NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Risk Elements Guide for Development of the 2015 CMEP IP

September 8, 2014

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road N
Suite 600, North Tow
Atlanta, GA 3032
404-446-2560 | www.nerc.co

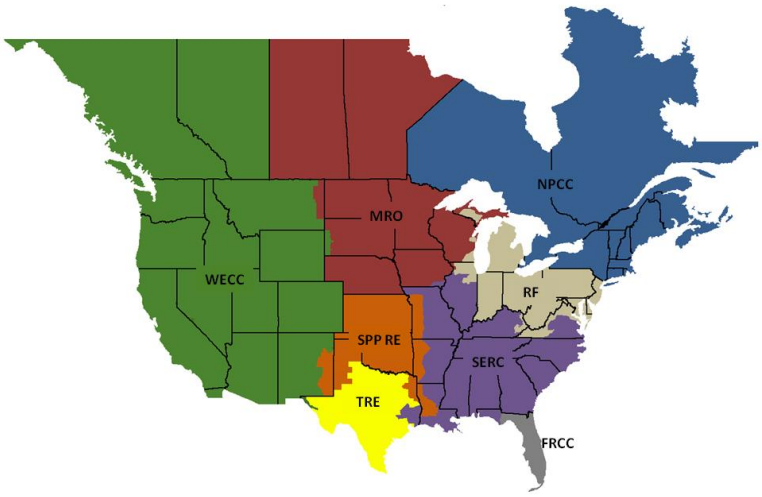
Table of Contents

Preface

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

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

The ERO Enterprise is comprised of NERC and the eight REs.



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

Risk Elements Development Process

The ERO Enterprise has always assessed risks to the reliability of the BPS, as well as mitigating factors that may reduce or eliminate a given reliability risk, and the ERO Enterprise will continue to do so in 2015 and beyond.

The purpose of the Risk Elements Guide is to outline the process by which NERC will identify continent-wide risks to the reliability of the BPS, as well the Reliability Standards and registration functional categories related to those risks. This information will be used to develop the annual ERO Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan (Implementation Plan).[1] The annual Implementation Plan, in turn, will provide guidance to Regional Entities on identifying regional risks which will then be reflected in the Regional Entity Implementation Plans.[2] The process of identifying risk elements, described below, replaces the existing processes for developing the Implementation Plan and the Actively Monitored List (AML). The new approach to the Implementation Plan will provide input to a more individualized compliance oversight plan for registered entities. The transformation to focus on identifying and prioritizing risks replaces a static, one-size-fits-all list of Reliability Standards and prioritizes functions and Reliability Standards based on risk to determine the appropriate oversight method.

NERC annually identifies and prioritizes risks to reliability of the BPS, taking into account compliance findings and event analysis experiences, data analysis provided in several NERC publications and reports, and expert judgment of ERO Enterprise staff, committees and subcommittees. Each year, NERC compliance assurance staff, with input from other departments at NERC and the Regional Entities, will execute the following process to identify risk elements and select specific requirements from the Reliability Standards for increased focus. The results of this process will be reflected in Implementation Plan and will also guide the development of the Regional Entity Implementation Plans.

The risks identified through this process do not constitute the entirety of the risks that may affect the reliability of the BPS. Regional Entities are expected to consider local risks and specific circumstances associated with individual registered entities within their footprint in developing their compliance oversight plans.

1. Between May and August of each year, NERC staff will collect the ERO Enterprise data, reports and publications, available at the time, that identify reliability risks. Examples of such data and reports include the State of Reliability Report, the Long-Term Reliability Assessment, publications from the Reliability Issues Steering Committee (RISC), special assessments or reports, the ERO Enterprise Strategic Plan, ERO Event Analysis Process insights, significant occurrences noted by NERC and Regional Entity Situation Awareness staffs, and other relevant documents pertaining to risks to the reliability of the BPS.
2. Beginning in August, NERC staff will review those reports to develop a matrix and prioritize reliability risks. This risk prioritization will be informed by facts and circumstances, but will consider, among other factors, the sources of the risk, how many different sources identified the same risk, and the level of analysis that supports the assertion that the risk merits action.
3. NERC staff will then identify the effective body of Reliability Standards for the relevant year that are related to those reliability risks. NERC staff will note those risks that are not addressed or mitigated by existing Reliability Standards as potentially requiring further analysis, consideration and potential action in other areas of ERO Enterprise operations.

[1] CMEP (Appendix 4C to the Rules of Procedure) § 4.1. See also Rules of Procedure § 401.6.

[2] CMEP (Appendix 4C to the Rules of Procedure) § 4.2.

4. From the set of identified reliability risks, NERC staff will select a sub-set of risks for additional focus based on the significance of each risk and the existence of NERC's Reliability Standards to help manage the risk. This subset should generally include between 3 and 10 reliability risks.
5. From the set of Reliability Standards related to the subset of risks, NERC staff will identify the specific Requirements related to their management of risk. In the case of emerging or newly identified risks, such Requirements may not exist. As mentioned earlier, these risks, if relevant for the upcoming year, will be referred to other areas of ERO Enterprise operations for consideration.
6. From that set of Requirements, NERC staff will consider the following additional factors and remove those Requirements that are not appropriate for additional focus:
    a. Is the Requirement appropriate for proactive compliance activities? For example, a Requirement that states: "When experiencing an IROL exceedance, the registered entity shall not allow the exceedance to last more than 30 minutes" could only be observable in real time, and could not be validated unless an IROL exceedance occurred. Such a Requirement would be better evaluated with a more reactive compliance monitoring approach (self-reports, investigations, etc…). However, a Requirement that states, "Entities shall monitor IROLs and have written processes for managing IROL exceedances that can reasonable ensure the exceedance last no more than 30 minutes" is preventative in nature, occurs ahead of time, and can easily be verified proactively.
    b. Does the Requirement contribute strongly to reliability? One way to evaluate this is to consider the FERC-approved Violation Risk Factor (VRF) of the Requirement. Though VRFs are not the sole criterion to measure risks to reliability, in general, Low-VRF requirements are not good candidates for increased focus, while High-VRF Requirements typically merit consideration.
    c. Have the Requirements and associated Reliability Standards been identified through compliance data analysis as having moderate or significant impacts on BPS reliability when violated?
7. NERC staff also will review the functional entities to which the remaining Requirements apply. Are some functions more important to reliability with regard to a specific Requirement than others? NERC staff will then remove functions from consideration for Requirements as appropriate.
8. Finally, NERC staff will consider the resulting set of Requirements and functional entities and whether additional guidance should be provided to CEAs to assist in their evaluation of an entity's compliance with the Requirement.

By September of each year, NERC staff will take the results of the steps described above and include such results in that year's Implementation Plan. The Implementation Plan will be posted on or about September 1 of each year.[3]

Regional Entity Implementation Plans should take into account the most important reliability risks within a given Regional Entity footprint and initiate plans for managing them through appropriate elements of the compliance assurance process. These may include, but are not limited to, the risk elements identified in the Implementation Plan, regional risks identified by the Regional Entity, or a combination of both. The Regional Entity Implementation Plan should explain how it identified the risks in a particular Regional Entity footprint, including reasons why risk elements identified in the ERO CMEP IP are not included. Not all risks identified in the Implementation Plan need to be monitored with respect to each entity registered for a particular function.

Regional Entity Implementation Plans are provided to NERC staff on or about October 1. Regional Entity Implementation Plans are subject to review and approval by NERC.[4]

[3] CMEP (Appendix 4C to the Rules of Procedure) § 4.1.

Following the development of the Regional Entity Implementation Plan, Regional Entities, through the Inherent Risk Assessment process, may add or remove Reliability Standards or Requirements for specific entities, and through the Internal Control Evaluation process will further tailor the Reliability Standards and Requirements for monitoring. The Regional Entity may use any of the available compliance and monitoring tools in assuring compliance of a given entity. Registered Entities are, as always, required to comply with all applicable Reliability Standards, whether or not they are scheduled to be monitored on that particular Reliability Standard.

An ERO Enterprise feedback loop from compliance assurance activities will help inform future priorities and projects in the NERC standards development process as well as other ERO Enterprise processes. This feedback loop will operate in areas where there may be gaps as well as areas in which Requirements should be retired. It is expected that the feedback loop will mature as more experience with the development and implementation of risk-based compliance monitoring methods is gained.

The following section provides an example of the application of this process for risks identified and reflected in the Implementation Plan.

[4] Rules of Procedure § 402 and CMEP (Appendix 4C to the Rules of Procedure) § 4.0.

Risk Elements for the 2015 Implementation Plan

Development

NERC began development of the 2015 Implementation Plan by reviewing selected data and reports. Those reports included the following:

- The ERO Enterprise Strategic Plan 2014-2017
- The ERO Top Priority Reliability Risks 2014-2017 report
- The ERO Priorities: RISC Updates and Recommendations report, dated July 26, 2013
- The 2013 Long-Term Reliability Assessment
- The State of Reliability 2014 report
- The Standards Independent Experts Review Project report, dated June 2013
- The Cyber Attack Task Force final report, dated May 9, 2012

NERC reviewed the risks described within these documents and evaluated them based on any indication of risk priority contained within the source reports as well as the prevalence of the concern across sources.

2015 Considerations	
• Issues identified as a significant risk to reliability by the Reliability Issues Steering Committee (RISC) and included in the ERO Priorities: RISC Updates and Recommendations report.	• Systemic issues identified as a significant risk to reliability by NERC and included in the ERO Top Priority Reliability Risks 2014-2017 report and ERO Enterprise Strategic Plan 2014-2017.
• Systemic issues identified as a significant risk to reliability by NERC Performance Analysis (based on data contained in GADS, TADS, Misoperations, outages) and included within the State of Reliability report.	• Systemic issues identified as a significant risk to reliability in the Standards Independent Experts Review Project report.
• Systemic issues identified as a significant risk to reliability by NERC Reliability Assessment and included within the Long-Term Reliability Assessment (LTRA).	• Systemic issues identified through compliance oversight activities.
• Systemic issues identified as a significant risk to reliability by enforcement (frequently violated with serious potential or actual consequences).	• System issues that could adversely affect situational awareness and cause or exacerbate BPS instability (Cyber Attack Task Force).

Figure 1. Summary of Criteria for Consideration

NERC identified those Reliability Standards related to managing the identified risks. Based on this review, NERC identified a number of risk elements for which it is requesting focus.

As noted above, Regional Entity Implementation Plans should take into account the most significant reliability risks within a given footprint and initiate plans for managing them through appropriate elements of the compliance assurance process. These may include, but are not limited to, the risk elements identified below and in the Implementation Plan, local risks identified by the Regional Entity, or a combination. The Regional Entity Implementation Plan should explain how it identified the risks in a particular Regional Entity footprint, including reasons why risk elements identified in the Implementation Plan are not included. Not all risk elements identified in the Implementation Plan need to be monitored with respect to each entity registered for a particular function.

2015 Risk Elements

The nine risk elements below are not a comprehensive list of all risks to the reliability of the BPS. Where issues are being addressed through other mechanisms, they are not included herein for compliance assurance activities.[5]

1. Infrastructure Maintenance

As the BPS continues to age, lack of infrastructure maintenance is a reliability risk that continues to grow in importance.

AC Substation Equipment Failures

As reported in the State of Reliability 2014 report, AC Substation Equipment Failures had the largest positive correlation with automatic transmission outage severity in 2013. The correlation is statistically significant: a pattern and underlying dependency exists between AC substation equipment failures and transmission outage severity. While it is unclear whether or not there is a relationship between substation equipment failures and maintenance, such a relationship may exist. The issue of AC Substation Equipment Failure is one that is still being investigated, and action plans to address this concern are being developed. Thus, the ERO CMEP IP may be updated during the year to reflect new activities based on NERC's investigation.

Aging Infrastructure

The general concern of Infrastructure Maintenance has been highlighted in other NERC documents. The 2013 Long-Term Reliability Assessment highlighted this area of concern, stating:

> Aging transmission system infrastructure has many challenges, such as the availability of spare parts, the obsolescence of older equipment, the ability to maintain equipment due to outage scheduling restrictions, and the ability to keep pace with technological advancements … Larger scale "infrastructure revitalization" may be necessary in the future; however, with older generation retiring throughout the next decade, the average age of BPS generation facilities will be relatively young. Implementation of any replacement strategy and in-depth training programs requires additional capital investment, engineering and design resources, and construction labor resources, all of which are in relatively short supply.

[5] For example, vegetation management and right-of-way clearances, while key priorities, are not areas of focus for compliance assurance activities because they are being addressed through other ongoing targeted initiatives.

Areas of Focus

Table 1 – Infrastructure Maintenance		
Standard	**Requirements**	**Entities for Attention**
PRC-005-2	R3, R4	Generator Owners Transmission Owners Distribution Provider
PRC-008-0	R1, R2	Distribution Providers Transmission Owners
PRC-011-0	R1	Distribution Providers Transmission Owners
PRC-017-0	R1	Distribution Providers Generator Owners Transmission Owners

2. Uncoordinated Protection Systems

Protection systems that trip unnecessarily can contribute significantly to the extent of an event. When protection systems are not coordinated properly, the order of execution can result in either incorrect elements being removed from service or more elements being removed than necessary. This can also occur with Special Protection Systems, Remedial Action Schemes, and Underfrequency Load Shedding and Undervoltage Load Shedding schemes. Such coordination errors occurred in the September 8, 2011 event (see recommendation 19)[6] and the August 14, 2003 event (see recommendation 21).[7] Both the RISC's ERO Priorities: RISC Updates and Recommendations report and NERC's ERO Top Priority Reliability Risks 2014-2017 report recognize protection systems as a significant risk based on the extensive work and detailed analysis contained in the State of Reliability reports from 2012 and 2013.

Areas of Focus

Table 2 – Uncoordinated Protection Systems		
Standard	**Requirements**	**Entities for Attention**
PRC-001-1.1	R3, R5	Generator Operator Transmission Operator
	R4	Transmission Operator

3. Protection System Misoperations

Protection systems are designed to remove equipment from service to avoid damage to equipment when a fault occurs. A protection system that does not trip or is slow to trip may lead to the damage of equipment (which may result in degraded reliability for an extended period of time), while a protection system that trips when it should not can remove important elements of the power system from service at times when they are needed most. Unnecessary trips can even start cascading failures as each successive trip can cause another protection system to trip.

NERC's 2012 and 2013 State of Reliability Reports identified protection system misoperations as a significant threat to BPS reliability. Additional activities are needed to ensure this risk is managed adequately.

Key Finding 3 of NERC's State of Reliability 2014 report was based on the continuing history of misoperations being a significant contributor to events. The report notes:

[6] See Arizona-Southern California Outages on September 8, 2011.

[7] See Final Report on the August 14, 2003 Blackout.

> In 2013, there were 71 transmission-related system disturbances that resulted in a NERC Event Analysis reported event. Of those 71 events, 47 (about 66 percent) had associated misoperations. Of these 47 events, 38 (about 81 percent) experienced misoperations that were contributory to or exacerbated the severity of the event. In several cases, multiple misoperations occurred during a single disturbance. Cause coding has not yet been completed for all 2013 events, but it is estimated that there were 60–75 misoperations associated with these 38 reportable events. Therefore, out of approximately 2,000 total misoperations in 2013, approximately 3.0 to 3.5 percent were causal to or exacerbated by the severity of reportable system disturbances.

Both the RISC's ERO Priorities: RISC Updates and Recommendations report and NERC's ERO Top Priority Reliability Risks 2014-2017 report recognize protection systems and their failures as a significant risk based on the extensive work and detailed analysis contained in the State of Reliability reports from 2012 and 2013.

Areas of Focus

Table 3 – Protection System Misoperations

Standard	Requirements	Entities for Attention
PRC-004-2.1a	R1.	Transmission Owner Distribution Provider
	R2.	Generator Owner
PRC-016-0.1	R1, R2	Transmission Owner Generator Owner Distribution Provider
PRC-023-3[8]	R1.	Transmission Owner Generator Owner Distribution Provider
PRC-025-1	R1	Transmission Owner Generator Owner Distribution Provider

4. Workforce Capability

A lack of knowledge, experience, and capabilities is a common threat in any industry that relies on skilled workers. The RISC, in its ERO Priorities: RISC Updates and Recommendations report, highlighted Workforce Capability and Human Error as a priority area needing focus. Findings of the RISC focused around the need to improve organizational performance and culture to ensure support for the individual worker to gain knowledge and address known issues in advance of their reoccurrence. This is also reflected in NERC's ERO Top Priority Reliability Risks 2014-2017 report.

NERC has also identified the challenge of maintaining a robust and knowledgeable workforce for a number of years. In the 2013 Long-Term Reliability Assessment, NERC notes, "Workers entering the power industry will be tasked with understanding and implementing a variety of new technologies and smarter systems and devices. Across the industry, there is substantial interest in training and hiring workers to support these industry needs as well as transferring the expertise and knowledge of retiring workers."

[8] Reliability Standard PRC-023-3 is effective October 1, 2014. However, PRC-023-2 remains relevant as Criterion 6 of Requirement R1 will remain in effect until PRC-025-1 is fully implemented pursuant to its phased in implementation plan.

Areas of Focus

Table 4 – Workforce Capability		
Standard	**Requirements**	**Entities for Attention**
CIP-004-3a	R1, R2	Balancing Authority Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
EOP-001-2.1b	R2, R3 R4	Transmission Operator Balancing Authority
EOP-003-2	R8.	Transmission Operator Balancing Authority
EOP-005-2	R10.	Transmission Operator
	R11.	Transmission Operator Transmission Owner Distribution Provider
	R17.	Generator Operator
EOP-006-2	R9, R10	Reliability Coordinator
PER-005-1	R3.	Reliability Coordinator Balancing Authority Transmission Operator
TOP-004-2	R6	Transmission Operator

5. Monitoring and Situational Awareness

Without the right tools and data, operators can make uninformed decisions which may or may not be appropriate to ensure reliability for the given state of the system. NERC's ERO Top Priority Reliability Risks 2014-2017 notes that "stale" data and lack of analysis capabilities contributed the 2003 and 2011 events. Certain essential functional capabilities must be in place, with up-to-date information, available for use on a regular basis, and utilized by staff to make informed decisions.

An essential component of Monitoring and Situational Awareness is the availability of information when needed. Unexpected outages of tools, or planned outages without appropriate coordination or oversight, can leave operators without visibility to some or all of the system they operate. While failure of a decision-support tool is rarely the cause of an event, such failures manifest as latent risk that further hinders the decision-making capabilities of the operator. One clear example of this is the August 14, 2003 event.

NERC has analyzed data and identified that outages of tools and monitoring systems are fairly common occurrences. The RISC's ERO Priorities: RISC Updates and Recommendations report, NERC's ERO Top Priority Reliability Risks 2014-2017 report, and the Cyber Attack Task Force final report recognize this concern.

Areas of Focus

Table 5 – Monitoring and Situational Awareness		
Standard	**Requirements**	**Entities for Attention**
EOP-010-1[9]	R2	Reliability Coordinator
IRO-002-2	R6, R7, R8	Reliability Coordinator
IRO-005-3.1a	R1	Reliability Coordinator
IRO-008-1	R1, R2	Reliability Coordinator
IRO-014-1	R1	Reliability Coordinator
PRC-001-1.1	R6	Transmission Operator Balancing Authority
TOP-002-2.1b	R4, R19	Transmission Operator Balancing Authority

[9] EOP-010-1 becomes effective on April 1, 2015. Pursuant to the implementation plan, Requirement 2 of EOP-010-1 will become effective on the first day following the retirement of IRO-005-3.1a.

Table 5 – Monitoring and Situational Awareness		
Standard	**Requirements**	**Entities for Attention**
	R11	Transmission Operator
TOP-006-2	R2	Reliability Coordinator Transmission Operator Balancing Authority
TOP-008-1	R4	Transmission Operator
FAC-011-2	R1, R2, R3	Reliability Coordinator
FAC-014-2	R5, R6	Reliability Coordinator Planning Authority Transmission Planner Transmission Operator

6. Long Term Planning and System Analysis

Long term planning and system analysis is related to several other areas (such as increased use of DSM, integration of variable generation, changes in load and system behavior, Smart Grid, increased dependence on natural gas, fossil requirements and retrofit outage coordination, nuclear generation retirements and outages, and resource planning). Long-term planning and analysis have been highlighted as a concern in RISC's ERO Priorities: RISC Updates and Recommendations report, and in NERC's ERO Top Priority Reliability Risks 2014-2017 report.

Areas of Focus

Table 6 – Long Term Planning and System Analysis		
Standard	**Requirements**	**Entities for Attention**
TPL-001-0.1[10]	R1.	Planning Authority Transmission Planner

7. Threats to Cyber Systems

Threats to cyber systems remain an area of significant importance. The need for attention in this area is addressed in the 2013 Long-Term Reliability Assessment report, in the RISC's ERO Priorities: RISC Updates and Recommendations report, the Cyber Attack Task Force final report, and in NERC's ERO Top Priority Reliability Risks 2014-2017 report. The risk includes threats and vulnerabilities that result from compromise of technology or communications that support the reliable operations of the BPS.

Areas of Focus[11]

Table 7 – Cyber Security		
Standard	**Requirements**	**Entities for Attention**
CIP-002-3	R2, R3	Balancing Authority Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner

[10] The effective date of TPL-001-4 is January 1, 2015. However, as a result of the phased implementation plan, earlier versions of the TPL Reliability Standards are referenced here.

[11] While Table 7 lists the CIP version 3 Reliability Standards (as those are currently enforceable), the ERO, through release of its Cyber Security Reliability Standards CIP V5 Transition Guidance, actively encourages and supports registered entities transitioning from compliance with the version 3 Reliability Standards directly to the version 5 Reliability Standards. As stated in that guidance, NERC and the Regional Entities will take a flexible compliance monitoring and enforcement approach for the CIP Reliability Standards, recognizing that the details of implementing a version 3 to version 5 transition may cause a significant impact on certain compliance monitoring activities.

Table 7 – Cyber Security		
Standard	**Requirements**	**Entities for Attention**
CIP-003-3	R4, R6	Balancing Authority Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
CIP-004-3a	R3, R4	Balancing Authority Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
CIP-005-3a	R1, R4	Balancing Authority Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
CIP-006-3	R1, R4, R5	Balancing Authority Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
CIP-007-3a	R1, R2, R4, R6, R8	Balancing Authority Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
CIP-009-3	R1, R2	Balancing Authority Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner

8. Human Error

Human Error remains a key focus for the ERO Enterprise. Included in this subset are communication errors which can pose a significant potential risk to BPS reliability. Human Error was identified as a key issue by both the RISC in its ERO Priorities: RISC Updates and Recommendations report and by NERC in its ERO Top Priority Reliability Risks 2014-2017 report.

Areas of Focus

Table 8 – Human Error		
Standard	**Requirements**	**Entities for Attention**
COM-002-2	R2.	Reliability Coordinator Transmission Operator Balancing Authority

9. Extreme Physical Events

Extreme Physical Events are those events that result in extensive damage to equipment, irrespective of cause. Such events could include earthquake, GMD events, high wind, flooding, physical attack, or sabotage. NERC identified this concern as a significant risk in its ERO Top Priority Reliability Risks 2014-2017 report. As concluded in the report, risk avoidance is insufficient to manage this risk, and additional focus must be given to those things that focus on resiliency and recovery.

Risk mitigation efforts (reducing the potential consequence) are underway, but additional focus is needed to address and minimize both the magnitude and duration of the consequences of an extreme physical event.

Areas of Focus[12]

Table 9 – Extreme Physical Events

Standard	Requirements	Entities for Attention
EOP-002-3.1	R6, R7, R8	Balancing Authority Reliability Coordinator
EOP-004-2	R2	Reliability Coordinator Balancing Authority Transmission Owner Transmission Operator Generator Owner Generator Operator
EOP-005-2	R1, R6	Transmission Operator
EOP-005-2	R9.	Transmission Operator
EOP-006-2	R1.	Reliability Coordinator
EOP-008-1	R3	Reliability Coordinator
EOP-008-1	R4	Balancing Authority Transmission Operator
EOP-010-1	R1.	Reliability Coordinator
	R3.	Transmission Operator
TPL-002-0b	R1.	Planning Authority Transmission Planner
TPL-003-0b	R1.	Planning Authority Transmission Planner
TPL-004-0a	R1.	Planning Authority Transmission Planner

The risk elements referenced above will be included in the Implementation Plan. The Implementation Plan will be posted on September 8, 2014. As noted above, these risk elements and other information contained in the Implementation Plan should be used by Regional Entities in the development of the Regional Entity Implementation Plans.

[12] CIP-014-1 – Physical Security also addresses extreme physical events, but it is not yet FERC-approved. Table 9 may be modified to reflect the requirements of CIP-014-1 following such approval.