do you know of any consensus building activities[5] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.

This SAR is an outcome of the white paper produced by the NERC IRPTF and approved by the NERC PC, which can be found here: https://www.nerc.com/comm/PC/InverterBased%20Resource%20Performance%20Task%20Force%20IRPT/Review_of_NERC_Reliability_Standards_White_Paper.pdf

The SAR is a follow-on to the recommendation contained within the white paper, developed by the NERC IRPWG under the NERC RSTC.

Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?

No

Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

The NERC IRPWG (previously IRPTF) has published multiple technical reference documents, white papers, and reliability guidelines related to the performance, modeling, and studies of BPS-connected inverter-based resources. These technical materials are used widely by industry and have provided significant value for improving planning practices. However, those efforts do not address the larger issue related to the TPL-001 standards language being written predominantly for synchronous generation technology and not adequately considering or clarifying how the requirements relate to BPS-connected inverter-based resource technologies.

Reliability Principles

Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.

☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☒	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

[5] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information	
□	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
□	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
□	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
□	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
□	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
None	None

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
□ Draft SAR reviewed by NERC Staff □ Draft SAR presented to SC for acceptance □ DRAFT SAR approved for posting by the SC	□ Final SAR endorsed by the SC □ SAR assigned a Standards Project by NERC □ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Agenda Item 14
Reliability and Security
Technical Committee Meeting
June 8, 2021

Generating Availability Data System (GADS) Data Request for Utility-Scale Solar Plants and Updates for GADS Wind and Conventional GADS

Action

Accept to post for a 45-day comment period.

Background

NERC has required reporting of conventional generation inventory, performance, and event data since 2012. In 2015, NERC issued a Section 1600 data request to expand the collection of GADS data to include wind generation. Reporting of wind generation data became mandatory in 2018 with a phased-in approach; in 2020, the final phase of wind plants began reporting. The increasing penetration of solar generation has prompted the need for NERC to have information about utility-scale solar facilities whose operation may impact the bulk electric system.

In 2018, NERC and the GADS Working Group (now the GADS User Group) began developing data reporting requirements for utility-scale solar facilities and connected energy storage at the plant. During the development of the data reporting requirements for solar facilities, gaps in the reporting requirements for wind reporting were identified, namely event reporting and connected energy storage at the plant. The expansion of data requirements for GADS Wind will improve NERC's ability to evaluate performance of renewable and conventional generation and provide comparable reporting requirements for both wind and utility-scale solar generation.

Conventional GADS reporting of design data is currently limited to basic location information, (i.e., address details) and the Energy Information Administration code. This limits NERC's ability to conduct detailed analysis to evaluate whether certain types of unit configurations or key operating components are impacted by operating conditions such as extreme weather. As part of the modifications being requested in this GADS Data Request, NERC and the GADS User Group propose to modify conventional GADS reporting to include limited design data by unit type and add a Contributing Operating Condition field.

Per NERC Rules of Procedure, NERC has notified FERC and will post the GADS Data Request for a 45-day stakeholder comment period. NERC staff and the GADS User Group will review the comments received and make appropriate revisions. Following the public comment period, the GADS Data Request will be provided to the RSTC for endorsement and recommendation to the NERC Board of Trustees for approval in the second half of 2021.

Agenda Item 15
Reliability and Security Technical
Committee Meeting
June 8, 2021

2021 State of Reliability Report

Action
Information

Background
The State of Reliability Report (SOR) is prepared annually to provide objective, credible, and concise information to policy makers, industry leaders, and the NERC Board of Trustees (Board) on issues affecting the reliability and resilience of the North America bulk power system (BPS). Specifically, the report:

- Identifies system performance trends and emerging reliability risks,
- Determines the relative health of the interconnected system, and
- Measures the success of mitigation activities deployed.

The key findings and recommendations of the report serve as the technical foundation for NERC's range of risk-informed efforts addressing reliability performance and serve as key inputs to the ERO Reliability Risk Priorities Report prepared by the Reliability Issues Steering Committee (RISC). The metrics measured in the report address the characteristics of an adequate level of reliability (ALR).

In developing the 2021 SOR, NERC staff and the Performance Analysis Subcommittee continue to tailor content for the policy maker and industry leader audience. NERC management expects to issue the 2021 SOR in August. The review schedule below identifies key milestones for the report.

2021 State of Reliability Report Schedule	
Date	**Description**
June 8 - 9	Webinar presentation to the Reliability and Security Technical Committee
June 22	Comments due from the Reliability and Security Technical Committee members
July 7	Electronic voting begins by the Reliability and Security Technical Committee for acceptance
July 29	Report sent to NERC Board of Trustees and MRC for review
August 12	Report presented to NERC Board of Trustees for acceptance
August 13	Report release (Target)

Agenda Item 16
Reliability and Security
Technical Committee Meeting
June 8, 2021

Vice Chair Election

Action

Approve

Summary

Due to a member resignation, the RSTC's Nominating Subcommittee (NS) held a nomination period to fill the RSTC Vice Chair role. Per the RSTC Charter, *"The NS proposes chair and vice-chair candidates. The full RSTC will elect the chair and vice chair. The chair and vice chair shall not be from the same sector. The elected chair and vice chair are approved by the NERC Board."* Once approved by the NERC Board, the elected member will complete the remainder of the term for the vacated seat. The NS reviewed the nominees during a May 24, 2021 conference call and recommends Rich Hydzik (Avista) to be elected as the RSTC Vice Chair.