NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

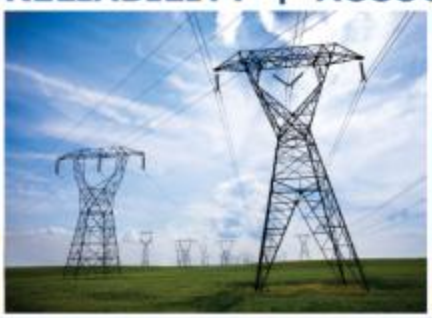
ERO Priorities

RISC Updates and Recommendations

July 26, 2013

RELIABILITY | ACCOUNTABILITY






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

Table of Contents

Introduction

Summary of Recommendations

Following additional analysis since the presentation of its February 2013 report to the Board of Trustees (Board), the Reliability Issues Steering Committee (RISC) makes the additional following recommendations:

1. Continue collaboration between NERC, the RISC, and Standing Committee leadership to develop a data-driven reliability risk strategy development process that integrates with overall electric reliability organization (ERO) planning (currently being developed as the "Reliability Risk Control Process").
2. Continue existing NERC efforts to control the risk associated with the high- and medium-priority issues, as the efforts are well aligned and appropriately scoped relative to the priorities assigned.
3. Continue collaboration between NERC and the Technical Committees to develop measures for use in determining the success and ongoing performance of those existing risk control efforts.
4. A new high-priority issue based on consolidating several other related issues (entitled "Adaptation and Planning for Change") should be processed through the post-prioritization steps of the "Reliability Risk Control Process."
5. Additionally, the set of issues contained in "Operational Modeling and Model Inputs" should also be processed through the post-prioritization steps of the "Reliability Risk Control Process."

Background

The RISC is an advisory committee that reports directly to the Board and triages and provides front-end, high-level leadership and accountability for issues of strategic importance to Bulk-Power System (BPS) reliability. The RISC assists the Board, NERC standing committees, NERC staff, regulators, Regional Entities, and industry stakeholders in establishing a common understanding of the scope, priority, and goals to develop solutions to address these issues. In doing so, the RISC provides a framework for steering, developing, formalizing, and organizing recommendations to help NERC and the industry effectively focus their resources on the critical issues needed to best improve the reliability of the BPS. Benefits of the RISC include improved efficiency of the NERC standards program. In some cases, that includes recommending reliability solutions other than the development of new or revised standards and offering high-level stakeholder leadership engagement and input on issues that enter the standards process.

To carry out its responsibility to help NERC and the industry focus resources on the most critical issues, the RISC completed an initial assessment of all ongoing efforts at NERC and made a set of recommendation to the Board in February 2013. In that recommendation, the RISC identified for further study four high-priority areas and five medium-priority areas.

After review and discussion of the initial RISC report, the Board adopted the following resolutions:

> **RESOLVED**, that the Board hereby accepts the report of the Reliability Issues Steering Committee (RISC), expresses its appreciation to the RISC for the excellent report, and endorses continued work by the RISC on a gap analysis on the high-priority and then the medium-priority issues and requests continued reports to the Board.
>
> **FURTHER RESOLVED**, that the Board hereby directs NERC management to continue to work with the RISC to consider how the priority rankings should be reflected in the development of the ERO's business plan and in the work plans of NERC committees.
>
> **FURTHER RESOLVED**, the Board hereby directs NERC management to work with the RISC and, as appropriate, NERC committee leadership to consider how NERC should utilize a data-driven reliability strategy development process that integrates with budget development and overall ERO planning (e.g., Standing Committee planning, department, and employee goal-setting).

The following is an update on the progress made with respect to these resolutions. Similar to its Feburary 2013 report to the Board, the RISC has based these estimates of risk primarily on the expert judgment of its members and that of NERC's staff and stakeholder subject matter experts. This is based on the maturity of the ERO's process for analyzing and developing interventions related to relaiblity risk, as shown in Figure 1. While "expert judgment" is invaluable, as the

process matures, the RISC continues to recommend that NERC focus on data collection and clear problem definition, as well as defining success and developing metrics for all projects going forward. With mature data collection and management for decision support, as well as formal decision-making processes, expert judgment can more effectively be used in the analysis of performance and project effectiveness.

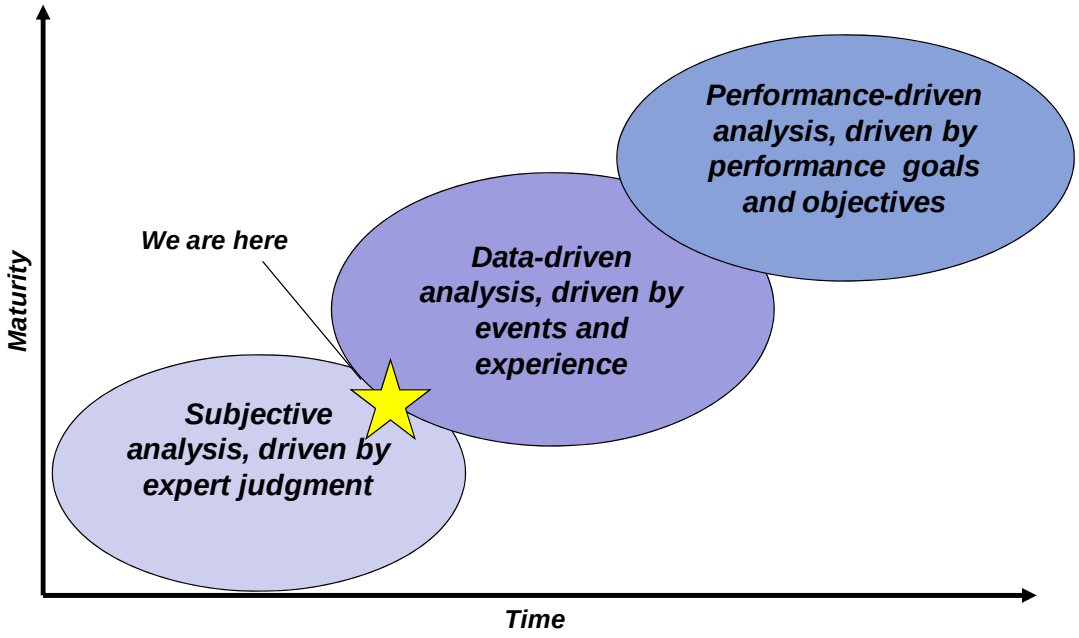


Figure 1: ERO Analysis and Intervention Maturity

Gap Analysis Activities

Following the February Board meeting, the RISC immediately began working with NERC staff to perform a gap analysis on each of the high- and medium-priority issues. The gap analyses included the following considerations:

- Are the existing efforts in this area sufficient?
- Are all of the existing efforts needed? If not, what can be eliminated?
- Are any of the existing efforts duplicative of what other organizations are doing?
- Are any of the existing efforts done in concert with the work of other organizations?
- If the existing efforts are not sufficient, what gaps do you see and how do you propose to solve them?
- If new efforts are needed:
  - Is the new effort within NERC's scope, or should it be directed to another organization?
  - What gap in existing efforts was identified that this new effort was meant to address?
  - What data is available to scope the new activity?
  - How will we measure performance? What metrics will define and track success?

Working collaboratively with stakeholders, NERC staff collected and consolidated information to be used in the gap analyses. This effort included reviews by the leadership of the technical committees as well as representatives from the North American Transmission Forum and North American Generator Forum (see Appendix 1 for complete details of the gap analyses). Following this effort, the information was reviewed over the course of two days in an open RISC meeting held in Washington, D.C., during which input both from RISC members and observers was solicited. The results of these efforts were used to develop this update. The RISC commends NERC staff and the many stakeholders who participated in the preparation and discussion of these gap analyses.

After the review of these gap analyses, it became clear that the earlier prioritization exercise conducted by the RISC did not indicate that issues were not well controlled. In the majority of cases, the high-priority and medium-priority areas are either well controlled or in the process of becoming well controlled. Placement on the high-priority list generally indicates that the scope of a given issue is ERO-wide and deserves increased focus from the ERO and industry. To a large extent, this is already occurring through previously initiated activities (e.g., the System Protection Initiative) or new activities already in development (e.g., NERC's efforts to improve analysis of events through the use of cause-coding and root-cause techniques).

It was also noted during the gap analyses that no individual problem is likely to result in a negative reliability outcome. The power system was designed so that no single error or contingency should be capable of impacting reliability to a point at which service is interrupted. This inherent resilience presents a challenge when trying to analyze risk to reliability, as it is rare that any one thing can directly lead to an observable degradation in reliability.

Key Prioritization Determinations

This update reflects the RISC's additional analyses completed since its February report. In that report, the RISC identified several high-priority issues. During the development of this update, one new issue was added to the high-priority list: Adaptation and Planning for Change. This issue was added to recognize the importance the industry and the ERO place on constantly assessing the reliability risks of the power system and doing the necessary planning to be ready for any change so it does not manifest as an operational risk. Absent the rapid pace of certain elements of change driven by economics, policy, regulatory, and legislative activities, a number of the issues associated with change that were considered in the February 2013 report are medium- or low-priority issues. However, NERC's *Long-Term Reliability Assessment* properly notes that the pace of change, and the interaction of these factors with one another, introduces a new level of uncertainty that could affect the assumptions and models that underlie long-range planning. Accordingly, several issues that were previously given medium- and low-priority will be looked at through the lens of this new issue to determine what specific items in those broad categories should receive priority attention.

The Adaptation and Planning for Change issue also presents an opportunity to ensure closer alignment between the priorities of the RISC and areas of concern identified in NERC's *Long-Term Reliability Assessment*. Identifying these items and giving them separate treatment within this special category of risk ensures that the broader issues considered in long-term planning are handled differently. This will eliminate the somewhat difficult question of trying to compare and prioritize unlike things (e.g., "Monitoring and Situational Awareness" and "Increased Dependence on Natural Gas Generation" are both concerns worth of study, but in different ways, and for different reasons).

Adding this new issue and consolidating several other issues within this new area changed the total counts in each of the priority groups. The five high-priority issues are as follows:

- **Cyber Attack** – NERC is undertaking a number of activities in this important area. The RISC recommends that NERC continue its work in this area and continue to actively seek strong industry support in the areas of information sharing and efficient threat analysis. Improved sharing of information requires a structure in which open, timely and secure information can be shared without the threat of enforcement action and penalties, and the RISC encourages NERC to consider implementing approaches that minimize or eliminate any potential disincentives to information sharing.
- **Workforce Capability and Human Error** – NERC's Event Analysis program has identified a key problem that spans a number of potential issues: organizational culture's and management decision making's contribution to operational error. Specifically, stronger management and organizational support for enhanced robustness of entity event evaluation would be expected not only to reduce operational error, but to ensure such errors are not repeated. NERC staff is aggressively working to improve industry performance in this area through training and communication initiatives, and the RISC recommends continued allocation of resources to support these activities. However, the RISC notes that best-practice groups (such as the North American Transmission Forum and North American Generation Forum) are developing, and the RISC urges NERC to continue to work with those forums and other stakeholder and best-practices groups in the industry to ensure that lessons learned are developed and shared as quickly as possible, and that industry resources are used most efficiently.

- **Protection Systems** – NERC has identified a number of potential problems within this area, and has either completed or is in the process of completing efforts to reduce risks associated with Protection Systems. The RISC recommends that NERC continue its efforts in this area, such as the further analysis ongoing within NERC's Event Analysis and Performance Analysis programs.
- **Monitoring and Situational Awareness** – NERC's Event Analysis program reviews have shown a number of cases in which tools for monitoring system conditions are partially or totally unavailable, reducing the capability of operators to make informed decisions. While such conditions rarely produce negative reliability outcomes by themselves, they can serve as latent risks through which an otherwise small problem can expand unnoticed into one of greater magnitude and severity. NERC has begun undertaking efforts to make both industry and vendors more aware of the manner in which such systems fail, so that further analysis to develop corrective or mitigating strategies can be undertaken. The RISC recommends NERC continue its efforts in this area.
- **Adaptation and Planning for Change**. As technologies, policies, and the operating environment change, the industry faces significant changes in the way the power system operates. These issues all require careful consideration, preparation, and planning before they manifest, as interventions may not be immediately available or apparent.

There are also four areas of medium priority, and six of low priority. Figure 2 shows the updated list of issues the RISC considered during its analysis, grouped by priority.

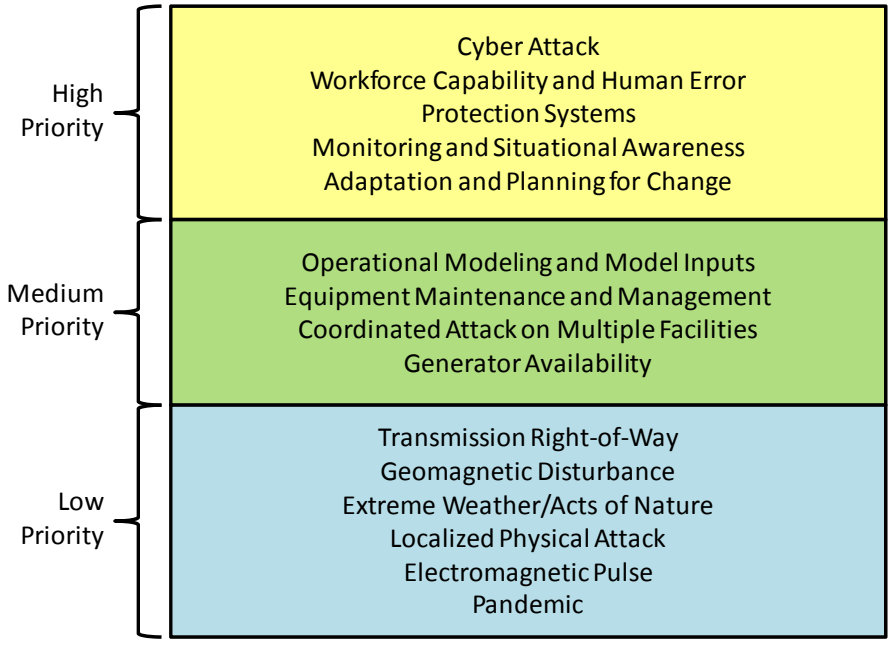


Figure 2 – Reliability Issues and Priorities

All-Hazards Planning

During the RISC's discussions regarding the gap analyses and the risks represented by various issues, one item that became clear was that no individual problem is likely to result in a negative reliability outcome. This is largely because of the conservative planning and design approaches utilized within the electricity industry. The power system has been designed so that no single error or contingency should be capable of impacting reliability to a point where service is interrupted. Service interruptions are most often related to distribution-level failures. In those cases where events occur at the bulk level, typically multiple barriers to failure have been breached such that the industry's inherent defense-in-depth approach to risk control has been rendered ineffective.

The industry does not know which of the many risks to bulk power reliability will actually occur. For this reason, the industry and the ERO properly focus on "all-hazards" planning. The focus is and should be on the resiliency of the system to operate reliably, regardless of which of the risks actually occur. While large investments could be made in an effort to prevent each specific risk, a more cost-effective approach is to focus on mitigating the impact on reliability - regardless of which risk actually occurs.

This approach to defense in depth and design underscores the importance of continued industry and ERO focus on the items that could affect the reliability of the power system. It is with this focus that the RISC prioritized the issues in the report. As such, it is critical that the issues identified in NERC's *Long-Term Reliability Assessment* are given appropriate attention, as they represent the constant and recurring analysis required to ensure the power system continues to meet the performance for which it was designed. The decision to create a new issue for Adaptation and Planning for Change, as described above, is intended to further emphasize the need for this consideration.

Collaboration Opportunities

In addition, the electricity industry is very focused on learning from experience. When events do occur, there is a significant amount of self-directed effort from industry to determine root causes of the event and develop reasonable plans to either address those causes (such that events are less likely to repeat), or better position the system (so that future events are less impactful and the system can be more efficiently returned to a reliable state).

Another significant discussion item during the development of the gap analyses was the increasing efforts being undertaken at the North American Transmission Forum and the North American Generator Forum. Further, additional collaborative groups are being formed that plan to focus their efforts on voluntary activities and sharing of best practices. By reaching out to collaborate with these and similar organizations, NERC can enhance its ability to address issues of concern through targeted interventions that may be just as effective as using its authority to develop reliability standards, but more efficiently or quickly, ensuring that lessons learned are developed and shared as soon as possible and industry resources are used most effectively. The RISC encourages NERC to continue its efforts to work collaboratively with these groups and to develop formal relationships when appropriate (such as the recent memorandum of understanding executed between NERC and the North American Transmission Forum).

ERO Planning Integration – The Reliability Risk Control Process

In addition to these prioritizations, working with the RISC, NERC staff is developing a process through which flagship NERC reports, such as the *State of Reliability Report* and the *Long-Term Reliability Assessment*, are used in concert with input from industry leaders to develop an overall set of priority recommendations for the ERO. Once accepted by the Board, those priorities will be provided to the technical committees for further analysis, refinement, and ultimately development of strategic interventions that can be included in NERC's activities consistent with its existing planning processes. The RISC believes this approach has the potential to ensure that ERO activities are aligned with the problems that matter most to reliability. Provided that the Board concurs with the prioritization recommended in this report, the RISC would expect those priorities to be reflected in the NERC business plan and in the ongoing work of the NERC committees and staff.

This process, tentatively referred to as the "Reliability Risk Control Process," will be initiated in October 2013 at a Leadership Summit through which industry leadership representing stakeholders, regulators, trade organizations, subject matter experts, and other interested parties will be asked to discuss their priorities and concerns in a collaborative environment. This discussion will serve as initial input into the development of the 2014 RISC Update and Recommendations.

Chapter 1 – High Priority Issues

Overview

As discussed in the Introduction, the four high-priority problem areas identified in the February report to the Board of Trustees remain, with the addition of a fifth high-priority area entitled "Adaptation and Planning for Change." Further detail regarding each of these areas is provided below. However, in general, NERC's activities in these areas are adequate and appropriate at this time.

Cyber Attack

Cyber Attack generally refers to malicious activities on the behalf of hackers, disgruntled employees, terrorists, unfriendly nation-states and non-governmental organizations, and other similar parties that occur though the use of computer-based attacks or exploits. Cyber Attack is an area of increased focus due to the potential for harm it represents.

The RISC's gap analysis in this area was conducted with input from NERC staff, the chair of the Critical Infrastructure Protection Committee (CIPC), the RISC representative from the CIPC, the North American Transmission Forum CEO, and the North American Generator Forum chair. A large number of threats and concerns were identified and discussed. In general, industry activities regarding Cyber Attack are in progress and only require time to be completed. However, there were two areas where the correct activities are being undertaken, but further efforts to accelerate progress would be beneficial. Those areas were sharing of information (or the failure to do so) and limited analytic capability at the ES-ISAC. Both of these areas are critical and foundational to the industry's ability to prevent or respond to a cyber attack.

NERC is already moving forward in these areas, but success is largely dependent on continued industry support. There are a number of areas, such as improving and automating the exchange of "indicators of compromise" and similar threat information, that could improve efficiency and timeliness of response. To this end, the RISC encourages NERC to continue reaching out to entities to seek their support for these activities. Expanded participation at the ES-ISAC, as well as improving industry and NERC staff capabilities for supporting analytics efforts, are also encouraged. The RISC notes that improved sharing of information requires a structure in which open, timely and secure information can be shared without the threat of enforcement action and penalties, and encourages NERC to consider implementing approaches that minimize or eliminate any potential disincentives to information sharing.

Additionally, the industry and the ERO rely on and cooperate with federal intelligence agencies and law enforcement to mitigate this risk. Accordingly, outreach to these groups should also continue.

Workforce Capability and Human Error

Workforce Capability and Human Error is an issue that spans multiple potential problem areas and generally refers to those situations in which a human being makes a decision, as well as the elements that influence that decision making.

NERC staff, the chair and vice chair of the Operating Committee, the RISC representative from the CIPC, the North American Transmission Forum CEO, and the North American Generator Forum chair provided input into this gap analysis. While there is a tendency to focus on individual errors, NERC's Event Analysis efforts have identified that current challenges within this area are more organizationally focused. Of the 273 reports reviewed and cause-coded in the Event Analysis database, 20 percent of those with identified root causes point to issues at the management or organizational level. When contributing causes are also considered, over half of the event reports to date indicate some management or organizational challenge that led or contributed to the event. Further, when both root cause and contributing cause are considered, a large number of events are associated with relatively similar causes. A large number of those causes are related to not fully understanding or addressing the cause of previous events.

As such, the RISC encourages and supports the activities NERC is currently undertaking to inform the industry regarding best practices for event analysis and cause coding. These activities aid in ensuring that when events occur, their causes are found and addressed in a timely manner, reducing the potential for repeat events under more adverse circumstances.

Both the North American Transmission Forum and the North American Generator Forum are actively undertaking efforts in this area as well, and the RISC encourages NERC to continue collaboration with those organizations. In so doing, NERC can

continue to encourage and promote voluntary participation in the sharing of event analysis information, while at the same time reducing the burden on registered entities by sharing scarce human resources more efficiently and streamlining information processing.

Protection Systems

Protection Systems are designed to remove equipment from service to avoid its being damaged when a fault occurs. Protection Systems are made up of a number of components, such as relays, associated communication systems, and voltage and current sensing devices. Protection System misoperations often contribute to the severity of an event. A failed protection system that does not trip or is slow to trip may lead to the damage of equipment (removing it from service for some period of time), while a failed 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.

The gap analysis for this area included input from NERC staff, the Planning Committee chair and advisors, the Standards Committee chair, and the North American Transmission Forum CEO. As System Protection has been an important initiative at NERC for some time, a number of activities to address concerns in this area are already well underway. At this time, these activities are progressing well and should be sufficient to address this area of risk.

During the gap analysis, it was proposed to remove one specific area (Special Protection Schemes (SPS) and Remedial Action Schemes (RAS)) from this category and place it into a new category. NERC already has plans to address this issue, and the RISC believes those plans should continue. At this time, further discussion should occur to determine the appropriate treatment of this area with regard to its categorization. Determination of whether SPS and RAS should be considered within the discussion of Protection Systems will be reconsidered at a future date.

Monitoring and Situational Awareness

Much like human error, monitoring and situational awareness is frequently identified as an issue that is central to failures. This functional area includes having the appropriate tools available, perceiving and comprehending the information those tools provide, sharing information, and coordinating mental models.

The RISC's gap analysis for monitoring and situational awareness was developed through collaboration of NERC staff, the Operating Committee chair and vice chair, the North American Transmission Forum CEO, and the North American Generator Forum chair. In general, given existing standards as well as the efforts planned and ongoing at NERC, the data at this time does not seem to indicate significant need for additional work in this area. Of special note is the failure of decision-support tools. This an occurrence that is frequent enough to merit further attention, and NERC efforts are underway to better understand and manage this risk. Failure of a decision-support tool is rarely the cause of an event. Instead, such failures manifest as latent risk that further hinders the decision-making capabilities of the operator. As such, addressing these failures reduces the chances that a poor decision will be made, indirectly reducing the likelihood that human error will cause an event. Educational conferences and information-sharing activities are currently in development at NERC to ensure this potential problem is monitored and controlled.

Adaptation and Planning for Change

During its gap analysis of the high- and medium-priority issues, members of the RISC began further consideration of some of the low-priority areas as well and determined that several of them may have an effect on long term planning. Therefore, a more optimal way of considering several of them would be to incorporate them into a broader category of concern for further analysis. Included in the consolidation were the following items[1]:

- Increased Dependence on Natural Gas Generation (previously identified as medium-priority)
- Generation Resource Adequacy (previously identified as low-priority)
- Long-Term Planning and Modeling (previously identified as low-priority)

[1] These issues were previously ranked as described. However, further analysis of this area is needed to identify and prioritize specific initiatives that could include consideration of some or all of the elements described. This may result in different priorities and a different or restructured set of issues.

- Climate Change, Environmental Regulations, Changing Resource Mix due to Environmental or Other Market Conditions, Integration of Variable Generation (previously identified as low-priority)
- Integration of New Technologies (previously identified as low-priority)
- Demand Response (previously identified as low-priority)
- Smart Grid (previously identified as low-priority)
- Post-Recession Demand Growth (previously identified as low-priority)

Absent the rapid pace of certain elements of change driven by economics, policy, regulatory, and legislative activities, a number of the issues associated with change that were considered in the February 2013 report are medium- or low-priority issues. However, NERC's *Long-Term Reliability Assessment* properly notes that the pace of change, and the interaction of these factors with one another, introduces a new level of uncertainty that could affect the assumptions and models that underlie long-range planning. At this time, further analysis of this area is needed to identify and prioritize specific initiatives that could include some or all of the elements described above. The RISC believes the Planning Committee (or its subcommittees) should work collaboratively with the members of NERC staff who are responsible for the development of the *Long-Term Reliability Assessment* and special assessments to perform this analysis.

Using the Reliability Risk Control Process that NERC is currently developing as the way to analyze and consider this area of concern would be a good transition into the more formal use of that new process. Additionally, it would offer NERC an opportunity to improve that process based on its experience with a smaller set of issues. Accordingly, the RISC recommends NERC take this approach.

Chapter 2 – Medium-Priority Issues

Overview

Similar to the high-priority items, the medium-priority items are largely consistent with those presented in the February 2013 report. NERC's activities in these areas are adequate and appropriately scaled at this time.

Operational Modeling and Model Inputs

This issue refers to lack of data or accurate models in Real time, such that correct decisions are difficult to make. NERC staff, the Planning Committee chair, and the North American Transmission Forum CEO contributed to this gap analysis.

The analysis identified a number of potential problems, all of which NERC or other organizations are addressing with one or more efforts. The RISC encourages NERC to continue analyzing and resolving these areas of concern collaboratively with stakeholders. Further analysis of this area is needed. The RISC believes the Planning Committee (or its subcommittees) should work collaboratively with NERC staff from the Reliability Initiatives and System Analysis team to perform this analysis .

As discussed earlier, using the "Reliability Risk Control Process" to evaluate this area would be a good transition into the more formal use of that new process and would offer NERC a hands-on opportunity to gain experience in its implementation. Accordingly, the RISC recommends NERC take this approach.

Equipment Maintenance and Management

This issue refers to transmission or resources not being available due to equipment being poorly managed or maintained, resulting in physical failure. Additionally, this area includes coordination problems in maintenance schedules and increasing complexity within generation plants as environmental regulations become more stringent. The gap analysis was performed by NERC staff and the Planning Committee chair.

NERC is addressing these threats through a variety of activities. The RISC encourages NERC to continue analyzing and resolving these areas of concern collaboratively with stakeholders.

Coordinated Attack on Multiple Facilities

This issue refers to a physical attack on a number of facilities simultaneously in a coordinated fashion. NERC staff, the Critical Infrastructure Protection Committee chair, the CIPC RISC representative, the North American Transmission Forum CEO, and the North American Generator Forum chair participated in the development of the gap analysis.

This area has a number of threats, all of which can be challenging to manage. In general, industry takes an all-hazards approach to planning, for which a number of potential failures, regardless of cause, have been planned. When events occur on the power system, usually, more than one layer in the "defense in depth" approach to reliability risk management employed by the industry has broken down. As such, physical attacks generally require some level of knowledge and sophistication in order to be effective.

However, the level of industry expertise and maturity in this area is diverse, and a coordinated attack that targets less-sophisticated participants with significant vulnerabilities could lead to a negative reliability outcome. Current industry activities are moving toward developing collaborative processes for sharing lessons learned and for peers assisting each other in assessments and preparation. NERC should stay engaged with these activities by collaborating with industry and the forums to increase information sharing and lessons learned.

Generator Availability

This issue refers to generators not being able to provide energy or related services in Real time. The gap analysis was performed by NERC staff and the Planning Committee chair.

Similar to other issues, NERC is already addressing this area via a number of activities. The RISC encourages NERC to continue analyzing and resolving these areas of concern collaboratively with stakeholders.

Chapter 3 – Low-Priority Issues

Overview

The following areas are considered to be of lower priority and do not to require any special attention from a RISC perspective because they are well controlled or covered by the industry's all-hazards planning. These issues should continue to be monitored, but additional resources should not be directed toward these issues.

Geomagnetic Disturbance (GMD)

Geomagnetic disturbance is a unique problem that is being handled separately based on a FERC initiative. NERC is taking an active role in this area based on FERC guidance. At this time, this risk is being adequately addressed.

Transmission Right-of-Way

The FAC-003 Vegetation Management standard, combined with the FAC-008 data request, has led to an increased awareness and industry focus on maintaining transmission rights-of-way, and performance in this area has improved greatly over the past several years. At this time, this risk is being adequately addressed.

Extreme Weather / Acts of Nature

This is always a concern for utilities, and the concern is being addressed through an ongoing effort of planning for all hazards. To the extent weather trends are changing, ongoing processes for all-hazards planning will include updated preparations that consider such changes. Additionally, the majority of problems related to extreme weather or acts of nature occur on the distribution system, rather than the bulk power system. At this time, this risk is being adequately addressed.

Localized Physical Attack

Similar to extreme weather, this is always a concern for utilities, and the concern is being addressed through an ongoing effort of planning for all hazards. To the extent physical security trends are changing, ongoing processes for all-hazards planning will include updated preparations that consider such changes. At this time, this risk is being adequately addressed.

Electromagnetic Pulse (EMP)

Unlike GMD, an electromagnetic pulse is based on a deliberate action, such as a low atmosphere detonation or a specifically designed weapon. Existing programs within the federal government, such as the FBI, the CIA, and the Department of Homeland Security, are relied on for management of this threat.

Pandemic

Industry has in the past prepared plans for responding to a pandemic. At this time, this risk is adequately addressed through the existence of those plans.

Chapter 4 – Moving Forward

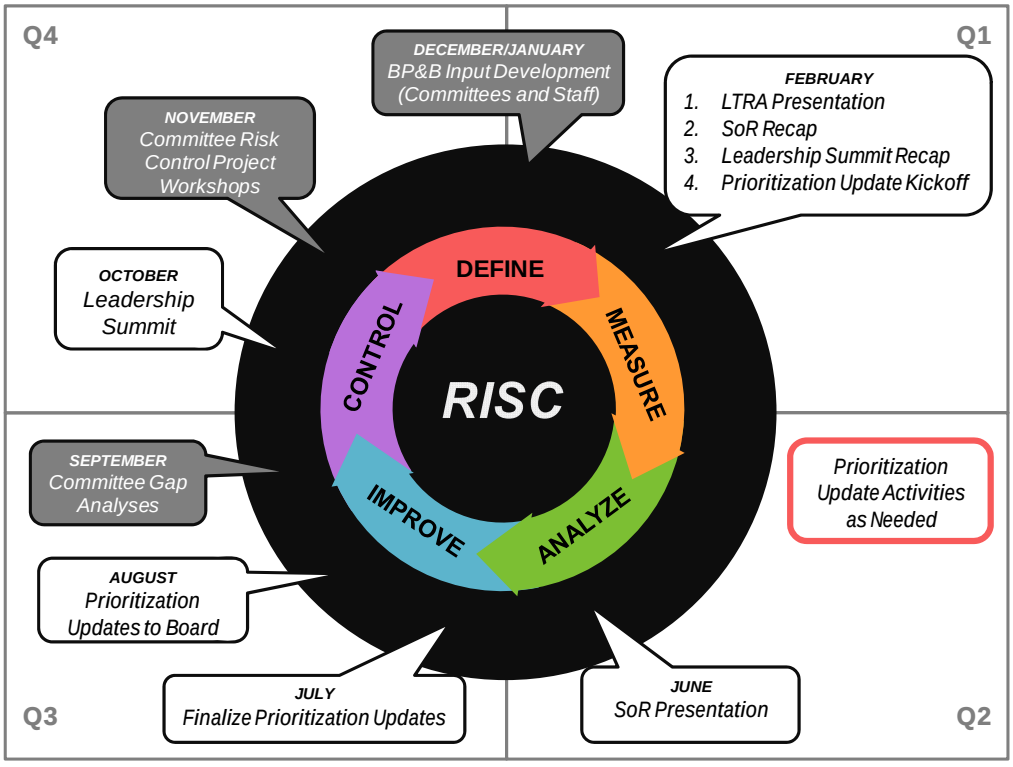
NERC's Reliability Risk Control Process

In February 2013, the NERC Board passed a resolution stating:

> The Board hereby directs NERC management to work with the RISC and, as appropriate, NERC committee leadership to consider how NERC should utilize a data-driven reliability strategy development process that integrates with budget development and overall ERO planning (e.g., Standing Committee planning, department, and employee goal setting).

Based on RISC input, NERC staff has been developing a more formal approach for the identification and resolution of reliability problems that can be used as described in the Board's resolution. Key foundational concepts for this effort include the belief that the process should be open and transparent and encourage stakeholder participation. It should ensure close strategic alignment between and across the RISC, the Operating Committee, the Planning Committee, the Critical Infrastructure Protection Committee, the Compliance and Certification Committee, and the Standards Committee. Further, it should acknowledge that in addition to mandatory reliability standards, NERC has a wide array of tools to address reliability concerns and promote the most effective and appropriate tools for each concern determined to require intervention.

The diagram below illustrates the process that is in development:



This process begins with a Leadership Summit. At the summit, industry leadership, trade association representation, regulators, and others are brought together to share their thoughts regarding what they perceive to be the greatest threats to reliability. This dialogue with the RISC becomes the first input into the development of the RISC's priority recommendations. Documents and conclusions from various NERC programs (e.g., the *Long Term Reliability Assessment* and the *State of Reliability* report) are considered as well. Together with input from other areas, this comprises the foundation upon which the RISC's priority recommendations are built.

Following the collection of this information, the RISC drafts its recommendations and presents them to the Board. If the Board approves the recommended priorities, they then proceed to the Technical Committees for further refinement and analysis, essentially performing the gap analyses that were undertaken in the development of this report. For those areas where gaps are identified and additional controls are needed, the Technical Committees, working with NERC staff, the Compliance and Certification Committee, and the Standards Committee, would meet together in a workshop setting to develop proposals for targeted interventions to address those gaps. Once developed, those proposals would either be included in the process for the development of the NERC business plan or, if urgent, be considered for inclusion within the current year's activities.

NERC staff continues to develop the details for implementing this process, with execution commencing this year with the Leadership Summit, planned for October 24–25, 2013, in Washington, D.C.

Activities for the Remainder of 2013

Although NERC is in the development and documentation stages of its Reliability Risk Control Process and expects to implement the process soon, there are near-term efforts that can and should be undertaken to ensure progress is made now.

Continued Support for Existing Efforts

As discussed above, NERC has a number of activities underway to address the high and medium risks that were identified in the February 2013 report. Further analysis reaffirms much of that report's conclusions and therefore indicates that those activities are appropriate. The information learned during the performance of the gap analyses shows adequate scoping of those activities as well. The RISC recommends that NERC complete these efforts.

Development of Key Metrics

As discussed, NERC has a number of activities underway to address key risks. However, because these projects were in already in existence, a number of them do not have clear and specific measures that can be tracked to monitor industry performance.

The RISC believes that having metrics through which performance can be measured is essential. Developing such metrics provides several functions to the organization:

1) It ensures a thorough understanding of the problem being solved.
2) It allows the development of a baseline against which changes in performance can be measured.
3) It provides a way to continually monitor the problem for future changes.

For this reason, the RISC recommends that NERC work with its technical committees to develop metrics for use in determining the success and ongoing performance of existing ERO activities. For example, there are a number of standards development projects related to Protection Systems, each addressing a different specific issue. It does not seem that there are published metrics that can indicate if performance in those specific areas is improving, staying the same, or declining. The RISC notes that NERC may already have the data it needs to calculate many of these metrics, and this may be a simple matter of developing more granular reports to focus on performance in more specific areas. However, visibility of these metrics is an essential part of moving NERC toward a data-driven process for reliability strategy development and execution.

Development of New Project Proposals

As presented earlier in this document, a new high-priority issue has been identified for which additional analysis is needed: that of "Adaptation and Planning for Change." Similarly, the area of "Operational Modeling and Model Inputs" is in need of further analysis. The RISC recommends that these issues be processed through the post-prioritization steps of the new "Reliability Risk Control Process" described previously; that is:

- Ask the Planning Committee to explore these issues further in the form of a gap analysis or similar activity, and identify the specific threats to reliability associated with each area.

- Ask the Planning Committee to select one or more of these threats for further refinement, through which the problem would be specified exactly, measures for use in analyzing performance would be developed, and appropriate goals and objectives would be identified.
- Ask the PC, OC, CIPC, CCC, and SC (or a subset of their members) to meet and collaboratively develop proposed interventions that would meet the goals and objectives identified.
- Provide those proposals to NERC in January of 2014 for consideration in the development of the 2015 business plan.

The RISC believes that this approach will allow NERC to work through the process it is developing on a smaller scale and identify any areas for improvement prior to moving into full-scale implementation in 2014.

Appendix 1 – Gap Analyses

The RISC has included for reference the results of the gap analyses undertaken for the high- and medium-priority problem areas. These documents were developed for discussion purposes only, and as such are not official statements of NERC, its Board, its committees, or its stakeholders.

Cyber Attack **DISCUSSION DRAFT**	An event occurs due to a cyber attack on BES cyber assets.		**Contributors:** • NERC Staff • Critical Infrastructure Protection Committee • Chair and RISC Representative • North American Transmission Forum CEO • North American Generator Forum Chair
Related NERC Standards CIP-002 through -009 version 3 CIP-002 through -009 version 4 CIP-002 through -011 version 5 EOP-001, -005, -006, -008, -009 address generically	**NERC Standards Development Projects** None.	**Other NERC and Industry Activities** ES-ISAC Monitoring and Metrics Classified Government Security Briefings for Cleared Personnel Industry/Government Information Sharing via the Public/Private Model Cyber Risk Preparedness Assessments (CRPA) Grid Security Exercises Grid Security Conferences Implementation of DOE/DHS/White House Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2 Model) Implementation of DOE/NERC Cyber Security Risk Management Process CIPC Efforts: Subcommittees, Working Groups and Task Forces HILF Efforts/Coordinated Action Plan CIPC Security Training WG to develop workshop on operator training scenarios including cyber-attack components Electricity Sub-sector Coordinating Council (ESCC) Electricity Sub-sector Information Sharing TF Report (CIPC approved, being submitted for BOT approval in August) New NERC Guidelines	**Non-NERC Activities** Entities: Internal and independent programs, monitoring, and testing North American Generator Forum: Security Practices Working Group, developing education initiatives and best practices. Federal government: Presidential EO/PPD-21 Department of Homeland Security: Cyber-Dependent Infrastructure Identification (CDII) National Institute of Standards and Technology (NIST): Security Framework Department of Energy/Department of Homeland Security: Information sharing and security clearances; Sector Incident Response Survey; sector response plan development; event lessons learned understanding Major Trade Organizations; collaborative staffing development support to Industry Incident Response Plan creation aligned to NERC Crisis Action Plan and public sector plans Department of Homeland Security: Updated National Infrastructure Protection Policy; Executive Order Working Group participation and facilitation of sharing North American Transmission Forum: Sharing Subject Matter Expert knowledge, practices. DHS, FBI, and OTHER GOVT AGENCIES: Participation in joint threat and vulnerability community briefings to analysts and sector participants DHS, DoD, DOE and ESCC, creation and participation in Energy Security Public Private Partnership (ES3P), a CIPAC Joint Working Group Industrial Control Systems Joint Working Group (ICS JWG): SME sharing on contemporary security issues involving control systems CYBERCOM: understanding of institutional role definition, authorities and capabilities pertinent to mission assurance, asset protection and response issues Energy and Interdependent Cross Sector Industry venues: various to address interdependency understanding Vendor and Service Provider venues: staying up to date on latest classes of technologies, services and the security practices and technologies which support them National Council of ISACs and various other ISAC events; cross sector information sharing, collaborative threat assessment, and interdependency planning considerations DHS NCCIC; floor watch participation and integration planning activity Software and Supply Chain Assurance Working Group; addressing supply chain, hardware, and software development assurance issues Multi-State Commissioners and Regional Resiliency Group Meetings; support for regional catastrophe planning and readiness Office of Assistance Secretary of Defense for Homeland Defense and America's Security Affairs; Mission Assurance matters Black Hat and similar security and technical conferences: maintenance of technical acumen commensurate with ISAC analytic role
Based on the existing efforts described above: • Are the existing efforts in this area sufficient?			

Yes, but proposed strategic capability maturation requires continued support so ensure delivery. The following have been identified as potential threats related to cyber attack, and NERC has a number of ongoing efforts to address these concerns:

1. Failure to share Security Information: Critical information regarding an actual or potential attack is not shared, leading to increased vulnerability or risk of harm.
   Background: In GRIDEX 2011, when exercise injects occurred, bi-directional information sharing between entities and the ES-ISAC did not occur as effectively as it should. The ES-ISAC needs a free, uninhibited exchange of information to enable it to respond effectively to a cyber event. There is reluctance to share security information due to compliance concerns.
   Response: CID and CIPC have assigned top priority to improving information sharing. Key initiatives are summarized in the CIPC Information Sharing Task Force (ISTF) and ES-ISAC Strategy, and include further developing the capability for cross sector information sharing and secure bi-directional communication. At this time, current activities are moving toward addressing this risk adequately; however, stronger industry support is needed to ensure short term objectives are met expeditiously – specifically, industry must be able to share (through automation and common protocols) and use information (i.e., indicators of compromise, or IOCs) in real-time. This concern will be reviewed again during GRIDEX II in 2013.

2. Limited Analytic Capability at the ES-ISAC: Evidence found during the progression of an attack is unable to be processed accurately in a timely fashion, limiting the ability to respond to an attack in progress on a proactive basis.
   Background: Sophisticated cyber attacks typically require some time for the adversary to take action in a series of steps which result in observable IOCs. By carefully collecting, organizing and analyzing the IOCs, patterns can be discerned to inform defensive actions which can reduce or eliminate the impacts of an attack in progress. Currently, many of the technical tasks associated with this work are manual and need to be automated or technology enabled for faster, more actionable analytic results. Advanced analytic capability is needed to fully leverage information sharing such that it delivers enhanced rapid mitigation and improved sector coordination.
   Response: There are two main aspects of analytic improvement – one is the ES-ISAC staff analytic capability. The other is providing self service analytic capability to entities. Our response, as detailed in the ES-ISAC strategy, answers both of these through initiatives aimed at rapid response and campaign analysis, such as an analyst workbench and cyber awareness monitoring tools. At this time, current activities are moving toward addressing this risk adequately; however, stronger industry support is needed to ensure short term objectives are met expeditiously. Although a number of entities have a wide variety of Security Information and Event Management (SIEM) capabilities, various proprietary products make automated translation and scripting of IOCs from ES-ISAC difficult – this will have to be addressed going forward.

3. Spearphishing: A spearphishing attack leads to penetration or the creation or disclosure of vulnerabilities that are then exploited.
   Background: Spearphising is an email spoofing attempt to target an organization or individual to collect conduct unauthorized collection of confidential information. This may be a general attack on all users or use advanced variants for specific targets. It offers the adversary opportunities to identify system topology and vulnerability, or to insert malicious content. Large numbers of spearphishing attacks have been noted in the media and other channels.
   Response: Indications of Compromise (IOCs) are being identified, analyzed and shared both within sector and across critical infrastructure sectors by ES-ISAC using portal, email, and government threat community networks. Common sharing formats and processes are being implemented. Watch lists are being employed. Additional information sharing and analytic capability is being proposed and implemented at ES-ISAC according to its strategic plan. Utilities are implementing defense in depth capabilities, which can be a good way to defend against this. User training and awareness must be significantly increased to address the Spearphishing threat. At this time, current activities are moving toward addressing this risk adequately.

4. DOS/DDOS: Access to functions or critical information is blocked by coordinated efforts to overload networks and/or servers.
   Background: Denial of service attacks are efforts to make one or more systems or devices unavailable. A distributed denial of service attack coordinates many computers in an attack where all coordinated systems send a stream of requests simultaneously towards targeted victim systems all at once. DOS/DDOS can restrict information flows relating to ICS or commercial and enterprise systems functionality. Large numbers of DOS/DDOS attacks have been noted in the media and other channels.
   Response: Indications of Compromise (IOCs) are being identified, analyzed and shared both within sector and across critical infrastructure sectors by ES-ISAC using portal, email, and government threat community networks. Common sharing formats and processes are being implemented. Watch lists are being employed. Additional information sharing and analytic capability is being proposed and implemented at ES-ISAC according to its strategic plan. Some Registered Entities are working with their Internet Service Providers to address these concerns. At this time, current activities are moving toward addressing this risk adequately.

5. Malware and Virus Injection: A virus or malware attack degrades or debilitates hardware or software.
   Background: Malware and virus injection or code injection is the act of placing computer programming code into a computer program to change the course of processing or execution instructions. It may result in degraded performance or adversary transparency and communications and control capability within the target victim network, computer or device. Multiple vectors for injection are possible. Techniques, tactics and procedures may be hybrid and advanced. A related sub-issue is data diode applicability to this threat, and the treatment of data diodes under applicable CIP-007-05 Requirements R1 and R2. This opportunity is listed separately below. Many well known cyber incidents, including Stuxnet, relied on the injection of malicious code, and these codes can cause computer worms to propagate across machines and networks.
   Response: Indications of Compromise (IOCs) are being identified, analyzed and shared both within sector and across critical infrastructure sectors by ES-ISAC using portal, email, and government threat community networks. Common sharing formats and processes are being implemented. Watch lists are being employed. Additional information sharing and analytic capability is being proposed and implemented at ES-ISAC according to its strategic plan. Additionally, a number of utilities are using various technologies (e.g., “White listing,” Intrusion Prevention Systems, USB controls, and additional Distributed Control Systems segmentation) to defend against these kinds of attacks. At this time, current activities are moving toward addressing this risk adequately.

6. Industrial Control Systems (ICS) Compromise: A mission critical control system is corrupted or disabled.
   Background: Industrial Control Systems can be compromised in many ways. Because there are many types of ICS devices and so many ways to access them, an asset protected by authentication could be compromised if a vulnerability that bypasses authentication is exploited, a non-authenticated trusted connection is utilized (SQL injection or similar) or a DOS attack is placed against open ports (barraged with hyper text transfer protocol [HTTP] or secure shell [SSH] requests that overwhelm the device and result in non-availability). There are many network examples, and recent attacks on ICS have occurred in some sectors and locations; hardware examples also exist, such as smart grid blue tooth enabled devices, and remote access port and point accessibility of both control devices, but also devices used to secure physical security perimeters around sensitive cyber assets, such as gate entry systems (access control systems). ICS compromise holds potential to reduce or deny grid operational control at key times or locations, either causing a BPS risk events or reducing the capability of dynamic operator response during a risk event.
   Response: Indications of Compromise (IOCs) are being identified, analyzed and shared both within sector and across critical infrastructure sectors by ES-ISAC using portal, email, and government threat community networks. Common sharing formats and processes are being implemented. Watch lists are being employed. Authoritative Alert guidance products are being developed and disseminated as appropriate. ES-ISAC subject matter experts participate in expert venues, such as the Industrial Control Systems Joint Working Group. Additional information sharing and analytic capability is being proposed and implemented its ES-ISAC according to its strategic plan. Utilities are deploying defense in depth capabilities, such as enhanced multi-level segregation; “White listing,” USB controls, Intrusion Prevention Systems, and limited communication across security zones. At this time, current activities are moving toward addressing this risk adequately.

7. Software Supply Chain Integrity Compromise: Software with a legitimate purpose is co-opted by an attacker for malicious purposes prior to or during installation.
   Background: Supply chain integrity refers to integrity throughout the full life cycle creation and use of software. For example, was the software designed and delivered in a form that accomplishes what it is known and designed to do, with additional (perhaps malicious) execution or processing steps, or steps that increase malicious observation of the software while it is performing its primary functions. This threat offers potential for adversary compromise of key software control, reporting or management products with possible increase to BPS risk. Observed examples include cases where software was designed with embedded “bugs” or, during installation (often performed by third party contractors) was known to have taken on additional information that caused it to depart from desired installation and performance specifications.
   Response: ES-ISAC subject matter experts participate in technical venues, such as collaborative Software Assurance events. Planned ES-ISAC capability maturation includes tools supportive of sharing and analysis related to this issue. Alert products and processes can be utilized to address these issues. After

ES-ISAC capability maturation is achieved, we may be able to more rapidly and fully learn more regarding this threat due to automated and cross sector information sharing using these capabilities, which are outlined in the ES-ISAC Strategy. At this time, current activities are moving toward addressing this risk adequately.

8. Hardware Supply Chain Integrity Compromise: Hardware is modified or replaced such that vulnerabilities are embedded prior to its installation.
   Background: If the hardware was not created within a trusted foundry environment, it may be subject to intentional (or unintentional due to false packaging or poor development quality controls) tampering or delivery out of specification for its intended use. This threat offers potential for adversary compromise of key hardware control, reporting or management products with possible increase to BPS risk. Numerous examples exist where counterfeit or out of specification products were shipped for use by Original Equipment Manufacturers or final product users. The result can be performance that is out of design specification.
   Response: ES-ISAC subject matter experts participate in technical venues, such as collaborative vendor and threat community events. Planned ES-ISAC capability maturation includes tools supportive of sharing and analysis related to this issue. Alert products and processes can be utilized to address these issues. At this time, current activities are moving toward addressing this risk adequately.

9. Design and Build Life Cycle Quality Assurance (QA) Compromise: A manufacturer inadvertently introduces a vulnerability in their product through a lack of design robustness or quality assurance.
   Background: If QA is compromised, the risk is that performance may be out of specification for the immediate device or product, and systems within which it operates, or which depend on its operation within specification. This threat offers potential for adversary compromise of key technologies with possible increase to BPS risk.
   Response: ES-ISAC subject matter experts participate in technical venues, such as collaborative vendor and threat community events. Planned ES-ISAC capability maturation includes tools supportive of sharing and analysis related to this issue. Alert products and processes can be utilized to address these issues. ICS-CERT provides proposed vendor acquisition language through its Cyber Security Evaluation Tool (CSET) to help with this and similar threats through improved vendor management and acquisition strategies. At this time, current activities are moving toward addressing this risk adequately.

10. Social Engineering: An attacker obtains information by gaining a target's confidence, resulting in inappropriate information disclosure.
    Background: Social engineering broadly includes the non-technical and human interaction aspects of intelligence gathering, including by adversary threat actors. This threat can result in preparing the attack space for further adversary reconnaissance of target victim systems, or subsequent advanced threats. For example, social media can be used to obtain personal information on targets, which can then be applied to broader efforts designed to obtain systems or device control, or to manipulate work processes in malicious ways.
    Response: Alert products and process are utilized to address these issues. ES-ISAC subject matter experts routinely participate in relevant threat and vulnerability collaborative events. Readiness assessment activities in the field are underway and help address this issue. Cyber hygiene is encouraged through outreach activities. Subject matter expert support and staff training are provided for various exercises. Cross sector sharing through the National Council of ISACs, DHS and other threat community channels is employed for early notification, entity education, and mitigation advice development. At this time, current activities are moving toward addressing this risk adequately.

11. Long term Exfiltration: Information is taken for the purpose of preparing for future attacks.
    Background: Results in unauthorized collection of data from devices, systems and networks. This threat can result in preparing the attack space for further adversary reconnaissance of target victim systems, or subsequent advanced threats. Examples include instances where adversaries gained access to commercial networks electronically, then lurk for long periods of time to extract data regarding routine operating patterns of use for devices on network or port status, to potentially leverage later in development of attacks.
    Response: Alert products and process are utilized to address these issues. ES-ISAC subject matter experts routinely participate in relevant threat and vulnerability collaborative events. Readiness assessment activities in the field are underway and help address this issue. Cyber hygiene is encouraged through outreach activities. Subject matter expert support and staff training are provided for various exercises. Cross sector sharing through the National Council of ISACs, DHS and other threat community channels is employed for early notification, entity education, and mitigation advice development. In addition, some utilities are encrypting sensitive data at rest to protect it from exfiltration. At this time, current activities are moving toward addressing this risk adequately.

12. Remote Access Vulnerabilities/Capabilities: An attacker uses vulnerabilities in remote access capabilities to collect or corrupt information or take control of equipment.
    Background: While many networks and devices allow remote access, which results in substantial benefits and efficiencies to organizations, remote access routes and the business practices and policies dependent on them can also cause a proliferation of potential attack surfaces for an adversary. This type of threat can allow contractor engineering service providers (OSP) channel or direct channel for threat actor to gain visibility or control of grid related operational systems. Consolidated remote access capability to sufficient grid operational assets or infrastructure in order to potentially cause grid risk events is the issue. For example, if a large organization or entity relies on remote access using third party services, what level of control does it have on security exposure of affected networks and devices?
    Response: Alert products and processes are utilized to address these issues. ES-ISAC subject matter experts routinely participate in relevant threat and vulnerability collaborative events. Readiness assessment activities in the field are underway and help address this issue. Cyber hygiene is encouraged through outreach activities. Subject matter expert support and staff training are provided for various exercises. Cross sector sharing through the National Council of ISACs, DHS and other threat community channels is employed for early notification, entity education, and mitigation advice development. The ES-ISAC Strategy document calls for collaborative information sharing and analytic capabilities which will be of primary importance in addressing this issue. With the addition of these added capabilities, we hope to explore this threat more fully, and better understand its scale and complexity. Additionally, data diode technology is being discussed through webinars and portal content to help educate entities about this broad class of technologies, its potential applicability, and issues related to its employment. Utilities are implementing multiple levels of segregation, jump hosts, multiple separate untrusted forest credentials and dual factor authentication to reduce this risk in accordance with NERC guidance. At this time, current activities are moving toward addressing this risk adequately.

13. Identification/Authentication Compromise: An attacker impersonates a legitimate user through presentation of the credential used to identify the user or authenticate their access.
    Background: Identity Management (IdM), Access Control (AC) and Identity and Access Management (IAM) are important enterprise services, particularly in environments where commercial networks may come in to contract with control networks. By properly establishing a trusted connection for communication, these functions enable enterprises to know that authorized direction is given to their important control systems and personnel functions. These compromises come in several forms, but may include token integrity, secret or infrastructure compromises, or faulty authentication rules and systems. If authentication is not properly accomplished with integrity, many of the other threats listed in this document can become more easily accomplished and more likely. These threats can result in malicious actor presence on target victim networks or access to grid control, coordination and reporting systems.
    Response: Alert products and process are utilized to address these issues. ES-ISAC subject matter experts routinely participate in relevant threat and vulnerability collaborative events. Readiness assessment activities in the field are underway and help address this issue. Cyber hygiene is encouraged through outreach activities. Subject matter expert support and staff training are provided for various exercises. Cross sector sharing through the National Council of ISACs, DHS and other threat community channels is employed for early notification, entity education, and mitigation advice development. Utilities are implementing multiple separate untrusted forest credentials, dual factor authentication, and segmentation such that no single compromise should cause significant impact to the BES. At this time, current activities are moving toward addressing this risk adequately.

14. Entity Level Network Awareness: An entity's system has been compromised without their knowledge.
    Background: In an environment where sophisticated cyber attacks and intrusions occur with greater frequency, an entity could easily have new additional malicious actors or malware resident within its networks and devices without its own knowledge. To the extent entities can monitor their own systems and networks more effectively; appropriate information for sharing can be identified, as well as emerging threat indications.
    Response: Some ES-ISAC capabilities currently provide ES-ISAC staff with additional visibility regarding malware travelling through domains so that this information might be supplied to affected or potentially affected entities. New planned capability may make some of this transparency available through self-service tools that the entity can access at ES-ISAC portal. ES-ISAC also routinely participates in expert and operator oriented venues designed to improve Network Awareness. Additional industry efforts are needed to standardize a method for exchanging IOCs with minimal effort. At this time, current

activities are moving toward addressing this risk adequately.

15. **Individual Security Errors: A failure in good security practices by individuals ("cyber-hygiene") results in a system compromise.**
    Background: The vast majority of cyber intrusions and attacks are nuisance attacks that can be nearly or completely avoided through good workforce adoption of cyber hygiene. Many attacks of lesser importance might precede or support larger or more sophisticated attack efforts which could be reduced substantially if excellent cyber hygiene implementation is in effect. Stronger cyber hygiene may also increase the chance that a prospective adversary might be deterred from selection of a particular target organization, in favor of one where the cost benefit appears to be higher due to lax cyber hygiene. In that way, sector security might be strengthened. Studies and casual expert observation indicate that substantial entity level and BPS risk reduction could result from improved applied cyber-hygiene in the workplace. This concern includes both cyber and physical aspects, including steps such as increased awareness regarding social media use risks, reduction of tailgating through controlled physical security perimeters, careful construction and protection of strong passwords, etc…
    Response: ES-ISAC routinely participates in expert and operator oriented venues designed to improve cyber hygiene and is taking steps to consider facilitation of cyber hygiene self education services to entities through its portal. At this time, current activities are moving toward addressing this risk adequately.

16. **Hybrid and Coordinated Attack: A threat actor employs advanced techniques which straddle cyber and physical domains, as well as exploits cross sector interdependencies.**
    Background: Advanced threats may leverage coincident cyber and physical attack vectors or vulnerabilities (such as a cyber attack on a hot day with low reserve margins). They might also leverage interdependencies between critical sectors (for example, eliminating fiber connections relevant to systems control and coordination before impacting control systems for direct impacts). Recent events have confirmed that impacts to one critical sector may be part of a coordinated or sophisticated threat against other sectors, and that physical security threats may exist due to threat actor intent to achieve cyber impacts or effects. We understand that prospective threats and contingencies may be novel. These may include cyber-physical hybrid elements or substantial cross sector interdependency issues. For example, "no fiber, no cyber" two step threat techniques. We acknowledge the requirement to better understand these for reliability performance and resilience.
    Response: NERC is collecting data, reviewing authoritative blue ribbon findings from NIAC, CIPC SIRTF/HILF, and others. NERC participates in a variety of exercises and expert collaborative events focused on this issue. NERC is pursuing increased information sharing and analysis capabilities, which will aid immensely in better understanding and managing mitigation development and delivery, as well as sector coordination, for these types of events. At this time, current activities are moving toward addressing this risk adequately.

- Are all of the existing efforts needed? If not, what can be eliminated?
  Yes. The above are needed for improved BPS reliability going forward.

- Are any of the existing efforts duplicative of what other organizations are doing?
  No. While within our sector there are some additional operations centers that perform some similar functions, they are mutually supportive of the ES-ISAC efforts and are valued partners. The authoritative nexus for the sector to the government threat and vulnerability community is the ES-ISAC, leaving it uniquely positioned to address these issues at lowest cost to the sector and its entities. In addition to providing centralized information sharing and analytic capabilities, ES-ISAC offers the potential to provide self-service capabilities and shared resource capabilities for entities at lower cost than they might otherwise have available organically with reduced duplication of effort.

- Are any of the existing efforts done in concert with the work of other organizations?
  Yes. All of the efforts above are accomplished or planned to be accomplished in close coordination with other public and private sector organizations due to their importance, scope and complexity. Capabilities and technologies to address these challenges is presently in the late stages of being documented at high level in both security unclassified and classified venues. Specifically, CID and ES-ISAC both work extensively with other organizations, such as Hydra Subject Matter Experts, Federal Technical Partners, Trades, Technology Vendors, other ERO participants, Registered Entities, National Council of ISACs and all National Infrastructure Protection Plan (NIPP), National Response Framework (NRF) and Unified Coordination Group (UCG) Partners.

- If the existing efforts are not sufficient – what gaps do you see and how do you propose to solve them?
  Current efforts are sufficient; however, filling gaps will require the steady execution of efforts such that current efforts continue and deliver expected results. CIP v5 has set a foundation in standards that is sufficient at this time; additional steps regarding automated information sharing and increasing participation in industry efforts are critical to further developing that foundation such that threats can be identified more readily and acted on in a timely manner. Present gap filling activity focuses on evaluation of pending CIPC Information Sharing Task Force (ISTF) findings for prospective implementation, ES-ISAC technology and business process development, and support to Trades for creation of an industry response plan.

If new efforts are needed: **(No)**

- Is the new effort within NERC's scope or should it be directed to another organization?
- What gap in existing efforts was identified that this new effort was meant to address?
- What data is available to scope the new activity?
- How will we measure performance? What metrics will define and track success?

Workforce Capability and Human Error DISCUSSION DRAFT	An event occurs due to someone (e.g., an operator or a field technician) making a mistake or having an error in judgment.		Contributors: • NERC Staff • Operating Committee Chair and Vice-Chair • North American Transmission Forum CEO • North American Generator Forum Chair
Related NERC Standards PER-001 through -005 COM-001 through -002	**NERC Standards Development Projects** 2007-02 Operating Personnel Communications Protocols IN PROGRESS ETC Q3 2013 2010-01 Support Personnel Training IN PROGRESS ETC Q4 2013	**Other NERC and Industry Activities** Events Analysis Program Lessons Learned Event Analysis Subcommittee Trend Working Group System Operator Certification Training	**Non-NERC Activities** North American Transmission Forum: Efforts related to Human Performance and Events Analysis, Lessons learned North American Generator Forum: Efforts related to Human Performance and Events Analysis, Lessons learned Entities: Simulations, management oversight, procedures and practices, human performance and operator training, human error prevention tools Vendors: Improvements to Human/Machine Interfaces i.e., Man-Machine Interfaces

Based on the existing efforts described above:

- Are the existing efforts in this area sufficient?
  No. NERC has identified six sub-areas for this issue, one of which is not being addressed adequately at this time.

  1. **Individual Skill Based Errors: Inattention or over-attention to performance of work led to or contributed to an event.**
     Response: At this time, data does not show a need for additional work in this area. Existing entity efforts appear to be sufficient to address this concern. NERC Staff continues to work with industry to collect and analyze data looking for these trends.
  2. **Individual Rule Based Errors: A misapplication of a good rule or application of a bad rule during the work process led to or contributed to an event.**
     Response: At this time, data does not show a need for additional work in this area. Existing entity efforts appear to be sufficient to address this concern. NERC Staff continues to work with industry to collect and analyze data looking for these trends.
  3. **Individual Knowledge Based Errors: A lack of knowledge during the work process led to or contributed to an event.**
     Response: At this time, data does not show a need for additional work in this area. Existing entity efforts appear to be sufficient to address this concern. NERC Staff continues to work with industry to collect and analyze data looking for these trends.
  4. **Organizational Challenges: A lack of support for good practices through adequate processes, controls, or procedures led to or contributed to an event.**
     Response: NERC's event analysis database shows this to be an area of concern. Of the 273 reports reviewed and cause coded in the EA database, 20% of those with identified root causes point to issues at the management or organizational level. When contributing causes are also considered, over half of the event reports to date indicate some management or organizational challenge that led or contributed to the event. Further, when both root cause and contributing cause are considered, a large number of events are associated with relatively similar causes. When analyzing event analysis data, cause codes A4B1C05, A4B1C08, and A4B1C04 make up 38 of the 163 cause codes represented (approximately 23%). These three causes are each associated with either not understanding root cause or not taking action to address root cause. Root causes most prevalent in the A4 area, Management and Organizational category include: 1) B3C08 - job scoping did not identify special circumstances or conditions, 2) B5C04 - risks/consequences associated with change not adequately reviewed, 3) B1C03 - direction created insufficient awareness of impact of actions on safety/reliability, 4) B1C04 - follow-up did not identify problems and 5) B1C05 - assessment did not determine cause of previously event or known problem. When considering the contributing causes in this area the top seven causes are: 1) B1C05 - assessment did not determine cause of previously event or known problem, 2) B3C08 - job scoping did not identify special circumstances or conditions, 3) B5C03 - inadequate vendor support of change, 4) B5C04 - risks/consequences associated with change not adequately reviewed, 5) B1C08 - corrective action responses to a known or repetitive problem was untimely, 6) B5C05 - system interactions not considered and 7) B1C04 - follow-up did not identify problems. Accordingly, NERC believes an appropriate intervention to address this area of concern is to encourage more in-depth root cause analysis that goes beyond identification of apparent cause, and aids in more timely resolution of root causes when they are determined. In addition to the internal benefits expected, this will also ensure NERC is more rapidly able to develop responsive interventions to issues rapidly, such as Lesson's Learned reports, Alerts, and similar work products.
  5. **Communication Errors: A message between operators is misunderstood, leading to incorrect decisions.**
     Response: The OC has developed a guideline describing current industry practices, in order to educate the industry on common communications strategies. Additionally, Standards Project 2007-02 Operating Personnel Communications Protocols is intended to put in place rules regarding appropriate communications protocols to minimize communication errors. These activities, once completed, should be sufficient to address this concern.
  6. **Design Errors: A poor design leads to a latent error in the system, which later manifests and contributes to an event.**
     Response: At this time, data does not show a general need for additional work in this area; however, Protection Systems seems to require additional work. See Protection Systems Gap Analysis.

- Are all of the existing efforts needed? If not, what can be eliminated?
  Yes, all are needed.

- Are any of the existing efforts duplicative of what other organizations are doing?
  No.

- Are any of the existing efforts done in concert with the work of other organizations?

  Yes. The North American Transmission Forum (NATF) is developing a voluntary companion process to NERC's Events Analysis process that should improve the overall quality of event analyses. The North American Generator Forum is considering activities in this area as well. In both cases, sloe coordination between NERC and these forums will help encourage and promote voluntary participation in the sharing of event analysis information, while at the same time reducing the burden on registered entities by sharing scarce human resources more efficiently and streamlining information processing.

- If the existing efforts are not sufficient – what gaps do you see and how do you propose to solve them?

  As discussed above, organizational challenges are an area which NERC believes additional work is merited. We believe one way to address organization challenges is to educate industry regarding proper root cause analysis techniques. NERC can also further enhance NERC's Events Analysis process and Cause Code Analysis Process (already in progress), and continue to hold conferences and provide education opportunities regarding root cause analysis and NERC's CCAP, including the use of "train the trainer" sessions. NERC can also use alerts to make entities aware of common problems (for example, Configuration Control Events Alert – November 08, 2011).

  Additionally, NERC can encourage and promote voluntary participation in the sharing of event analysis information through continued outreach efforts with entities and organizations.

If new efforts are needed:

- Is the new effort within NERC's scope or should it be directed to another organization?
  Yes, this is within NERC's scope.

- What gap in existing efforts was identified that this new effort was meant to address?
  Based on analysis of past events, it appears there are organizational challenges that could be addressed and would aid in reducing the probability of mistakes and errors that can lead to events.

- What data is available to scope the new activity?
  NERC's Events Analysis database and associated reports provide data that can be used to analyze performance and guide interventions.

- How will we measure performance? What metrics will define and track success?
  Initial measures will be broad. Although the focus will be on reducing the occurrence of event cause codes associated with A4B1C05 (assessment did not determine cause of previously event or known problem), A4B1C08 (corrective action responses to a known or repetitive problem was untimely), and A4B1C04 (follow-up did not identify problems), focusing on only these codes may not identify additional changes that may be seen in other areas. As such, we recommend that the effectiveness of these interventions be measured based on higher-level code metrics.

  In the subsequent three years following initiation of interventions described above, success will be defined as,

- **Metric 1: A reduction in the annual percentage of events that have been coded as "AZ," or "Information to determine cause less than adequate."**
  - **Number of AZ events divided by the number of total events**
    $$M_1 = \frac{E_{AZ}}{E}$$
- **Metric 2: A reduction in the annual percentage of events not coded as "AZ" that are coded as "A4," or "management/Organization."**
  - **Number of A4 events divided by the number of total events less the events coded as AZ**
    $$M_2 = \frac{E_{A4}}{E - E_{AZ}}$$

Protection Systems **DISCUSSION DRAFT**	An event becomes worse due to a protection system failing to operate correctly.		Contributors: • NERC Staff • Planning Committee Chair and advisors • Standards Committee Chair • North American Transmission Forum CEO
Related NERC Standards PRC-001, -003 through -005, -012 through -017, -023 TPL-003 and -004	**NERC Standards Development Projects** 2007-06 System Protection Coordination IN PROGRESS ETC Q4 2013 2010-05.1 Protection Systems Misoperations IN PROGRESS ETC Q3 2013 2010-13.2 Generator Relay Loadability IN PROGRESS ETC Q3 2013 2007-11: Disturbance Monitoring Equipment Standard IN PROGRESS ETC Q 2014 2007-17.2: Protection System Maintenance and Testing – Phase 2 (reclosing relays) IN PROGRESS ETC Q4 2013 2007-17.3: Protection System Maintenance and Testing – Phase 3 (sudden pressure and other non-electric devices) PENDING EVALUATION Project 2007-09 Generator Verification PENDING REGULATOR APPROVAL 2010-05.2 SPS and RAS **(Recommended for transfer; see below)** 2010-13.3 Stable Power Swings PENDING EVALUATION	**Other NERC and Industry Activities** Protection System Misoperation Task Force System Protection and Control Subcommittee Regional Criteria Operating Committee Event Analysis Subcommittee Trend Working Group Event Analysis Program Lessons Learned State of Reliability Report	**Non-NERC Activities** IEEE: Research and development efforts Entities: Internal company procedures North American Transmission Forum: Peer reviews of company Protection System methods and processes North American Transmission Forum: Sharing of best practices related to System Protection North American Transmission Forum: Regional pilot of best practice approaches for addressing Protection System Misoperations North American Transmission Forum: Evaluating the offering of System Protection expertise as part of member assistance function.

Based on the existing efforts described above:

- Are the existing efforts in this area sufficient? **Yes.**
  Analysis has identified eight ways in which threats within this general risk area may manifest. These are summarized below, along with a brief description of how the risk is being controlled.

1. **Field Personnel Errors: Settings specified in the protection system design are correct, but personnel in the field applied them incorrectly.**
   Response: Analysis of misoperation data does not support this as a major cause of misoperations or events involving protection systems. No interventions are suggested beyond regular internal company procedures.

2. **Relay Loadability: Part of the BES trips due to protection system settings being overly conservative, such that necessary equipment does not "ride through" an event and is subsequently unavailable to respond to or support the event.**
   Response: NERC has already completed Project 2010-13.1, which addressed the loadability of transmission protection system relays Project 2010-13.2, which will similarly address the loadability of generator protection system relays, is in progress. A potential third project to address the loadability of protection system relays during stable power swings through standards development is being evaluated. These activities are sufficient to address this concern.

3. **Lack of Redundant Protection for Critical Facilities: A protection system critical to the stability of the BES fails, leaving the system in essentially an N-0 state.**
   Response: NERC's SPCS has developed a document explaining Redundancy of Protection Systems and its application. At this time, these activities are sufficient to address this concern.

4. **Single Points of Failure in Protection Systems: A single component integral to a number of protection systems fails, resulting in several protection systems not functioning.**
   Response: A NERC Rules of Procedure, Section 1600 data request to the industry is underway to determine the extent to which such scenarios exist. This work is also in part to address the single point of failure issue raised in FERC Order 754. Following that analysis, a new standards development effort may commence if warranted.

5. **Coordination of Protection Systems: Two or more protection systems have setting or design conflicts (for example, such that the protective action of one system negates or overrides the intended operation of the other).**
   Response: Entities are already required to coordinate protection system settings. Project 2007-06 System Protection Coordination is intended improve existing standards, and require coordination activities when certain facility changes to the system are made, which will help reduce the potential for conflicts. This activity is sufficient to address this concern.

6. **Generator Frequency and Voltage Protective Relay Coordination: Generators without adequate coordination between generator protective relays and generator voltage regulator controls and limit functions may trip off-line during voltage and frequency excursions.**
   Response: Project 2007-09 Generator Verification, recently completed and awaiting Board adoption, includes Standard PRC-024-1 — Generator Frequency and Voltage Protective Relay Settings, which requires Generator Owners set their generator protective relays such that generating units remain connected during

defined frequency and voltage excursions. This activity is sufficient to address this concern.

7. **Reduction of common mode failures and repeat misoperations: The lessons learned from a single misoperation are not applied, resulting in an identical misoperation of the same equipment or a functionally identical misoperation on other equipment.**
   Response: Project 2010-05.1 Protection Systems Misoperations is intended to require analysis and corrective action plans to address misoperations, and will help reduce common mode failures and repeat misoperations. NERC and Standards Committee representation will be meeting with the Project 2010-05.1 standards drafting team to ensure the team's approach is correctly aligned with the conclusions identified in the recently published State of Reliability Report. Additionally, Project 2007-11: Disturbance Monitoring Equipment Standard will assist in the analysis of misoperations, further enhancing the ability of entities to discover root causes and take appropriate remediation steps. Outside the realm of mandatory reliability standards, the Protection System Misoperation Task Force has been investigating this area and recently developed a set of suggestions for addressing commonly seen problems and improving protection system performance through the development of guidelines. NERC's State of Reliability Report also identified areas for improvement and made recommendations in this area. NERC has begun disseminating more information regarding these commonly seen problems, and is developing training modules to further educate the industry in this area. These activities are sufficient to address this concern.

8. **Protection Equipment Failure: Protection system components fail to operate as expected. It is assumed that periodic maintenance and regular testing would catch these failures in a safe environment, rather than a live environment where their failure can adversely impact reliability.**
   Response: Project 2007-17 (Protection System Maintenance and Testing; completed), developed standards that specify how and when to maintain certain key protection system equipment. There is additional work regarding Reclosing Relays and Sudden Pressure Relays in progress. NERC's State of Reliability Report also identified areas for improvement and made recommendations in this area. These activities are sufficient to address this concern.

- Are all of the existing efforts needed? If not, what can be eliminated?
  No. The PC has reviewed the need for a standard related to "Protection System Commissioning Testing," and found that a standard is not necessary at this time. Additionally, NERC, under a Section 1600 data request, is collecting data for analysis (described above as "Single Point of Failure (Order 754) Data Request") to determine if a new standard is needed to address "Reliability of Protection Systems", if a modification of existing TPL standards would adequately cover the Single Point of Failure (SPOF) concern, or if existing TPL standards adequately cover the SPOF concern. Under the NERC PC, the SPCS and SAMS will review the Order 754 data and recommend if additional actions are required. Other NERC efforts to address Single Point of Failure include the NERC Board approved interpretation INT-2012-02 of TPL-003 and -004 and the new TPL-001-2, which is currently NERC Board approved and awaiting FERC approval.
- Are any of the existing efforts duplicative of what other organizations are doing?
  No.
- Are any of the existing efforts done in concert with the work of other organizations?
  No.
- If the existing efforts are not sufficient – what gaps do you see and how do you propose to solve them?
  We do not see any gaps. However, we make the following suggestions:
  - **Remove SPS and RAS from this risk discussion, and create a new priority area specifically for SPS and RAS. The technologies, goals, and functions are sufficiently different to merit a separate treatment.**
  - **Review the PSMTF Report on protection system misoperations to determine if there are next steps that the RISC should undertake.**

  Also, there may be additional value in NERC undertaking the following activities:
  - **Consider collecting data to determine if aging protection system equipment is an area of concern to be addressed**
  - **Coordinating more closely with the NATF and NAGF on their efforts related to protection systems**
  - **Evaluating the effectiveness of mandatory NERC requirements associated with protection systems**

If new efforts are needed: **(No)**

- Is the new effort within NERC's scope or should it be directed to another organization?
- What gap in existing efforts was identified that this new effort was meant to address?
- What data is available to scope the new activity?
- How will we measure performance? What metrics will define and track success?

Monitoring and Situational Awareness **DISCUSSION DRAFT**	An event occurs due to a control center or similar facility either not receiving, understanding, or acting on information related to system conditions.		Contributors: • NERC Staff • Operating Committee Chair and Vice-Chair • North American Transmission Forum CEO • North American Generator Forum Chair
Related NERC Standards BAL-005 COM-001 through -002 FAC-001 IRO-001 through -005 IRO-008, -010, -014 through -016 NUC-001 PER-001 through -005 TOP-001, -003 through -006 VAR-001	**NERC Standards Development Projects** 2007-02 Operating Personnel Communications Protocols IN PROGRESS ETC Q3 2013 2009-02 Real-time Reliability Monitoring and Analysis Capabilities IN PROGRESS ETC Q1 2014	**Other NERC and Industry Activities** Entity Certification and Registration RCIS Events Analysis Program Lessons Learned NERC Alerts SAFNR II NERC Bulk Power System Awareness NERC Functional Model Operating Committee Event Analysis Subcommittee EMS Task Force System Operator Certification September Vendor Conference OC-directed Tool Status Communication Practices research; assigned to the ORS, with the goal of guideline development Tools developed through NERC facilitated efforts (e.g., The Reliability Coordination Information System (RCIS), the System Data Exchange (SDX) program).	**Non-NERC Activities** Vendors: Alarms, Disturbance Monitoring Equipment Entities: Implementation of Teams (shared SA) North American Generator Forum: Efforts related to Human Performance and Events Analysis, Lessons learned North American Transmission Forum: Peer reviews, Tools Group.

Based on the existing efforts described above:

- Are the existing efforts in this area sufficient?
  Generally, yes, although one area can use some additional improvement. Seven ways in which errors associated with Monitoring and Situational Awareness can manifest are shown below, along with associated responses.

  1. **Appropriate Decision Support Systems do not exist: The tools needed to monitor or comprehend BES conditions have not been provided, leading the operator to make incorrect decisions.**
     Response: Standards Project 2009-02 Real-time Reliability Monitoring and Analysis Capabilities will list required capabilities for system operators. This activity is sufficient to address this concern.

  2. **Decision Support System Failure: Tools used by the operator to monitor or comprehend BES condition fail, leading the operator to make incorrect decisions.**
     Response: Data has shown this to be a significant threat to situational awareness. NERC recommends activities be undertaken to increase awareness of this problem, such that industry will implement creative, situation-specific solutions to increase availability. Additionally, NERC should educate the industry on good practices for mitigating the risk of problems should a failure occur. See additional details below.

  3. **Communication Error: A message between operators is misunderstood, leading to incorrect decisions.**
     Response: The OC has developed a guideline describing current industry practices, in order to educate the industry on common effective communications strategies. Additionally, Standards Project 2007-02 Operating Personnel Communications Protocols is intended to establish rules regarding appropriate communications protocols, thus minimizing communication errors. These activities, once completed, should be sufficient to address this concern.

  4. **Individual Perception Failure: An individual operator is unaware of a communicated condition, leading him or her to make incorrect decisions**
     Response: At this time, data does not indicate this to be a problem within the industry. NERC will continue to monitor this area for any change in performance.

  5. **Individual Comprehension Failure: An individual operator does not understand the impact of a communicated condition, leading him or her to make incorrect decisions**
     Response: At this time, data does not indicate this to be a problem within the industry. NERC will continue to monitor this area for any change in performance.

  6. **Intra-Entity Team Disagreement: Individual operators within the same entity disagree about system conditions, resulting in incorrect or postponed decisions.**
     Response: At this time, data does not indicate this to be a problem within the industry. NERC will continue to monitor this area for any change in performance.

  7. **Inter-Entity Team Disagreement: Operators from different entities disagree about system conditions, resulting in incorrect or postponed decisions.**
     Response: A number of NERC standards, programs, and guidelines address this concern. Coordination obligations, such as those defined in the TOP and PRC standards, help ensure agreement and consistency ahead of time. Tools developed through NERC facilitated efforts, such as RCIS and SDX, help ensure information is shared between entities. In real-time, IRO-014-2 requires that in situations in which Reliability Coordinators are in disagreement regarding system conditions, the Reliability Coordinator that identified the condition shall be given deference regarding how to mitigate the condition. At this time, it is believed this is sufficient to address this concern.

- Are all of the existing efforts needed? If not, what can be eliminated?
  Yes.

- Are any of the existing efforts duplicative of what other organizations are doing?
  No.

- Are any of the existing efforts done in concert with the work of other organizations?
  No.

- If the existing efforts are not sufficient – what gaps do you see and how do you propose to solve them?
  Regarding Decision Support System Failure, NERC recommends activities be undertaken to increase awareness of this problem, such that industry will implement creative, situation-specific solutions to increase availability. Additionally, NERC should educate the industry on good practices for mitigating the risk of problems should a failure occur. Approaches for accomplishing this could include:
  - **Using Alerts to make entities aware of common problems (for example, Preventable EMS and SCADA Events Alert – April 10, 2012)**
  - **Publishing Lessons Learned that provide insight into this problem (four Lessons Learned published in February 2013, two more in development)**

- **Presenting discussions of the concern and various mitigation strategies in public forums (e.g., meetings of the Event Analysis Subcommittee and Operating Committee).**
- **Holding a stakeholder/vendor conference where issues can be discussed and strategies for minimizing failures developed (Targeted for Sept 2013 Denver, CO).**

If new efforts are needed:

- Is the new effort within NERC's scope or should it be directed to another organization?
  Yes, although the assistance of other organizations would be beneficial.

- What gap in existing efforts was identified that this new effort was meant to address?
  Decision Support System Failures create latent risk that, when combined with other real-time events or conditions, can lead to significant failures.

- What data is available to scope the new activity?
  NERC's Events Analysis database and associated reports provide data that can be used to analyze performance and guide interventions.

- How will we measure performance? What metrics will define and track success?
  For determining the effectiveness of the interventions discussed above related to Decision System Support Failures, net decreasing trends in the following four metrics over the subsequent 18 months following initiation of the interventions will indicate success.
  - **Metric 1: Total count of all Full EMS Outages reported within a rolling 12-month period, as reported through the NERC Events Analysis Process**
  - **Metric 2: Total count of all Partial EMS Outages reported within a rolling 12-month period, as reported through the NERC Events Analysis Process**
  - **Metric 3: Mean duration of Full EMS Outages reported within a rolling 12-month period, as reported through the NERC Events Analysis Process**
  - **Metric 4: Mean duration of Partial EMS Outages reported within a rolling 12-month period, as reported through the NERC Events Analysis Process**

Operational Modeling and Model Inputs **DISCUSSION DRAFT**	An event occurs due to models and/or model inputs used in day-ahead and/or real-time being inaccurate or not available. **NOTE: THIS GAP ANALYSIS NEEDS FURTHER REVIEW AND ANALYSIS. THE RISC IS RECOMMENDING IT BE ANALYZED THROUGH THE "RELIABILITY RISK CONTROL PROCESS."**		Contributors: • NERC Staff • Planning Committee Chair • North American Transmission Forum CEO
Related NERC Standards BAL-005 COM-002 FAC-009, -014 INT-001 through -010 IRO-002, -003, -005, -008, -010 MOD-010, -012, -016, -017, -018, -019, -020, -021 NUC-001 TOP-002, -003, -005, -006	**NERC Standards Development Projects** 2010-03 – Modeling Data IN PROGRESS ETC Q4 2013 2010-04 Demand Data IN PROGRESS ETC Q4 2013 2008-12 Coordinate Interchange Standards IN PROGRESS ETC Q4 2013 2012-05 ATC Revisions – Order 729 IN PROGRESS ETC Q4 2013 2007-09 Generator Verification PENDING REGULATOR APPROVAL	**Other NERC and Industry Activities** Modeling Working Group Regional activities and working groups Western Interconnection Response to AZ/SoCal Outage	**Non-NERC Activities** ERAG-MMWG: Development of modeling guidelines. Eastern Interconnection Planning Collaborative: Development of modeling guidelines. North American Transmission Forum: Development of modeling guidelines.

Based on the existing efforts described above:

- Are the existing efforts in this area sufficient?
  Yes. There are a number of areas for potential improvement to industry modeling efforts, and various activities are underway to make those improvements.

1. **Generator Dynamics: Generator modeling has become suspect in trying to perform interconnection-wide dynamic analysis and cannot necessarily be counted on to correctly predict system behavior.**
   Response: NERC's Modeling Working Group (MWG) is working to develop an industry supported standardized component model library and common data exchange format, which will assist in the resolution of this problem. The North American Transmission Forum (NATF) and Eastern Interconnection Reliability Assessment Group (ERAG) are also developing modeling guidelines in this area. These efforts should be sufficient to address this concern at this time.
2. **Load Behavior: The use of new technologies is changing load characteristics and behavior, which makes traditional load modeling obsolete. An understanding of the changes is essential to more accurately model the operational characteristics of today's modern loads and predict their effects on the power system.**
   Response: WECC and other entities have developed composite load models allow for multiple types of loads for each bus with differing characteristics. Some of those load models are adaptive, changing characteristics when exposed to different voltages. WECC is implementing the use of the composite load model for regional interconnection-wide studies. Additionally, ISO New England is performing research on the composition of their loads and the characteristics in preparation for implementing a composite load for its system. At this time, monitoring these efforts are sufficient steps toward addressing this area of concern. As more knowledge is gained in this area, additional efforts such as the development of load modeling guidelines may be appropriate.
3. **Frequency Response: Inaccurate modeling of frequency response leads to a failure to predict system behavior during disturbances.**
   Response: A work plan is underway with the ERAG Multi-Regional Modeling Working Group (MMWG) to develop "generic" governor model light load case from the 2012 series and to adjust individual governor models in the 2013 series to reflect responsiveness. The work plan also calls for delivery of a corrected light load 2014 case by August 1, 2014.
4. **Inter-Area Oscillations: Models are insufficiently robust to predict inter-area oscillations, leading to behaviors that have not been analyzed and protected against.**
   Response: NERC's MWG is undertaking efforts to enhance system model validation. Additionally, WECC is developing a West-wide System Model that will help in their analysis of this problem. These efforts should be sufficient to address this concern at this time; however, analysis may identify additional work to be undertaken in the future.
5. **Equipment Modeling: A lack of standardized component models for BES equipment (e.g., static var compensators, static synchronous compensators, DC converter stations, frequency shifting transformers, etc.) impedes the construction of valid power system models needed to accurately predict interconnection-wide power system behavior.**
   Response: NERC's Modeling Working Group (MWG) is working to develop a industry supported standardized component model library and common data exchange format, which will assist in the resolution of this problem. An initial library of standardized models will be created using the current Regionally-approved dynamic model libraries. Additional models from the Institute of Electrical and Electronics Engineers (IEEE) and other appropriate organizations will be added as appropriate. Models for new technological innovations will be developed, validated, and added to the library of standardized models. This effort should be sufficient to address this concern.
6. **Modeling Errors – Errors in powerflow and dynamics models lead to predicted system behavior that differs from reality.**
   Response: Regional Entities are reviewing and comparing governor models against the 2010 governor survey done as part of the Frequency Response Initiative. The ERAG is testing a new topology database, which is expected to be in service in 2014. NERC's MWG is working to develop an industry supported standardized component model library and common data exchange format, which will assist in the resolution of this problem. The MWG is also beginning to consolidate modeling guidelines in support of generator owner and transmission modeling personnel, and is in the process of field testing a Model Validation Procedure. Additionally, efforts to standardize approach to modeling (node-breaker versus bus-branch) may reduce the potential for errors by eliminating the need for maintaining multiple models.
7. **Modeling Consistency: Differences in understanding of model parameters leads to models that do not accurately predict system behavior.**
   Response: NERC's Modeling Working Group (MWG) is working to develop an industry supported standardized component model library and common data exchange format, which will assist in the resolution of this problem. The North American Transmission Forum (NATF) and Eastern Interconnection Reliability Assessment Group (ERAG) are also developing modeling guidelines in this area. These efforts should be sufficient to address this concern at this time.
8. **Model Compatibility: Inability to share models through a common protocol lead to less detailed models and modeling error that can affect accurate prediction of power system behavior.**
   Response: The NERC MWG has been tasked to develop an industry supported standardized component model library and common data exchange format. The MWG is investigating the potential for use of the Common Information Model (CIM) as a standardized data exchange protocol for sharing information between companies and across interconnections. Additionally, the MOD B Standards Development project to modify NERC Reliability Standards MOD-010 through MOD-015 to improve transparency of data needed to accurately study power systems. These efforts should be sufficient to address this concern at this time.
9. **Approaches to Modeling: Planning and Operations models that use different representations (node-breaker versus bus-branch) lead to inconsistent understanding of contingencies and duplication of modeling efforts, both of which may lead to inaccurate prediction of power system behavior.**
   Response: NERC's MWG is proposing an effort to incorporate node-breaker modeling in off-line powerflow and dynamics cases and analysis. This initial effort should be sufficient to address this concern at this time.

10. **Special Protection Systems/Remedial Action Schemes: Lack of modeling of SPS and RAS result in unexpected and detrimental BES behavior during a disturbance.**
    Response: Research to develop modeling methods for modeling Special Protection Systems and Remedial Action Schemes in order to determine their potential interaction is underway with the WECC Modeling SPS and RAS Ad Hoc Task Force (MSRATF). This effort is sufficient to address this concern at this time.
11. **Protection Systems: Lack of accurate protection system details in dynamics models leads to predicted behavior differing from actual power system behavior.**
    Response: Research is underway on linking dynamics programs to existing corporate relay databases. While this holds promise, it can currently only be done for limited portions of an interconnection at this time.
12. **Turbine and Boiler Controls: Lack of understanding of how turbine and boiler controls interact with the power system has resulted in unexpected losses of generation.**
    Response: NERC has been seeking to perform research on which aspects of turbine and boiler controls should be modeled to correctly predict the behavior of generation during system disturbances. Defining which functions and behaviors should be modeled for transient and mid-term dynamics, coupled with recommendations on additional modeling of generator protection systems (such as Volts/Hertz, under-voltage, and under-frequency relays) will greatly improve the industry's ability to predict generation performance during disturbances. Under the guidance of the System Analysis and Modeling Subcommittee (SAMS), NERC will be seeking participation in this effort from Generator Owners, turbine manufacturers, and other technical experts. This effort should be sufficient to address this concern at this time.
13. **Model Input Data: Bad data, or lack of data, leads to a model used in operations producing an invalid result, negatively impacting operator decision making.**
    Response: Project 2010-03 (Modeling Data) and project 2010-04 (Demand Data) are both standards projects intended develop more consistency around the data used in modeling and forecasting. These efforts should be sufficient to address this concern at this time.
14. **Seams Coordination: Differences in fundamental assumptions between areas lead to inconsistency in local modeling and simulation results, negatively impacting operator decision making.**
    Response: There are limited activities in this area at this time. RISC recommends further analysis be done by the Planning Committee in this area.

- Are all of the existing efforts needed? If not, what can be eliminated?
  Yes.
- Are any of the existing efforts duplicative of what other organizations are doing?
  No.
- Are any of the existing efforts done in concert with the work of other organizations?
  Yes. As discussed above, efforts are being undertaken in collaboration with regional entities, registered entities, and other organizations, such as the NATF and IEEE.
- If the existing efforts are not sufficient – what gaps do you see and how do you propose to solve them?
  Existing efforts are sufficient at this time.

If new efforts are needed: **(No)**

- Is the new effort within NERC's scope or should it be directed to another organization?
- What gap in existing efforts was identified that this new effort was meant to address?
- What data is available to scope the new activity?
- How will we measure performance? What metrics will define and track success?

Equipment Maintenance and Management **DISCUSSION DRAFT**	An event occurs due to not maintaining equipment correctly or on schedule and having something fail.		Contributors: • NERC Staff • Planning Committee Chair • North American Transmission Forum CEO
Related NERC Standards PRC-005,-008, -011, -017 TOP-003	**NERC Standards Development Projects** 2007-17.2 Protection System Maintenance and Testing IN PROGRESS ETC Q4 2013	**Other NERC and Industry Activities** Ongoing analysis of failures related to equipment maintenance and management. Development of ALR metric ALR6-13 (AC Transmission Outages Initiated by Failed AC Substation Equipment) Formation of a team to further probe the AC substation equipment failures and identify potential solutions Spare Equipment Database and associated Task Force Long Term Reliability Assessment and the use of Probabilistic Reliability Assessments	**Non-NERC Activities** Entities: Maintenance Programs. Vendors: Warranty Requirements.

Based on the existing efforts described above:

Are the existing efforts in this area sufficient? **Yes.**

There are several areas in which Equipment Maintenance and Management issues may manifest:

1. **Transmission Lines Failure. A transmission line physically fails, resulting in less ability to transport energy to serve load.**
   Response: In general, NERC has not seen any unusual trend regarding the physical failure of transmission lines. NERC standards related to SOLs and IROLs, combined with market forces, have largely resulted in a strong desire to protect assets from damage. The exception in this area would be the impact of significant weather events on the transmission system, which are essentially transmission adequacy concerns. NERC's Long Term Reliability Assessment is currently the place where such concerns are discussed and considered. These activities have been sufficient to address this concern.
2. **Transmission Substation Failure. Equipment at a substation physically fails, resulting in a loss of transmission, generation, or both.**
   Response: NERC has identified that AC substation equipment failures are the second most significant contributor to disturbance events and automatic transmission outage severity. Analysis of the transmission outage and disturbance event information shows that circuit breakers are the most common type of ac substation equipment failure. NERC has formed a small subject matter expert technical group to further probe the ac substation equipment failures, particularly circuit breaker failures, and provide risk control solutions to improve performance. This activity is sufficient to address this concern until such time as conclusions are developed regarding how to proceed.
3. **Transmission Protection Systems Failure: A transmission protection system fails, resulting in equipment damage and/or larger areas of the system taking themselves out of service.**
   Response: Project 2007-17 (Protection System Maintenance and Testing; completed), developed standards that specify how and when to maintain certain key protection system equipment. There is additional work regarding Reclosing Relays and Sudden Pressure Relays in progress at the request of the FERC. Also see the Protection System Gap Analysis. These activities are sufficient to address this concern.
4. **Generator Protection System Failure: A generation protection system fails, resulting in and equipment damage and/or unnecessary reductions in available generation supply.**
   Response: Project 2007-17 (Protection System Maintenance and Testing; completed), developed standards that specify how and when to maintain certain key protection system equipment. There is additional work regarding Reclosing Relays and Sudden Pressure Relays in progress at the request of the FERC. Also see the Protection System Gap Analysis. These activities are sufficient to address this concern.
5. **Generator Failure: A generator physically fails, resulting in less generation supply to serve load.**
   Response: In general, NERC has not seen any unusual trends regarding generator performance. One highly visible exception is that of generator performance in abnormally cold weather. However, NERC's Operating Committee has developed a guideline to address this concern, and NERC will be undertaking a communication and education campaign to ensure entities are aware o the guideline and the recommended practices it describes. Also see the Generator Availability Gap Analysis. These activities are sufficient to address this concern.
6. **Inter-Entity Maintenance and Testing Coordination: Multiple entities are testing or maintaining their equipment, resulting in a system that behaves unexpectedly.**
   Response: The scope and magnitude of this risk is undefined. NERC's Planning Committee will be working to analyze this risk and develop a proposal for next steps.
7. **Increased Generation Plant Complexity: A plant fails or is subjected to forced derate because complex parasitic modifications and/or retrofits create increased operational risks to the overall power block (for example, clean air retrofits required to comply with the Mercury and Air Toxics Standards).**
   Response: The scope and magnitude of this risk is undefined. NERC's Planning Committee will be working to analyze this risk and develop a proposal for next steps.

- Are all of the existing efforts needed? If not, what can be eliminated?
  Yes.
- Are any of the existing efforts duplicative of what other organizations are doing?
  No.
- Are any of the existing efforts done in concert with the work of other organizations?
  No.
- If the existing efforts are not sufficient – what gaps do you see and how do you propose to solve them?
  We do not see any gaps at this time. However, depending on the results of the special subject matter expert technical group investigating substation failure, gaps may be identified that require specific interventions. We recommend NERC continue to monitor this issue and be prepared to respond as conclusions are determined.

If new efforts are needed: **(No)**

- Is the new effort within NERC's scope or should it be directed to another organization?
- What gap in existing efforts was identified that this new effort was meant to address?
- What data is available to scope the new activity?
- How will we measure performance? What metrics will define and track success?

Coordinated Attack on Multiple Facilities **DISCUSSION DRAFT**	An event occurs due to a physical attack on infrastructure.		Contributors: • NERC Staff • Critical Infrastructure Protection Committee Chair and RISC Representative • North American Transmission Forum CEO • North American Generator Forum Chair
Related NERC Standards CIP-001 CIP-006 (for certain BES cyber systems) EOP-001, -005, -006, -008, -009 address generically	**NERC Standards Development Projects** None	**Other NERC and Industry Activities** ES-ISAC Monitoring Grid Security Conference Grid Security Exercise CIPC Efforts RCIS OC, PC, CIPC, and associated Subcommittees Spare Equipment Database	**Non-NERC Activities** Local Government: Local Security efforts. North American Generator Forum: Security Practices Working Group, developing education initiatives and best practices. Department of Homeland Security: Protective Security Advisors Federal Bureau of Investigation: Joint Terrorism Task Force Department of Homeland Security /State Police: Fusion Centers

Based on the existing efforts described above:

- Are the existing efforts in this area sufficient?
  While the ERO has worked with industry to produce physical security guidance and the ES-ISAC remains a resource for information sharing, more work should be devoted to ensuring proper protection across North America. Issues that should be looked at further include:
  1. **Shooting of high voltage transmission lines, bushings, and transformers**
  2. **Copper theft**
  3. **Unauthorized access to electric facilities (substations, generation sites, control centers)**
  4. **Security training (bomb threat, piggybacking, suspicious package procedures, security exercises, suspicious activity reporting)**
  5. **Entity response to a coordinated attack on multiple critical facilities**

- Are all of the existing efforts needed? If not, what can be eliminated?
  Yes. No current effort should be eliminated.

- Are any of the existing efforts duplicative of what other organizations are doing?
  No.

- Are any of the existing efforts done in concert with the work of other organizations?
  Yes. For example, the Joint Product Physical Security (JPPS) is a NERC best practices document currently in development, built in conjunction with the Department of Homeland Security, Federal Bureau of Investigation, and the Royal Canadian Mounted Police. The document will address physical security protection measures and provide items for consideration to industry. The GridEx II exercise, scheduled for November 13-14, 2013, will be a physical and cybersecurity exercise with approximately 140 organizations from industry, government, and academia.

- If the existing efforts are not sufficient – what gaps do you see and how do you propose to solve them?

  While NERC has had numerous opportunities for physical security training and the development of relevant guidelines, there are different levels of sophistication and maturity across North America. Some entities are excellent in this area, while others are still learning. Sharing of best practices and collaborating through peer assessments will help ensure maturity in this area is increasing. Peer assessments will suggest industry best practices with a focus on mitigating a single site attack/sabotage or a coordinated physical attack to targeted electrical infrastructure. CIPC guidelines, in conjunction with *American Society for Industrial Security (ASIS International) Physical Security Manual* best practices, can be used to develop a voluntary physical security outreach program that will highlight current practices, inform entities of recent physical security events, and communicate current threats and vulnerabilities. Such an outreach and awareness campaign would focus on learning and advancing the industry to a more consistent and robust physical security posture.

If new efforts are needed:

- Is the new effort within NERC's scope or should it be directed to another organization?
  Yes. However, collaborating with other entities (such at the North American Transmission Forum, the North American Generator Forum, and others) will be essential to ensuring industry experts are sharing their knowledge and entities are receiving information efficiently.

- What gap in existing efforts was identified that this new effort was meant to address?
  While NERC has had numerous opportunities for physical security training and the development of relevant guidelines, there are different levels of sophistication and maturity across North America. Some entities are excellent in this area, while others are still learning. Efforts should be undertaken to increase industry maturity.

- What data is available to scope the new activity?
  Voluntary reporting, lessons-learned from events (PGE Metcalf substation event), and metrics from outside the Electricity Sub-sector to determine can be used to determine general effectiveness.

- How will we measure performance? What metrics will define and track success?

  Success can be measured by increased reporting/engagement to the ES-ISAC, as well as through voluntary reporting and feedback.

Generator Availability **DISCUSSION DRAFT**	An event occurs due to generation not being available when needed (not enough generation operating).		Contributors: • NERC Staff • Planning Committee Chair
Related NERC Standards BAL-001 through -003 IRO-003, -005, -014, -015 MOD-010, -012 TOP-006	**NERC Standards Development Projects** 2010-13.2 Generator Relay Loadability IN PROGRESS ETC Q3 2013 2007-12 Frequency Response PENDING REGULATOR APPROVAL 2010-14.1 Balancing Authority Reliability-Based Controls IN PROGRESS ETC Q4 2013	**Other NERC and Industry Activities** Generating Availability Data System and GADS Working Group Reserve Guideline in development at Operating Committee Information sharing with regulators and NARUC through NERC Reliability Assessments (e.g., LTRA, Special Assessments) and the State of Reliability Report	**Non-NERC Activities** ISOs, RTOs: Market Solutions

Based on the existing efforts described above:

- Are the existing efforts in this area sufficient?
  Yes. These efforts are summarized below, along with a brief description of how the risk is being controlled.

  1. **Generator Outages and Deratings: Generation adequacy in real time is insufficient due to outages or deratings, leading to an inability to balance generation and load.**
     Response: NERC has been collecting generator performance and event data from Generator Owners (GOs) for over three decades. The data is used to calculate important performance statistics and supports bulk power trend analysis by providing information on forced outages, maintenance outages, planned outages, and deratings. NERC also uses historical GADS data to trend outage impact to system reliability, including severity risk index (SRI) curves. The SRI was developed to track annual changes and establish performance reference for the bulk power system's characteristics. The annual SRI curves have been applied prospectively for particular risk events and performance assessments. Other than isolated incidents (such as the February 2011 Southwest Cold Weather Event, which is being addressed through development of a guideline and an education/awareness campaign), trends have not indicated any significant concerns in this area. Any trends identified in this area would be communicated to the industry through NERC's reliability assessments. At this time, this risk seems to be adequately addressed.
  2. **Loss of Fuel: Generation adequacy in real time is insufficient due to a lack of fuel, leading to an inability to balance generation and load.**
     Response: NERC has written a special assessment related to increased dependence on natural gas, highlighting this risk and making specific recommendations. It is anticipated that consideration of this risk will become part of the seasonal and long-term reliability assessments as well. At this time, NERC is relying primarily on voluntary industry actions and the actions of other organizations (e.g., FERC, organized markets, regional study groups, etc…) to address this concern. NERC is also considering enhancing its Generator Availability Data System to track gas-related outages more closely, and will be working with its stakeholder groups to identify lessons learned and common practices. NERC's Planning Committee will be working to establish a task force to consider the benefits or integrated strategic planning efforts between the gas and power industries, with a focus on ensuring fuel supply adequacy.
     Aside from concern with increased natural gas dependence, at this time, this risk seems to be adequately addressed.
  3. **Frequency Responsive Reserve Availability: Frequency recovers slowly following a disturbance due to a lack of Frequency Responsive Reserves.**
     Response: BAL-003 (recently modified as part of Project 2007-12 Frequency Response, which is now pending regulator approval) is intended to address this concern. If future analysis indicates this to be a reliability problem, additional efforts to ensure adequate provision of frequency responsive reserves (e.g., federal, state, or local regulation; market development) may be required in some areas. However, at this time, this risk seems to be adequately addressed.
  4. **Regulating Reserve Availability: System balancing performance is outside expected tolerances due to a lack of Regulating Reserves.**
     Response: BAL-001 (currently being modified as part of 2010-14.1 Balancing Authority Reliability-Based Controls) is intended to address this concern. At this time, this risk seems to be adequately addressed.
  5. **Contingency Reserves Availability: Contingency Reserves are unavailable to replace lost generation, resulting in excessive reliance on Frequency Responsive or Regulating Reserves.**
     Response: BAL-002 (currently being modified as part of 2010-14.1 Balancing Authority Reliability-Based Controls) is intended to address this concern. At this time, this risk seems to be adequately addressed.

- Are all of the existing efforts needed? If not, what can be eliminated?
  Yes.
- Are any of the existing efforts duplicative of what other organizations are doing?
  No.
- Are any of the existing efforts done in concert with the work of other organizations?
  No.
- If the existing efforts are not sufficient – what gaps do you see and how do you propose to solve them?
  Existing efforts are sufficient.

If new efforts are needed: **(No)**

- Is the new effort within NERC's scope or should it be directed to another organization?
- What gap in existing efforts was identified that this new effort was meant to address?
- What data is available to scope the new activity?
- How will we measure performance? What metrics will define and track success?

Increased dependence on Natural Gas Generation **DISCUSSION DRAFT**	An event occurs due to insufficient natural gas deliveries. **NOTE: THIS ISSUE WILL BE CONSOLIDATED AND CONSIDERED WITHIN THE NEW ISSUE, "ADAPTATION AND PLANNING FOR CHANGE," WHICH THE RISC IS RECOMMENDING BE ANALYZED THROUGH THE "RELIABILITY RISK CONTROL PROCESS."**		Contributors: • NERC Staff • Planning Committee Chair
Related NERC Standards None specifically address this issue	**NERC Standards Development Projects** None	**Other NERC and Industry Activities** NERC Reliability Assessments OC, PC, associated Subcommittees	**Non-NERC Activities** State and Local Regulators: Resource Adequacy Provisions ISOs, RTOs, Pipelines: Market Solutions Entities: Planning, Regulatory communications and lobbying Industry: Awareness and Study, Conferences FERC: Technical Conferences; docket on inter-industry coordination NAESB: Gas Electric Harmonization Task Force

Based on the existing efforts described above:

- Are the existing efforts in this area sufficient? **At this time, yes.**
  There are four primary failure modes which need to be considered. These are summarized below, along with a brief description of how the risk is being controlled.
  1. **Electric outages: Load management or forced outages result in the loss of key gas transportation components (e.g., electric compressor stations, electric controls at non-electric compressor stations), leading to further fuel interruptions and generation loss.**
     Response: NERC has written a special assessment, highlighting this risk and making specific recommendations. At this time, NERC is relying on voluntary industry actions and the actions of other organizations (e.g., FERC, organized markets, regional study groups, etc…) to address this concern.
  2. **Gas curtailments: High demand for gas results in insufficient pipeline capacity to serve all customers; using non-firm transportation to supply gas-fired generation results in curtailment of fuel and subsequent loss of the generation.**
     Response: NERC has written a special assessment, highlighting this risk and making specific recommendations. It is anticipated that consideration of this risk will become part of the seasonal and long-term reliability assessments as well. At this time, NERC is relying primarily on voluntary industry actions and the actions of other organizations (e.g., FERC, organized markets, regional study groups, etc…) to address this concern. NERC is also considering enhancing its Generator Availability Data System to track gas-related outages more closely, and will be working with its stakeholder groups to identify lessons learned and common practices.
  3. **Pipeline transportation system fails: A key component of the gas transportation system fails, resulting in the concurrent loss of multiple generation sources.**
     Response: NERC has written a special assessment, highlighting this risk and making specific recommendations. It is anticipated that consideration of this risk will become part of the seasonal and long-term reliability assessments as well. At this time, NERC is relying on voluntary industry actions and the actions of other organizations (e.g., FERC, organized markets, regional study groups, etc…) to address this concern.
  4. **Pipeline and Gas Supply Adequacy: Because of external conditions (e.g., a heat wave), the gas system is unable to meet with firm gas or transportation commitments.**
     Response: The scope and magnitude of this risk is undefined. NERC's Planning Committee will be working to establish a task force to consider the benefits or integrated strategic planning efforts between the gas and power industries, with a focus on ensuring fuel supply adequacy.
- Are all of the existing efforts needed? If not, what can be eliminated?
  Yes.
- Are any of the existing efforts duplicative of what other organizations are doing?
  No. While many regions (e.g., planning coordinators, groups of planning coordinators, interconnection/regional study groups) are performing studies, regional differences and challenges must be uniquely studied.
- Are any of the existing efforts done in concert with the work of other organizations?
  Yes. NERC has undertaken its research of this issue in close collaboration with other entities from both the power and natural gas industries.
- If the existing efforts are not sufficient – what gaps do you see and how do you propose to solve them?
  At this time, we believe existing efforts are sufficient. However, close monitoring of this issue is appropriate to ensure it is being properly addressed. Reliability assessments are a key tool NERC can leverage to support tracking and trending of this issue.

If new efforts are needed: **(No)**

- Is the new effort within NERC's scope or should it be directed to another organization?
- What gap in existing efforts was identified that this new effort was meant to address?
- What data is available to scope the new activity?
- How will we measure performance? What metrics will define and track success?