NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Severe Impact Resilience: Considerations and Recommendations

Severe Impact Resilience Task Force

Board of Trustees Accepted: May 9, 2012

RELIABILITY | ACCOUNTABILITY




NERC's Mission

The North American Electric Reliability Corporation (NERC) is an international regulatory authority established to enhance the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; assesses adequacy annually via a ten-year forecast and winter and summer forecasts; monitors the BPS; and educates, trains, and certifies industry personnel. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the U.S. Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada.[1]

NERC assesses and reports on the reliability and adequacy of the North American BPS, which is divided into eight Regional areas, as shown on the map and table below. The users, owners, and operators of the BPS within these areas account for virtually all the electricity supplied in the U.S., Canada, and a portion of Baja California Norte, México.

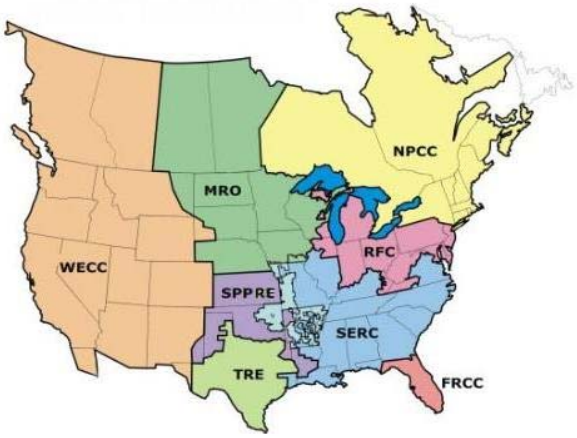


Table A: NERC Regional Entities	
FRCC Florida Reliability Coordinating Council	**SERC** SERC Reliability Corporation
MRO Midwest Reliability Organization	**SPP** Southwest Power Pool, Incorporated
NPCC Northeast Power Coordinating Council	**TRE** Texas Reliability Entity
RFC Reliability*First* Corporation	**WECC** Western Electricity Coordinating Council

Note: *The highlighted area between SPP and SERC denotes overlapping regional area boundaries: For example, some load serving entities participate in one region and their associated transmission owner/operators in another.*

[1] As of June 18, 2007, the U.S. Federal Energy Regulatory Commission (FERC) granted NERC the legal authority to enforce Reliability Standards with all U.S. users, owners, and operators of the bulk power system, and made compliance with those standards mandatory and enforceable. In Canada, NERC presently has memorandums of understanding in place with provincial authorities in Ontario, New Brunswick, Nova Scotia, Québec, and Saskatchewan, and with the Canadian National Energy Board. NERC standards are mandatory and enforceable in Ontario and New Brunswick as a matter of provincial law. NERC has an agreement with Manitoba Hydro making reliability standards mandatory for that entity, and Manitoba has recently adopted legislation setting out a framework for standards to become mandatory for users, owners, and operators in the province. In addition, NERC has been designated as the "electric reliability organization" under Alberta's Transportation Regulation, and certain reliability standards have been approved in that jurisdiction; others are pending. NERC and NPCC have been recognized as standards-setting bodies by the Régie de l'énergie of Québec, and Québec has the framework in place for reliability standards to become mandatory. NERC's reliability standards are also mandatory in Nova Scotia and British Columbia. NERC is working with the other governmental authorities in Canada to achieve equivalent recognition.

Table of Contents

1.0 Executive Summary

The North American bulk power system (BPS) is one of the most critical of infrastructures, vital to society in many ways, but it is not immune to severe disruptions that could threaten the health, safety, or economic well-being of the citizens it serves. The electric power industry has well established planning and operating procedures in place to address "normal" emergency events (e.g., hurricanes, tornadoes, ice storms) that occur from time to time and disrupt electric reliability. However, the electricity industry has much less experience with planning for and responding to high-impact events that have a low probability of occurring.

To help the electricity industry better understand these low probability risks, NERC and the U.S. Department of Energy (DOE) issued a report titled, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System"[2]. Subsequently, the NERC Board of Trustees approved a Coordinated Action Plan under the leadership of the NERC Technical Committees to establish four Task Forces to address this work. This report provides the conclusions of the Severe Impact Resilience Task Force (SIRTF).

The report provides guidance to industry asset owners and operators (entities) in the form of recommendations to enhance the resilience of the bulk power system. Three high-impact, low frequency (HILF) scenarios were specifically considered as the initiating events, but the recommendations in this report may be applicable to any severe-impact scenario.

- **Coordinated physical attack** – A coordinated physical attack on key nodes of the BPS critically disables difficult to replace equipment in multiple generating stations or substations and could have a significant effect on the remainder of the system. A prolonged period of time is required to fully restore the BPS to normal operation.
- **Coordinated cyber attack** – A coordinated disruption disables or impairs the integrity of multiple control systems, or intruders take operating control of portions of the BPS such that generation or transmission system is damaged or mis-operated.
- **Geomagnetic disturbance**[3] – A severe geomagnetic disturbance damages difficult to replace generating station and substation equipment and causes a cascading effect on the remainder of the system. A prolonged period of time is required to fully restore the BPS to normal operation.

The report offers 33 key recommendations that are of a planning and operational nature, and entities are strongly encouraged to consider these from a strategic and leadership perspective, in particular:

- Enhance existing restoration drills and exercises to incorporate HILF scenarios that include interdependencies with other critical infrastructures such as telecommunications.

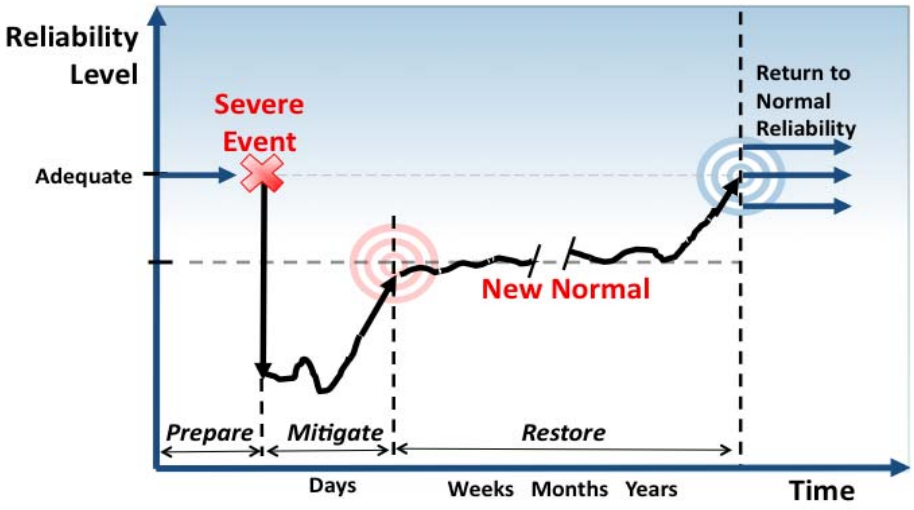
[2] Ref. High Impact Low Frequency report http://www.nerc.com/files/HILF.pdf

[3] Ref. *Interim Report: Effects of Geomagnetic Disturbances on the Bulk Power System* http://www.nerc.com/files/2012GMD.pdf. This report concluded that the loss of reactive power is the most likely outcome from a severe solar storm centered over North America.

- Recognize that plans and operating practices will need to be continually assessed and adjusted as necessary over an extended period that could last months or years following a severe event.
- Involve neighboring jurisdictions and government agencies by sharing plans and building a better understanding of how these plans will be coordinated and implemented.

Understanding a Severe Event

The guidance offered in this report is intended to reach beyond the emergency response capabilities entities typically have in place. To emphasize this, the SIRTF developed two important concepts that run throughout this report; Severe Event and New Normal. A Severe Event is an emergency situation so catastrophic that complete restoration of electric service is not possible. The BPS is operated at a reduced state of reliability and supply for months or possibly years through the New Normal period as illustrated below.



Enhancing Resilience

By definition, a Severe Event will present enormous challenges as entities within the electricity industry strive to restore and maintain reliable operations under rapidly changing circumstances never before experienced. It will not be possible to meet all electricity consumers' demands for rapid restoration of service as entities prioritize their work with limited resources. The recommendations and suggestions offered throughout this report are intended to prompt BPS entities to develop their own approaches and flexible plans that would be applicable under a wide variety of circumstances. These suggestions are in the form of industry guidelines that describe practices that may be used by individual entities according to local circumstances, as opposed to standards.

Recommendations

The SIRTF has considered what aspects of emergency operation and restoration would be particularly challenged through a Severe Event and considered options to enhance the resilience of the BPS. Entities are encouraged to consider how they might apply the recommendations offered in this report to their own circumstances in a Severe Event scenario. Entities are encouraged to test their plans through drills or exercises that build further on the Severe Event scenarios.

The following summarizes the key recommendations of this report and are described in the body of the report in further detail.

Operations

The Operations section of this report discusses the many challenges associated with operating the BPS following a Severe Event. Rather than operating as part of a large interconnected (and therefore more stable) grid, system operators may need to manage a number of small electrical islands and implement load shedding or rotating blackouts for extended periods of time (weeks, months or years). The Operations section proposes that entities consider the following key recommendations.

1. Consider which entities would take the independent actions and the tools needed to stabilize islands when communications capability is severely disrupted or unavailable.
2. Consider how operating reserve would be managed during islanded operation and frequent periods of insufficient supply to meet demand.
3. Consider ways to adopt and apply the terms critical load and priority load across all BPS entities to improve consistent use during a Severe Event.
4. Consider alternate means to dispatch generation if normal automated systems, including automatic generation control, are unavailable.
5. Consider if or how variable generation would be dispatched through restoration and islanded operation.
6. Consider enhancing regular restoration drills and exercises to train staff on communication protocols and independent control actions in the event of loss of or degraded telecommunications.
7. Consider using more extreme exercise scenarios that involve simulated rotating blackouts and islanded operations on a larger scale and for extended periods of time.

Monitoring the Bulk Power System

The Monitoring the BPS section discusses the challenges associated with maintaining situational awareness in order to operate the BPS following a Severe Event. A Severe Event may disrupt the flow of data, tools, or facilities needed to operate the BPS. Alternate mechanisms and processes would be needed to maintain a wide area view of situational awareness when it is more important than ever. The Monitoring the BPS section proposes that entities consider the following key recommendations.

8. Consider developing processes to quickly study island configurations and develop suitable temporary operating limits.
9. Consider developing processes to monitor BPS flows in the absence of reliable automated systems and communications.
10. Consider the simultaneous loss of primary and backup control centers and how essential functions will continue to be performed.

Communications

The Communications section discusses the challenges associated with restoring and operating the BPS when communications facilities are severely degraded or unavailable. The Communications section proposes that entities consider the following key recommendations.

11. Consider installing renewable generation (e.g., wind, solar) or expanding fuel storage capabilities at critical BPS facilities to supplement standby generators.
12. Consider alternate means to communicate when primary means of communication are completely unavailable for extended periods of time.
13. Consider robust training, drills, and exercises to fully test critical restoration steps using alternative voice and data communications (e.g., satellite telephones).

Short-term and Long-term System Planning

The Short-term and Long-term System Planning section discusses the challenges associated with providing sufficient personnel and facilities to prepare the necessary system studies and plans needed to support restoration and long-term recovery. This section proposes that entities consider the following key recommendations.

14. Consider the potential loss of planning resources (e.g., equipment, data) as well as damage to the system. Review business continuity plans to ensure that system planning resources are adequately considered.
15. Consider the appropriate use of key system planners who may be required immediately, and for prolonged periods, to perform studies not previously considered.
16. Consider performing selected studies in advance (e.g., equipment interchangeability) that could help speed restoration.
17. Consider the spare equipment critical to BPS restoration and ways to improve availability of these spares.

Protection and Control

The Protection and Control section discusses the challenges associated with safely operating the BPS as its configuration continues to change to respond to the loss or unavailability of critical elements. This section proposes that entities consider the following key recommendations.

18. Consider ways to implement large-scale changes in system protection schemes to support islanded operation and changing BPS configurations, and what decision points would be needed.
19. Consider ways to quickly reconfigure relay settings in the event large-scale changes are needed.

Interdependencies with Other Critical Infrastructures

The Interdependencies with Other Critical Infrastructures section discusses the contribution and impact that other industries such as communications, oil and natural gas, and water have on the ability of the electricity industry to restore and operate the BPS. This section proposes that entities consider the following key recommendations.

20. Consider working with communications service providers to identify which of their facilities are critical to BPS operations. Determine which BPS and distribution facilities supply them and what backup power capacity is in-place (e.g., batteries, standby generators).
21. Consider alternate suppliers, transportation paths, and agreements to support generating station fuel supply chains (e.g., coal, natural gas).
22. Consider working with information technology service providers that are critical to BPS operations and consider augmenting the subject matter expertise of staff and suppliers to support these systems.
23. Consider alternate means to supply BPS power to nuclear plants and confirm these loads as critical to restoration and public safety.

Coordination with Government

The Coordination with Government section discusses the need to build effective relationships with the appropriate government agencies in order to help manage serious public health and safety issues. This section proposes that entities consider the following key recommendations.

24. Confirm the roles, authorities, and points of contact between BPS entities and as appropriate, local, state/provincial, and federal governments.
25. Coordinate with local and state/provincial government authorities and consumer stakeholders to identify priority loads to mitigate the impact on public health and safety.
26. Consider developing a list of regulatory exemptions or waivers that will materially improve restoration and operation (e.g., plant emissions, truck driver hours) and consult with state/provincial and federal agencies.

Taking Care of People

The Taking Care of People section discusses how entities can assist with the extraordinary demands that employees and their families may face. This section proposes that entities consider the following key recommendation.

27. Consider ways to support the health, safety, and well-being of personnel and their families in the face of extraordinarily demanding circumstances.

Logistics and Self-Sustained Operations

The Logistics and Self-Sustained Operations section discusses the challenges associated with the logistics of acquiring the equipment needed to restore and operate the BPS. This section proposes that entities consider the following key recommendations.

28. Consider with fuel suppliers ways to prioritize the supply and delivery of fuel for emergency standby generators and essential work vehicles.
29. Consider how your business continuity or disaster recovery plan would change if you are unable to rely on mutual support arrangements.

Preventing and Responding to Physical Attacks

The Preventing and Responding to Physical Attacks section discusses the unique challenges associated with physical attacks. This section proposes that entities consider the following key recommendations.

30. Consider actions that can be taken to protect BPS assets by involving local communities and law enforcement (e.g., reinforcing their awareness of BPS facilities that are critical to operations).
31. Consider ways to improve security when designing or refurbishing existing BPS facilities.
32. Consider ways to improve coordination and cooperation with local/state/provincial law enforcement.

Emergency Financing

The Emergency Financing section briefly discusses the challenges associated with the extraordinary requirements for funds needed to restore the BPS when major facilities need to be rebuilt or replaced. This section proposes that entities consider the following key recommendation.

33. Consider how extreme financial challenges will be addressed in consultation with financial institutions, suppliers, and government agencies.

Conclusions

This report addresses important aspects related to enhancing the resilience of the bulk power system in the face of a Severe Event. It provides entities with practical options to enhance their capabilities to prepare, mitigate and restore the operation of the bulk power system.

Recommendations for Entity Action

This report examines the aspects of emergency operation and restoration that would be particularly challenged through a Severe Event and provides options to enhance the resilience of the bulk power system. The suggestions offered throughout this report are intended to prompt entities to develop their own approaches and flexible plans that would be applicable under a wide variety of circumstances. This report considers all aspects of resilience; robustness, resourcefulness, rapid recovery, and adaptability. Entities are encouraged to critically examine their current capabilities, and to consider what else they may need to do to manage restoration and operations during a Severe Event.

While the report offers 33 key recommendations that are of a planning and operational nature, entities are strongly encouraged to consider these from a strategic and leadership perspective, in particular:

- Enhance existing restoration drills and exercises to incorporate Severe Event scenarios that include interdependencies with other critical infrastructures such as telecommunications.
- Recognize that plans and operating practices will need to be continually assessed and adjusted as necessary over an extended period that could last months or years following a Severe Event.
- Involve neighboring jurisdictions and government agencies by sharing your plans and building a better understanding of how these plans will be coordinated and implemented.

NERC's Reliability Standards under a Severe Event

While this report does not propose that new standards be developed to address a Severe Event, as entities consider and implement the recommendations in this report there may be opportunities to enhance existing standards.

The SIRTF discussed the applicability of the NERC[4] standards through a Severe Event, and whether entities should be exempt from possible compliance actions[5] under these circumstances. The SIRTF reviewed the NERC standards and concluded that standards support safe and reliable operation and should be applicable during a Severe Event. While it is conceivable that during a Severe Event an entity will violate certain standard requirements given the intensity of planning and operating challenges through the New Normal period, it would be impossible to predict these circumstances in advance.

[4] Ref. NERC Standards, http://www.nerc.com/page.php?cid=1|7

[5] NERC has the legal authority to enforce compliance with NERC Reliability Standards, which it achieves through a rigorous program of monitoring, audits and investigations, and the imposition of financial penalties and other enforcement actions for non-compliance.

On balance, the SIRTF concluded that entities do not need guidance on the applicability of standards during a Severe Event. Although a Severe Event may put entities in a position where they cannot comply with all standards, entities are in the best position to "do the right thing" for reliability and public safety, and self-report any violation of NERC standards as time and circumstances permit.

Acknowledgements

This report was prepared by a team of industry subject matter experts with a broad understanding of what is needed to respond to emergency situations to reliably restore and operate the interconnected bulk power system. They contributed their knowledge, experience, and time to the SIRTF in technical areas such as power system operation, transmission planning, generating plant operation, protection and control, distribution operations, communications, logistics, emergency planning, crisis response, and cyber and physical security.

Members of the SIRTF Report Drafting Team are identified in Appendix 7 of this report.

Many other SIRTF members provided valuable feedback and are identified in Appendix 6.

2.0 Introduction

The North American bulk power system (BPS) is one of the most critical of infrastructures and is vital to society in many ways. The electric power industry has well established planning and operating procedures in place to address the "normal" emergency events (e.g., hurricanes, tornadoes, ice storms) that occur from time to time and disrupt electricity reliability[6]. However, the electricity industry has much less experience with planning for and responding to high-impact events that have a low probability of occurring or have not yet occurred.

To help the electricity industry better understand these low probability risks, in June 2010, NERC and the U.S. Department of Energy issued a report titled, "*High-Impact, Low-Frequency Event Risk to the North American BPS*"[7]. In November 2010, the NERC Board of Trustees (BOT) approved the Electricity Sub-sector Coordinating Council's (ESCC) *Critical Infrastructure Strategic Roadmap*[8] that provides the framework to identify the actions needed to enhance reliability and resilience under these high-impact low-frequency (HILF) scenarios. At the same time, the NERC board approved a *Coordinated Action Plan*[9] developed by NERC and the leadership of the NERC Technical Committees that identifies specific initiatives, key deliverables, and milestones to implement the ESCC's Strategic Roadmap. The Coordinated Action Plan identified four Task Forces needed to address this work. This report provides the conclusions of one of them – the SIRTF.

The SIRTF was established in December 2010 by the NERC Operating Committee to develop guidance and options to enhance the resilience of the bulk power system to withstand and recover from three severe-impact HILF scenarios:

- Coordinated physical attack
- Coordinated cyber attack
- Geomagnetic disturbance[10]

This effort has challenged the SIRTF in a number of ways.

- The industry has already demonstrated its ability to respond to large-scale emergencies such as the 2003 Northeast Blackout, Hurricane Katrina and more recently Hurricane Irene using flexible response plans that are designed to be effective regardless of the cause or

[6] Ref. NERC Adequate Level of Reliability
http://www.nerc.com/docs/standards/Adequate_Level_of_Reliability_Defintion_05052008.pdf
[7] Ref. High Impact Low Frequency report http://www.nerc.com/files/HILF.pdf
[8] Ref. Critical Infrastructure Strategic Roadmap
http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf
[9] Ref. Coordinated Action Plan
http://www.nerc.com/docs/ciscap/Critical_Infrastructure_Strategic_Initiatives_Coordinated_Action_Plan_BOT_Apprd_11-2010.pdf
[10] Ref. *Interim Report: Effects of Geomagnetic Disturbances on the Bulk Power System* http://www.nerc.com/files/2012GMD.pdf. This report concluded that the loss of reactive power is the most likely outcome from a severe solar storm centered over North America.

consequences of the event. As a result, some entities may feel they are already prepared and nothing more needs to be done.

- By definition, high-impact, low-frequency (HILF) events have rarely or never occurred, and therefore it is very difficult to determine with confidence what additional action is required even by industry experts who are responsible for planning and operating the BPS through extreme emergency events. The Tohoku, Japan earthquake and tsunami that devastated the Fukushima nuclear plant is a vivid reminder that HILF events can occur.
- The postulated HILF events could cause service disruptions lasting weeks, months and perhaps years – well beyond the industry's experience over the past 100 years of reliable operation.

The SIRTF has recognized these challenges and through this report offers the electricity industry a wide range of suggestions and ideas. The diverse nature of HILF events does not lend itself to technical engineering solutions broadly applicable across the electricity industry. Therefore, the report does not propose mandatory requirements. Instead, the report offers suggestions and ideas to entities that own or operate the BPS. Entities are encouraged to consider these suggestions and apply them according to their own local circumstances and needs.

The SIRTF considered what aspects of emergency operation and restoration would be particularly challenged through these severe-impact events, and considered options to enhance the resilience of the BPS. In many cases, the suggestions can be applied to any HILF scenario, regardless of the specific threat.

2.1 Background and Key Concepts

At an early stage in its work, it became apparent that SIRTF members had different experiences and therefore no common view of what is meant by terms such as "severe impact" event, "resilience", and "New Normal" operation. The SIRTF needed to define these terms so that members would have a common platform from which to propose solutions that build on the electricity industry's current ability to respond to emergencies and prepare for worse in a consistent manner.

2.1.1 Use of Terms

A number of technical terms related to the planning and operation of the BPS are used throughout this report. Please refer to the NERC Glossary of Terms[11] for definitions.

2.1.2 Understanding a Severe Impact Event

A severe impact event (Severe Event) means that complete restoration is not possible and the BPS is operated at a reduced state of reliability and supply for an extended period of time, for months or possibly years – a New Normal. The following describes a Severe Event; one that stresses the electricity industry's capabilities well beyond its already robust emergency response capabilities.

[11] Ref. NERC Glossary of Terms http://www.nerc.com/files/Glossary_12Feb08.pdf

2.1.3 Impact of a Severe Event on the Bulk Power System

- The event is beyond the planning criteria provided by NERC planning standards[12], such as System Performance Following Extreme BES Events.
- The event is beyond the scenarios typically exercised by entities as part of the NERC Emergency Preparedness and Operations standards[13].
- It is expected to take six months to a year to return the BPS to pre-event operations.
- As a result of insufficient generation and transmission resources, system operators must shed load without advanced notice and regularly implement rotating blackouts to manage BPS reliability.
- The duration and magnitude of these rotating blackouts have a direct societal impact and risk further degradation to the BPS as other critical infrastructures are affected by the electricity disruptions.
- Multiple information technology and communications systems have failed – entities contend with issues that restrict the ability of system operators to effectively communicate, operate, and monitor the BPS.
- The event is persistent or recurring throughout the mitigation and restoration phases, further hindering recovery and restoration.

2.1.4 Impact of a Severe Event on Society

- The media or government authorities describe the magnitude of the event using words such as “catastrophe”, “disaster” or “massive disruption”.
- BPS entity staff experience a high degree of physical and psychological demands for an extended period of time.
- The safety and well being of large numbers of the public, entity staff, or their families are at risk.
- The resources required to respond exceed the financial capacity of some entities.

2.1.5 Understanding Resilience

“Resilience” is generally defined as the ability to recover or adjust to misfortune or change. More specifically, the ASIS SPC.1-2009 standard on Organizational Resilience[14] defines, “Resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event.” In recent years, in the context of strategies needed to enhance the reliable operation of critical infrastructures, resilience has come to be valued as much as protection. But what exactly is meant by resilient critical infrastructures? How is resilience measured and how do we determine how much is needed?

[12] Ref. NERC standard TPL-004, ref. http://www.nerc.com/files/TPL-004-0.pdf
[13] NERC Emergency Planning and Operations standards, ref. http://www.nerc.com/page.php?cid=2|20
[14] ASIS SPC.1-2009, http://www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf

In October 2010, a study group[15] of the National Infrastructure Advisory Council issued its report "*A Framework for Establishing Critical Infrastructure Resilience Goals*[16]". The report provides a broader construct for resilience originally conceived by resilience expert Stephen Flynn. The construct is based on four features organized in a sequence of events prior to, during, and after a Severe Event.

Infrastructure Resilience

Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.

[15] The NIAC Study Group included a number of representatives from the electricity industry, including several members of the Electricity Sub-sector Coordinating Council.

[16] Ref. http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf

Figure 1: NIAC Resilience Construct

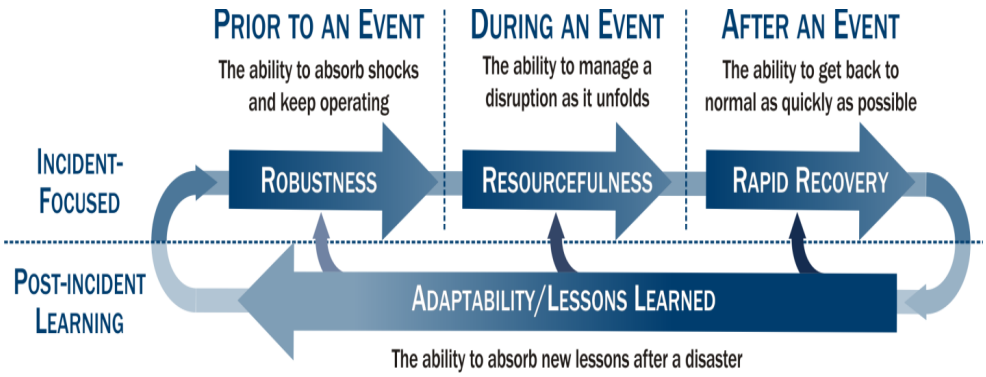


Table 1: NIAC Resilience Construct	
Sequence	**Feature**
Prior to an Event	**Robustness**—The ability to keep operating or to stay standing in the face of disaster. In some cases, it translates into designing structures or systems to be strong enough to take a foreseeable punch. In others, robustness requires devising substitute or redundant systems that can be brought to bear should something important break or stop working. Robustness also entails investing in and maintaining elements of critical infrastructure so that they can withstand low-probability but high-consequence events.
During an Event	**Resourcefulness**—The ability to skillfully manage a disaster as it unfolds. It includes identifying options, prioritizing what should be done both to control damage and to begin mitigating it, and communicating decisions to the people who will implement them. Resourcefulness depends primarily on people, not technology.
After an Event	**Rapid recovery—** The capacity to get things back to normal as quickly as possible after a disaster. Carefully drafted contingency plans, competent emergency operations, and the means to get the right people and resources to the right places are crucial.[17]
At All Times	**Adaptability—** The means to absorb new lessons that can be drawn from a catastrophe. It involves revising plans, modifying procedures, and introducing new tools and technologies needed to improve robustness, resourcefulness, and recovery capabilities before the next crisis.

[17] "Rapid" recovery as used by the SIRTF does not mean rapid recovery to the pre-crisis operational level but to the New Normal.

2.1.6 Understanding the New Normal

North America's bulk power system is one of the most reliable in the world. BPS owners and operators consistently demonstrate their ability to respond to emergencies and restore service under the most challenging and adverse circumstances.

Emergency Restoration

The entities that operate North America's bulk power system are well practiced in preparing for and responding to emergencies. North America experiences far more severe weather events such as hurricanes, tornadoes, and ice storms than any other continent. This challenge will continue, as extreme weather events appear to be increasing in both frequency and intensity.

The electricity industry makes extensive use of emergency and business continuity planning, risk modeling, supply chain management, accountable organizational structures, emergency exercises, tabletop drills, operator training, safety procedures, redundant and backup systems, mutual assistance, and effective operational communications protocols.

While this industry-wide capability has proven effective in responding to the "normal" emergencies entities face from time-to-time, it is unlikely to be sufficient through a Severe Event. The SIRTF uses the term "New Normal" to describe degraded planning and operating conditions unlike anything the industry has ever experienced in North America that could exist for months or years.

Figure 2: Severe Event Phases

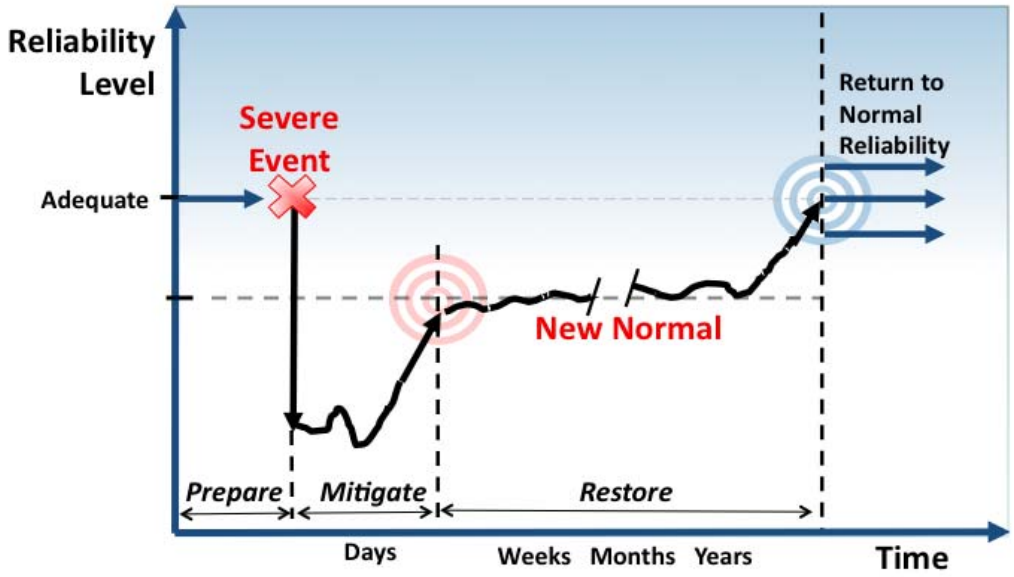


Table 2: Severe Event Phases		
Phase	**Duration**	**Characteristics**
Prepare	At all times	Entities enhance existing and develop new emergency response capabilities.
Mitigate	Days	Entities implement plans to minimize the impact on BPS equipment and maximize electricity service to consumers. Resources such as reserve capacity, spare equipment, and personnel are inadequate to return the BPS to normal operation.
Restore	Weeks, months, possibly years.	There is a risk that further Severe Events may occur. Resources such as personnel, spare equipment, and manufacturing capacity become increasingly limited. Other critical infrastructures are affected, reducing communications services and the availability of water, food, fuel, medical care, fire and police response. Over time, consumer load patterns change as people re-locate or implement their own energy solutions.
Return to Normal Reliability	Months, possibly years.	Reliability may not return to pre-event levels. Lessons-learned from the event may eventually increase reliability in some areas as the BPS is reinforced, or decrease in other areas where consequences of the event continue to impose operational limitations.

2.1.7 New Normal Challenges

The following describes some of the challenges that would need to be managed through the weeks and months of New Normal operation. This is not an exhaustive list and is intended to illustrate conditions that owners and operators have not yet experienced and may have difficulty imagining.

- Although power is reliably restored to some consumers, planned and unplanned rotating blackouts disrupt service without warning as system operators manage BPS reliability with limited generation and transmission resources and unfamiliar operating conditions.
- Equipment damage and resource limitations force the BPS to be operated as a number of electrically disconnected islands, reducing the stability and reliability inherent in the large interconnected BPS.
- Other critical infrastructures are affected by electricity disruptions. For example, gasoline and diesel fuel shortages will occur as oil refineries take several days or longer to recover from each electricity service disruption.
- System operators need to dispatch generation and operate the transmission system manually using verbal direction that increases the likelihood of human error. Sporadic or limited electronic communications mean system operators need to rely on hardcopy documents that are less frequently updated.
- As a result of reduced generation and transmission resources and uncertain operating conditions, the BPS is operated with reduced efficiency and requires a larger margin of operating reserve, further aggravating the shortage of generation.
- Consumers experience large fluctuations in voltage and frequency that may trip sensitive electronic equipment.
- System protection devices configured for normal operation may be too restrictive for the voltage, current, and frequency variations inherent in a degraded operating state and would need to be adjusted to reflect these different operating conditions.
- Disrupted or unreliable automated trading or tagging systems limit the ability of balancing authorities and reliability coordinators to schedule and manage electricity flows between balancing areas.
- Extreme workload pressures on system operators, engineers, and other personnel limit the ability to meet certain standards requirements that do not compromise safe and reliable operations.

2.1.8 The Applicability of NERC Standards During a Severe Event

By definition, a Severe Event will present enormous challenges to electricity entities as they strive to restore and maintain reliable operations under rapidly changing circumstances never before experienced. It will not be possible to meet all electricity consumers' demands for early service restoration, as entities prioritize their work with limited human and material resources.

The SIRTF discussed the applicability of the NERC[18] standards under these circumstances, and whether entities should be exempt from possible compliance actions[19] through a Severe Event. The SIRTF reviewed the NERC standards and concluded that the vast majority of the standards support safe and reliable operation that would be equally applicable during a Severe Event, as they would during normal operation. While it is conceivable that an entity may decide to violate a certain standard in order to accelerate broader restoration objectives, it would be impossible to predict these circumstances in advance of any event, let alone a Severe Event.

Some of the NERC standards are administrative in nature and require, for example, that entities perform periodic documentation reviews in order to demonstrate compliance with the standards. Clearly, these activities would not be considered a high priority during a Severe Event. While there may be some merit in identifying these "administrative" standards as not applicable during a Severe Event, on balance, the SIRTF felt any discussion of standards and compliance during an event may be more of a distraction for entities, rather than help them remain focused on making the right operational decisions. Furthermore, as NERC's standards are evolving, and efforts are being made for all standards to become more performance and outcome-based. Over time, this will reduce or eliminate standards that are administrative in nature.

On balance, the SIRTF concluded that entities do not need guidance on the applicability of standards during a Severe Event. Although a Severe Event may put entities in a position where they cannot comply with all standards, entities are in the best position to "do the right thing" for reliability and public safety, and self-report any violation of NERC standards as time and circumstances permit.

[18] Ref. NERC Standards, http://www.nerc.com/page.php?cid=1|7

[19] NERC has the legal authority to enforce compliance with NERC Reliability Standards, which it achieves through a rigorous program of monitoring, audits and investigations, and the imposition of financial penalties and other enforcement actions for non-compliance.

3.0 Operations

This section identifies the challenges associated with operating the BPS following a Severe Event. Many aspects of operations in the New Normal are not entirely different from what entities have experienced to date but will be much more challenging for a number of reasons. For example, island operation in itself is nothing new – the North American grid is operated in four large islands known as the Interconnections. The challenge in operating islands following a Severe Event scenario is that the islands will be much smaller, more numerous, may comprise areas that fall under the authority of several different operating entities, and last for significantly longer periods of time (weeks, months or years) than previously experienced. Load shedding activities are also likely to be similar to, and very likely based upon, existing load shedding and rotating blackout plans required to respond to EEA-3 conditions (interruption of firm load). However, experience with implementing load shedding plans has been limited to relatively short periods of time – a few hours or at most a day or two. In contrast, under Severe Event conditions, rotating blackouts may need to be implemented for an extended period of time and for significantly longer rotation intervals.

Following a Severe Event on the BPS entities should expect that it will not be possible to fully restore the BPS to pre-event conditions and the system will be significantly degraded. In order to operate the BPS it will likely be necessary to operate in multiple electrical islands[20], and use emergency criteria, rotating blackouts, and a number of independent control actions[21] to maintain the supply and demand balance and manage frequency and voltage. Rotating blackouts help manage the supply and demand balance by rotating supply to different blocks of load, typically on a geographic basis, on a defined schedule or timeline.

The operation of these electrical islands may need to be performed by entities that are not normally responsible for system operator[22] functions such as Distribution Providers. As a result, these entities could become the system operator until such time as control is returned to the Balancing Authority or Transmission Operator for the balancing area. Following a Severe Event, it is not possible to predict what islands will be formed and this is further complicated when these island boundaries cross the balancing areas that are very familiar during normal operation. In fact, this occurred following the August 14, 2003 blackout that affected large portions of the Midwest and Northeast United States and Ontario (see sidebar).

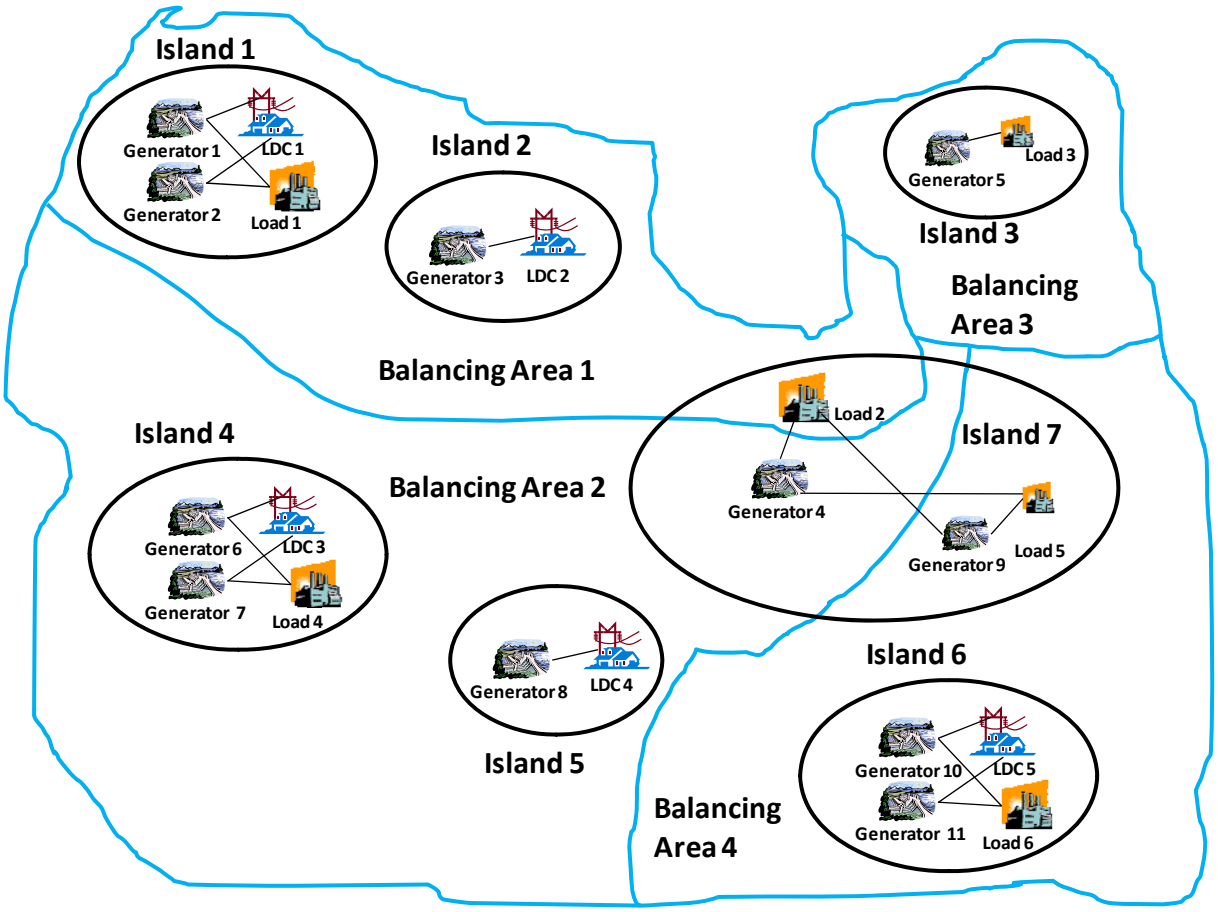
Islanding Experience from the 2003 Northeast Blackout

Ontario's Beck and Saunders hydroelectric stations, along with some Ontario load, the New York Power Authority's Niagara and St. Lawrence hydroelectric stations and 765 kV AC interconnection with Quebec, remained connected to the western New York system, supplying load in upstate New York immediately following the event.

[20] Islanding is the complete separation of a portion of the power system from the remaining interconnected system following a system disturbance. Islands can be comprised of generation sources, transmission elements, distribution elements and loads.
[21] Independent actions are those operating actions required to enable power system restoration without prior communication to the Reliability Coordinator for approval.
[22] A System Operator is anyone who performs the system operator function as defined in NERC's Glossary of Terms.

The following diagram illustrates a likely scenario following a Severe Event. The BPS may form islands that do not respect traditional operator boundaries. While many islands depicted are within a single Balancing Authority (BA) Area, Island 7 is shown to exist in three distinct Balancing Areas.

Figure 3: Islanded Operation



The following sections provide more details around these challenges and the need for delegated authority and independent actions.

Assumptions

This section assumes that a substantial number of supply resources are unavailable for an extended period of time and as much as or more than 50% of total instantaneous demand cannot be served in the islands. The cause(s) for this inability may vary significantly and are not limited to a lack of generation resources. The situation may be extremely widespread or it could be limited to specific areas within a single balancing area. At least initially, communication and control is impaired such that at least a portion of switching will need manual operations by field personnel.

3.1 Immediate Automatic Response

Immediately following the Severe Event, islands are likely to form as transmission lines between areas of the system trip. Automatic under-frequency load shedding and generator tripping may also occur as protective relays react to the transient voltages, frequency and power flows caused by the separation. Islands with small amounts of generation and load have less inertia and as such experience larger frequency swings, are harder to control, and are more likely to collapse from subsequent generation loss than are the existing four Interconnections.

Also, many of today's loads are frequency or voltage sensitive or both (such as computers, industrial control systems, other electronic devices) and may trip off-line as a result of these swings. The challenge with frequency or voltage sensitive load loss is that it will come back on the system once electrical parameters are within the prescribed range. Also this can be further complicated with the increase in automatic schemes within the distribution system for "self healing" (smart grids). This uncoordinated load restoration possibly increases the risk of island collapse.

Recommendations

Entities should develop policies on how to treat smart grid components and frequency or voltage sensitive loads in islanding situations. The appropriate management of these components will increase situational awareness.

3.2 Operational Authority

Following the immediate, automatic system response, it is critical to determine the extent of the islands and which entity(s) are in "control" of the surviving islands. This determination would likely be made by the Transmission Operators (TOP). To be in control of an island an entity needs to have the ability and decision making authority to monitor and control the assets (generation, transmission and load) within the island's boundaries. Decisions may include the need to shed load, dispatch generation, put equipment in service, etc. Although the Reliability Coordinator maintains overall responsibility of the BPS, including the synchronization[23] of the islands, it may not have sufficient monitoring and communication to direct the operation of each island. With limited or no communication it is important that each of the entities know what independent actions they should take on loss of BPS supplied power.

Recommendations

- Reliability Coordinators and Balancing Authorities should consider developing loss of communications and delegation protocols for responsible entities in their footprint and

[23]Synchronization is the closing of a circuit breaker between two electrically disconnected, energized parts of the power system. When synchronizing islands it is crucial to match voltages on both sides of the circuit breaker before closing. If this matching or "synchronizing" process is not done correctly, a power system disturbance will result and equipment (including generators) can be damaged. In order to synchronize properly, three different aspects of the voltage across the circuit breaker must be closely monitored. The three aspects of the voltage are called the synchronizing variables and are:
1. The voltage magnitudes
2. The frequency of the voltages
3. The phase angle difference between the voltages

with adjacent Reliability Coordinators and BA to allow seamless transfer to the responsible entity during loss of communication or monitoring scenarios or when islands cross jurisdictions.

- Establish and practice through simulation or tabletop exercises the independent actions that entities are expected to take upon loss of BPS supplied power. This might include:
  - TOP, Local Distribution Companies and directly connected wholesale customers opening all de-energized breakers under their operational control.
  - Generator Operators (GO) opening all de-energized unit and switchyard circuit breakers under their direct operational control, and beginning blackstart procedures for certified blackstart facilities.
  - GO securing station service with any available generation units in accordance with local instructions and agreements. This may include restarting hydroelectric generation units to run them at speed-no-load by closing the unit breaker (using synch bypass or synchronizing to other units).
  - For generation facilities with the capability to energize-out a portion of the BPS, GO would stabilize units and prepare them to energize transmission circuits as directed by the TOP.

    Note: It is important to establish the bounds for such independent actions to ensure that stability and reliability are not jeopardized.

Key Recommendation #1 | Operations
Consider which entities would take the independent actions and the tools needed to stabilize islands when communications capability is severely disrupted or unavailable.

3.3 Initial Operator Response

Following the immediate, automatic response the next priority is to take operating control actions to stabilize any islands of generation and load that remain.

Recommendations for System Operators

In order to stabilize the island the System Operator should:

- Determine the extent of the island (i.e., its electrical boundaries) and monitor frequency.
- Determine if the energy management system is communicating with the power plant control systems. If so, then setting Automatic Generation Control (AGC) to flat frequency control is desirable to allow a faster response to frequency deviations. This may not be desirable if telemetered tie-lines to adjacent systems are part of the island.
- In the absence of AGC, determine which generating units can have their droop curves adjusted to operate as the 'driver' unit in isochronous mode. It may be appropriate to spread this control over a number of units and set the unit's basepoint to the mid range of its operation.

- Once the size of the island increases consider if and when it is appropriate to restore the droop setting on the 'driver' unit.
- Manage the load-generation balance by dispatching available generation and by using load shedding as necessary. Operators must also recognize the difficulty in solving for Area Control Error (ACE) with limited telemetry.

Recommendations for Reliability Coordinators

In addition to the above System Operator actions, the Reliability Coordinator may be in a position to perform some high level coordination tasks to facilitate a long-term islanded operation, including:

- Generator fuel supply tracking, scheduling and prioritization[24].
- Providing situation assessments (e.g., status of nuclear plants) and future prognoses to stakeholders including government, the media, and the general public.
- Assisting system operators to operate their islands within the context of the situation. The Reliability Coordinator may have a wider area view of the BPS and be able to coordinate operation and restoration activities across the various islands.
- Document and keep current the voice communications technologies and procedures available to communicate with other entities. Other entities could contact their Reliability Coordinator to determine alternate means to communicate.

Recommendations for Power Plant Operators

Rapidly changing frequency outside normal bounds is likely an indication that the plant has formed an island with some load on the system. As noted above, the operation of the island may need to be performed by entities that are not normally responsible for System Operator functions, so that the plant operator may well communicate with a different entity than its normal system operator (e.g., BA, TOP). As a result of island formation, power plant operators should examine their plant outputs and consider doing the following:

MW Output

- For AGC plants, power plant operators should determine if the energy management system is communicating with the power plant control system and leave any units on AGC.
- If no longer receiving signals, place units in manual and try to contact the System Operator and maintain unit output.
- For all other units, follow protocols for loss of communication and await further instruction from the System Operator.

[24] In some jurisdictions, for example those within competitive electricity markets for generation, the Reliability Coordinator has no role in tracking, planning or scheduling generator fuel supplies.

Frequency

- Maintain output and attempt to contact the System Operator.
- Use the NERC Y2K Constant Frequency Operations Guide[25] to inform operational strategy in the event of communication loss.
- Make all available units ready for operation.
- If units trip, stabilize them and prepare to resynchronize following direction from the System Operator.
- Secure station service.

Voltage

- Maintain Automatic Voltage Regulation (AVR) on automatic.
- When AVR is unavailable, minimize changes to MVAR output unless the plant is at risk.
- As directed by the System Operator, adjust power system stabilizer.

3.4 Island Stability

Large interconnected power grids are inherently stable because they have many sources of governor-controlled generation and relatively predictable load patterns. Conversely, small islands are 'high gain' systems where relatively small changes in generation or load can cause large changes in power system parameters such as voltage and frequency which may cause equipment to trip on existing protection settings. Although this action may impede restoration, these settings are critical to ensure that critical assets essential to restoring the BPS are not damaged. Also, many of the mechanisms and criteria that dictate how the BPS is managed may be unavailable or require significant rethinking.

System Operators should consider the following to build and maintain stable islands.

Load

- Use distribution load controlled by SCADA to rapidly restore initial load, as time considerations may prohibit local manual operation.
- Maintaining the load-generation balance will require that System Operators anticipate the changing load pattern over time. This ability to forecast primary demand without historical data will be limited by a lack of detailed knowledge of the load in a portion of the normal balancing area. Although the peak load that can be served in the island is limited by available generation, the System Operator will need to understand the load pattern to manage frequency deviations as load picks up and drops off throughout the day. In addition, load levels in the island will likely be significantly lower than pre-event levels as industrial and commercial loads take time to recover following the Severe

[25] Ref. NERC Constant Frequency Operations Guide, https://www.frcc.com/handbook/Shared Documents/COM - Communications/Constant Frequency Operations Guide 100208.pdf

Event and resume some level of operation. The load will grow over time as operations resume but be limited by available generation.

- Prepare to limit restoring loads that are highly variable (e.g., smelter or arc furnace loads).
- Local field personnel who are familiar with the characteristics of loads at the distribution level will be critical to the development of a workable plan to anticipate and respond to changing conditions as the New Normal evolves.

Generation

- Maintaining the load-generation balance requires that the capability and limitations of the various generation sources in the island are known, and mechanisms are in-place to dispatch them. Market mechanisms, schedules, and automatic generation control are likely to be unavailable or impaired.
- Governor response of the surviving units may be limited or may not be available. Also, in the absence of AGC, generators that can operate in isochronous mode become extremely important to maintain system frequency. Therefore the location and availability of generators that can operate in isochronous mode needs to be known to allow stable island operations. BA's should consider identifying the governor responses of generators within their balancing area and those that can operate in isochronous mode so this can be shared appropriately following a Severe Event.
- Variable generation, such as wind and solar, require special consideration which may require these generation sources be limited if they are in relatively small islands.
- Generation may be limited due to regulatory requirements or license conditions that are appropriate for normal operation but may need to be revised under New Normal conditions.
- Generators that remain off-line for extended periods of time require BPS-supplied power or backup generation to support station service, further limiting the generation resources available to serve other loads.

Operating Reliability

Adequate operating reliability must be re-examined in the context of an island – normal operating reserve and system operating limits may no longer be appropriate.

- It is important to understand the limitations imposed by large voltage angle differences[26] and synch-check relays when reconnecting generation

The Importance of Phase Angle Requirements

During the Italian blackout of 2003, auto-reclosers failed to restore key inter-tie lines due to the large voltage angle across them – about 42 degrees. During the 2003 Northeast Blackout, synch check relays hindered system restoration.

[26] UCTE, "Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy," ed, 2004 and NERC, "Final Report on the August 14, 2003 Blackout in the United States and Canada," ed, 2004.

to the BPS. In order to protect nearby generators from high electromechanical transient stresses that occur during the switching of network elements, through studies, consider increasing the allowed maximum angle to accelerate or enable the restoration process or to allow reclosing.

- Adequate operating reliability must be re-examined in the context of an island. Normal operating reserve and System Operating limits may no longer make sense when all available generation needs to be on-line to serve as much load as possible. Manual and automatic load shedding may become the main source of operating reserve.
- The System Operator should consider how they might optimize operating reserve while operating is islands.

Key Recommendation #2 | Operations
Consider how operating reserve would be managed during islanded operation and frequent periods of insufficient supply to meet demand.

3.5 Load Shedding

In the early stages of islanded operation, System Operators need to quickly determine their energy and capacity situation. During this time, they are likely to manage the load-generation balance using load shedding. Load shedding plans need to consider the priority or importance of loads such as critical power system loads and other dependent critical infrastructures such as telecommunications. System Operators must also ensure that sufficient load remains available for automatic underfrequency load shedding (UFLS) to help protect the island from collapse. It is assumed that UFLS set points will not be adjusted initially following a Severe Event, as these levels are still required to arrest frequency decay. However, they may be examined periodically during the New Normal timeframe. This is discussed more thoroughly in the *Protection and Control* section of this report. As restoration progresses, system operators will be challenged to forecast anticipated load patterns for numerous smaller load pockets contained within each electrical island.

System Operators must also be aware of the different load types in the islands, particularly those prone to large swings in consumption such as electric arc furnaces and large motors. If not already shut down, these consumer loads may need to be severely curtailed until the island becomes sufficiently robust to cope with the load variability. Similarly, System Operators will need to know the maximum load block they can restore in an island as additional generation becomes available.

Recommendations:

- It is important to define, up front, what are considered "critical"[27] and "priority" loads for system restoration and managing load shedding. These terms are defined in the table below. Ensure that critical power system loads and other critical infrastructure loads such as certain telecommunications centers are excluded from load shedding plans.

[27] The term "critical load" is different than the term Critical Asset as defined in the NERC Standard CIP-002.

- Conversely, consider loads that might be non-essential (e.g., street lighting, billboards) which might be without power until full restoration (to the pre-event levels) is achieved.

Table 3: Critical and Priority Loads	
Critical Loads	**Priority Loads**
Critical loads are BPS loads essential to perform restoration and maintain reliability. In some cases, these loads are within distribution systems. During restoration, other loads may be designated as critical loads if they are essential to support restoration (e.g., load required to manage voltage). Examples of critical loads include: • Station service at control centers, transmission substations and generating stations • Power system communications facilities • Protective relays and schemes • Monitoring and control systems	Priority loads are important consumer loads that need to be restored promptly to mitigate the impact on public health and safety, the environment, or the economy. Priority loads connected to the high voltage transmission system or to the distribution system are often excluded from load shedding schedules. Some examples of priority loads include: • Oil refineries and pipelines • Telecommunications centers • Hospitals • Water treatment and sewage plants • Key military facilities.

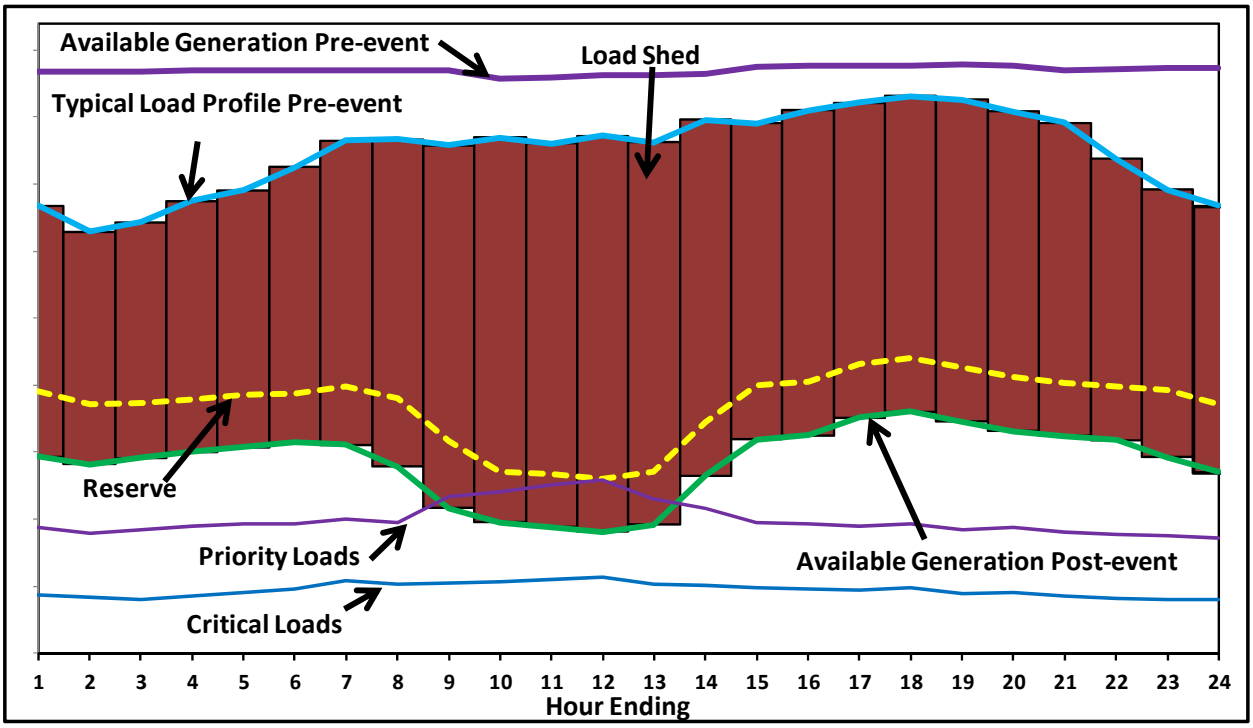
Key Recommendation #3 | Operations
Consider ways to adopt and apply the terms “critical load” and “priority load” across all BPS entities to improve consistent use during a Severe Event.

- In the event of sustained rotational load shedding (rotating blackouts) communication becomes a key factor to ensure that affected areas understand what power supply they will have, at what time and for how long. Due to the potential impacts on public health and safety, these communications need to be carefully considered and coordinated with local distribution companies, local law enforcement agencies, emergency responders and government officials. Although the specifics of this communication cannot be established ahead of time, entities should develop a communication strategy in consultation with key stakeholders.
- Develop mechanisms to predict new load patterns in each island.
- Identify loads characterized by large swings in demand. Detailed knowledge of the types of loads in each island will allow the system operator to appropriately manage them to maintain island operating reliability.

- Develop through system studies and industry experience, rules of thumb to help the operators determine the maximum size of a block of load that can be safely added to an island, based on the available MVA of synchronized generation.
- Since it is impossible to predict the extent of islanding formation following a Severe Event, it may not be practical to share operational information ahead of time. It is important therefore that information-sharing strategies are established in preparation for such events to expedite this information dissemination and address any confidentiality concerns.

The ability to serve load within islands is expected to be limited following Severe Events. The blue line in the figure below shows a typical load profile for an area under normal conditions. The green line represents the load that can be served following a Severe Event, the difference between the red and green lines is the total amount of load that will not be served, and the difference between the green line and the dashed yellow line represents generation or load shed reserved for contingencies.

Figure 4: Inability to Serve All Load During Restoration



3.6 Generation Dispatch and Automatic Generation Control (AGC)

Following the formation of islands, it may not be viable to have a centralized dispatch function based on bids and offers, so system operators will need to have an alternate means to dispatch. Similarly, AGC may not be available due to limitations on the number of islands it can control or loss of frequency or tie-line measurement. Even in the absence of AGC capability, the System Operator must have a reliable frequency measurement in the island. Also, one or more generators must be capable of isochronous operation (i.e., zero droop) to restore frequency following changes in load. System Operators need to have information on the capability and limitations of the various generation types in the island, including those that are energy limited or may have fuel supply or other operational restrictions.

Recommendations:

- Develop alternate dispatch mechanisms, including communication protocols.
- Investigate the viability of installing more frequency measuring devices to increase signal redundancy or using other sensing devices such as phasor measurement units.
  - Alternatively, coordinate with other infrastructures that may be monitoring frequency from distributed devices and develop the means to share this information.
- Investigate using multiple sources for tie-line flow measurement (e.g., Inter-Control Center Communication Protocol from neighboring entities, redundant metering capability).
- Consider the viability of using AGC to simultaneously control multiple islands.

- Consider mechanisms that allow the transfer of pockets of load and associated generation near a tie line to an adjacent BA for operation within the electrical borders of that BA. Generation within the pocket could be dispatched via voice communications at a relatively fixed level while the adjacent BA provides load following capability via the tie lines.
- Determine which generators can change their droop curves – modify governors as necessary.
- Plan that nuclear generation may be off-line, and develop contingency plans in conjunction with the generator owners and operators to help ensure that BPS-supplied power is available.
- Document generator capabilities and limitations in an area so this information can be readily shared should the dispatch function be delegated to an entity that does not normally perform this role.
- Information sharing protocols should be developed ahead of time with organizations that are most likely to need this type of information following a Severe Event. These protocols may need non-disclosure agreements.

Key Recommendation #4 | Operations
Consider alternate means to dispatch generation if normal automated systems, including automatic generation control, are unavailable.

3.7 Variable Generation

Variable generation (Wind & Solar) is becoming a more prevalent form of generation, and has unique characteristics that must be considered during restoration. Some (generally smaller) wind turbines are not truly dispatchable, but have variable output as a function of wind speed. For those wind generators connected to the distribution system, operators need to be aware of their impact but may not have real-time system monitoring of their output.

Normally, automatic controls connect and disconnect banks of wind generation according to the wind speed and any maximum cap set by the wind generator operator. This variability of output is not a concern when the system is in a normal state, but can be problematic during a restoration, particularly when trying to stabilize or synchronize islands.

Recommendations:

- System operators should consider developing policies on how they treat variable generation (i.e., wind, solar) during island operation. These policies could address such matters as:
  - Treatment variable generation when their varying outputs cause unacceptable voltage or frequency deviations.
  - The impact of disconnecting all wind and solar generation at once either through tripping or directed actions. This may cause the island to collapse if the variable generation exceeds a specific percentage of the island's generation capacity.

- Disconnecting wind generation in banks and the need to compensate with other generation or through load shedding to maintain frequency.
- In blacked-out areas, consider disconnecting these resources and leaving them out of service until the latter stages of restoration.
- Consider connecting variable generation to large-scale storage devices radially to optimize variable generation output.

Key Recommendation #5 | Operations
Consider if or how variable generation would be dispatched through restoration and islanded operation.

3.8 Training

Consider enhancing existing training for system operators and field personnel to address the challenges of a Severe Event.

- Manual synchronization of islands
- Islanded operations with local control area operators assuming control of certain islands
- Communication tabletop exercises to verify and train on new coordination and communication protocols between various entities including a loss of, or significantly degraded, communications.
- Implementing rotating blackouts for extended periods of time.
- Identify, accommodate, and implement changes to priority loads.

Key Recommendation #6 | Operations
Consider enhancing regular restoration drills and exercises to train staff on communication protocols and independent control actions in the event of loss of or degraded telecommunications.

Key Recommendation #7 | Operations
Consider using more extreme exercise scenarios that involve simulated rotating blackouts and islanded operations on a larger scale and for extended periods of time.

4.0 Monitoring the Bulk Power System

The 2003 Blackout Report[28] emphasized the importance for system operators to maintain situational awareness of the BPS. In the case of Reliability Coordinators, there is also the need to maintain situational awareness over a wide area that extends beyond their immediate operating zone. Due to the interconnected nature of the BPS, system operators also rely on the system conditions and data of their interconnected neighbors.

August 2003 Northeast Blackout – Recommendation

"#22. Evaluate and adopt better real-time tools for operators and reliability coordinators."

Since the 2003 Blackout the industry has continued to evaluate and adopt better tools that support real-time operation. System operators and Reliability Coordinators have enhanced their tools to provide decision support and situational awareness with greater granularity, accuracy, and a wider area view. In addition, NERC's reliability standards require minimal acceptable levels of this capability for system operators. Entities continue to explore and leverage state of the art technologies such as phasor measurement units and other new methods to monitor, anticipate, and respond to real-time thermal, voltage, and stability challenges.

To achieve and maintain situational awareness the electricity sector has over the past decades developed increasingly sophisticated tools consisting of metering points, communications networks and sophisticated software to monitor the BPS more frequently, accurately, and precisely than ever before. Within each entity, these tools typically monitor thousands of data points every few seconds at transmission sub-stations, lines, and generators.

While these tools are designed to be robust with availability rates of at least 99%, they do occasionally fail. Therefore, every operating entity has backup, call-out, and response plans to rapidly diagnose and address problems. Yet as strong as these regularly exercised plans are, a Severe Event could create such wide spread degradation of these tools or data that many operators throughout the interconnections may at best see only a portion of the BPS required to operate the system reliably.

System operators need to ensure that they have sufficient visibility and control in order to sustain a stable island. Inability to control the various parameters can lead to instability of the island and result in equipment damage. In this section, options are provided to continue to monitor the operation of the BPS, in spite of degraded system monitoring tools such as:

- **Energy Management System (EMS)** – provides system operators with data and analysis to monitor and operate the transmission system. An EMS includes several important functions.
  - The "model" of the EMS provides a mathematical representation of the BPS to enable contingency analysis and other monitoring functions.

[28] US-Canada Joint Power Outage Task Force https://reports.energy.gov/BlackoutFinal-Web.pdf

  - The State Estimator uses the model to calculate data points that are not physically metered and can help validate data or estimate missing data in the event of metering failures.
  - Security Analysis software provides sophisticated "What If" contingency analysis so operators can be prepared to take prompt action if BPS elements such as generating units or transmission lines become unavailable.
  - Automatic Generation Control (AGC) to automatically raise or lower the output of certain generators to dynamically balance total generation output with consumer demand.
- **Generation Management System (GMS)** – provide power plant operators with data and analysis to monitor, control and operate multiple power plants to keep generation resources on schedule. GMS may also include AGC functions.

Assumptions

This section assumes that the tools used to maintain BPS situational awareness are compromised or substantially degraded for an extended period of time. Telecommunications capabilities are also in a significantly degraded state. Entities must monitor and operate a BPS that is unfamiliar and likely in an unstudied state. Entities will need to communicate and share information both internal to its operating footprint and external to neighboring entities.

4.1 Generator Output

Either MW or MVar output data is unavailable from the energy management systems or is of questionable quality. System operators should consider the following:

Recommendations

- Following an event, create communication schedules to have power plant operators report current and projected MW and MVar output for each unit.
- Develop block loading schedules so that Generator Operators understand in advance what actions will be taken depending on system conditions (e.g., frequency readings, time of day, interconnection point voltage schedules).
- System operators could define specific operating ranges for generators that could assist in verifying that operating directives are reasonable and authentic.
- Operating to such schedules might be difficult in the early stages of a Severe Event as the system may be less stable and operating with fewer resources. As a result, ranges may need to be larger to provide greater operating latitude, but as operating experience with the New Normal system is achieved operators might tighten these ranges.

4.2 Operating Limits

System operators must continually ensure they are operating equipment within established limits in order to avoid further damage to equipment and support reliability. Operating limits may need to be recalculated as configuration changes will alter system impedances and system flows will be radically different from normal operation. Operators will need to perform these recalculations periodically throughout the Severe Event. For each recalculation, affected entities will need to consider how close they should operate to the limit based on their understanding of the risk of the next contingency. If the risk is determined to be high, it may be better to operate further away from the limit but serve less load. If the risk is determined to be lower, it may be better to operate closer to the limit and serve more load.

Recommendations

- **Hard Copy Reference Material** – Provide thermal limit ratings for each facility in hardcopy form. Periodically confirm these ratings with automated values when on-line calculations are available.
- **Standard Operating Procedures** – BPS entities change their facility ratings at particular triggers depending on system conditions. Some entities change their ratings seasonally, others have very granular temperature sets of ratings that are different for day and night operations. During a Severe Event, system operators could implement standard operating procedures for switching to different temperature sets at established times. This will help ensure that control actions are coordinated and both parties use the same limit at the same time and under the same conditions. However, these ideas would likely only be explored after the system has returned to a greater level of predictability. It is more likely that following a Severe Event the best recourse would be for operators to use conservative limits.
- **Conservative Limits** – System Operators could default to pre-studied conservative limits to provide additional robustness to the transmission system in order to absorb an anticipated threat. These conservative limits could represent N-2 or maximum credible contingencies and position the BPS in a more resilient mode of operation.
- **Revisit Design/Operating Assumptions** – Following an event, system operators may need to revisit the assumptions underpinning their limits (i.e., operating in a number of small islands will create far different flows on the system than during normal interconnected operation). Design assumptions that need to be reviewed include the type and amount of load, the interconnected/networked nature of the system, generation mix, and system transfers and flows.
    - The New Normal operating environment may require system operators to operate with far more risk of potentially damaging equipment and/or cascading islands. Redefining these operating assumptions may provide greater flexibility to serve more customers provided any short-term gains are balanced against potential long-term consequences.
    - Reassessment of operating limits may also be driven by physical damage or long-term unavailability of assets.

- If these changes in assumptions drive changes to limits, the operating entity should communicate these changes with its Reliability Coordinator and any interconnected neighbor.

Key Recommendation #8 | Monitoring the Bulk Power System
Consider developing processes to quickly study island configurations and develop suitable operating limits.

- **Operate to the Most Conservative Reading** – During normal operations, when either a limit or the monitored flows are in question, operators should always operate to the most conservative readings/limits. Entities should consider when this fundamental requirement might not be achievable in the New Normal. Example decision criteria might include:
  - Reconsider operating to the more conservative reading/limit when the result might create far greater social impact (e.g., inability to serve priority loads that have a clear impact on public safety).
  - What entities need to be consulted to understand possible consequences? Can emergency management organizations better help frame such decisions?
  - Safety of nuclear units may be put at greater risk if an operator were to default to the more conservative limit that would require switching a line providing BPS power out-of-service. Accepting the short-term risk of keeping the line in service, might be the more prudent and safe decision for the overall community.

4.3 Monitor Flows on BPS Facilities

Having system operators continually understand either the actual or modeled flows of tie lines and internal transmission facilities is essential in system operations (these readings are as critical as an altimeter is to a pilot). As such, an adversary could have either altered an EMS Model's representation of the topology of the system (altered which elements are modeled in service or out) or have changed the modeled flows and possible impacts (impacts to State Estimation and Security Analysis results).

Recommendations

Consider operating without any state estimation, relying only on actual power system flows for weeks to months.

- Prior to an event, conduct studies with the EMS to understand the bare amount of data required to keep the current state estimation model and security analysis applications solving.
- Assess whether greater levels of load or generation aggregation could be used to reduce the amounts of required data.
- Consider if a simplified model with reduced granularity could be stored locally or on a separate portion of the Information Technology (IT) network. Consider if this model could be uploaded to the EMS and integrated with the state estimator and identify:

  - Subject matter experts needed
  - Time and effort required
  - Procedures needed to implement if subject matter experts are not available?
  - Testing and training
- Assess what conservative operating restrictions may be needed to mitigate the reduced accuracy of the simplified model (e.g., conservative limits for certain facilities).
- Create a prioritized list of the data points most critical to understanding the operating state of a given operating area (the canaries in the coal mine).
- Consider the need to reconfigure study models to reflect an extended period of islanded operation, and at what stage of the New Normal this would be undertaken.
- Consider the field personnel and communications capabilities needed to sustain 24x7 manual monitoring at critical data points. To enhance this capability, consider:
  - Training required to provide accurate monitoring and maintain safety
  - Developing procedures and reporting formats for each facility
  - Using security personnel for some monitoring duties
  - Communications equipment, facilities and methods
  - Pre-arranged reporting times
- If the Internet is available, consider using social media (e.g., Twitter feed) to facilitate reporting.

Key Recommendation #9| Monitoring the Bulk Power System
Consider developing processes to monitor BPS flows in the absence of reliable automated systems and communications.

- **Use of Phasor Measurement Units** – Throughout the Eastern, Western and ERCOT interconnections, phasor measurement units (PMUs) are being installed to enhance the granularity of BPS data. PMUs provide system operators a paradigm shift in situational awareness. Rather than measuring the system every few seconds, PMUs can measure the system tens-of-times per second. As exciting as these emerging possibilities are for operations, what is intriguing from a resilience perspective is that many of the new applications using PMU data provide new opportunities compared with traditional EMS applications and data communication links.
  - System operators are currently field testing new PMU applications and considering how these may provide a completely independent source of data.
  - PMU applications could be driven by data collected at particular points via data concentrators, and may provide system operators with essential data using far fewer PMU readings.

  - As these PMU applications are developed to become full production operations applications, organizations may consider how to keep the PMU applications independent of EMS applications and support hardware. The end result may be that PMU applications might not only enhance current operational reliability but support reliability and resilience in a New Normal environment.

- **Use of FNET** – Research into island detection based upon the use of frequency disturbance recorders (FDRs) originally installed as part of the frequency monitoring network[29] (FNET) program developed at Virginia Tech is currently under way as part of the GridEye[30] program managed by the University of Tennessee and the Oak Ridge National Laboratory. The proposed project seeks to combine FDR data and offline analysis to provide a practical, low cost implementation of island boundary visualization based upon existing technology and real-time/historical data.

4.4 Loss of Control Centers – Both Primary and Backup

This section addresses concerns and issues that would result when there has been a loss of both the primary and backup control centers for a BA, TO, or Reliability Coordinator. Most likely the risk of losing both control centers is very remote. However, following the 2011 Fukushima disaster, the Chair of the Nuclear Regulatory Commission commented that if such a disaster had occurred in the U.S., the Commission would have directed evacuations within 50 miles of the impacted plant(s). How many operating entities have both of their control centers in the 50 mile radius of a single, if not multiple, nuclear plants? There is no panacea for the numerous problems that would be manifested in this scenario; however, there are a number of things that could be addressed before, during, and after such an event that would lessen its impact. Yet the following recommendations are not intended to encourage the building of tertiary (back-up to backup capability); however these ideas are shared to elicit consideration of the how to avoid or respond to the very remote possibility of losing both control centers.

Recommendations

- When considering a new location for the primary or alternate control centers, consider building the new facility a distance from the other which would avoid common risks including natural and man-made concerns such as 1) earthquake fault zones, 2) hurricane or tornado zones, 3) evacuation radius for nuclear and chemical plants, 4) tsunami risks 5) volcano eruption zones 6) chemical spills from rail or highway accidents and manufacturers, or other risks. It is understood that the greater the distance between control centers the longer it would take to occupy the backup control center; as such there are inherent tradeoffs between the possibility of losing the ability of controlling a portion of the grid while the entity is occupying its backup control center.
- Consider developing arrangements with neighboring Balancing Authority, Transmission Operator, or Reliability Coordinator, [Power Plant or Market Dispatch Office] to share or use their control facilities.

[29] Ref. FNET, http://fnetpublic.utk.edu/
[30] Ref. Grid Eye, http://www.ornl.gov/sci/electricdelivery/pdfs/GridEye Fact Sheet.pdf

  - Share telemetry between entities
  - Use Inter-Control Center Communication Protocol from a third party
- Deploy multiple, diversely routed telemetry communications paths from selected critical remote terminal units to data concentration hubs which are not co-located with the control centers.
  - From each of those data concentration hubs, telemetry could be fed to both the primary and alternate control centers, or a third party with which there is a contract to share their control center/capabilities.
  - An EMS, SCADA, or mini SCADA[31] could either be located at or mobilized to a data concentration hub to allow limited emergency system control with the loss of both control centers.
  - As the industry continues to deploy and leverage Phasor Measuring Units (PMU's) within operations, entities may consider concentrating the PMU data at a tertiary site away from the primary and back-up control centers. Having the PMU concentrator and user interfaces might provide for a bare bones tertiary control center.
- During the time the entity is required to operate at a location other than the primary and backup control center, physical security would have to be maintained at the alternate site. The physical design should enable this to be accomplished quickly and easily. Contracts should be developed in advance for any needed security services.
- Consideration should be given to the logistics required for self-sustained operations, at an alternate site. This would involve sufficient office space for engineering, computer, and dispatch personnel, as well as, the supplies and storage for food and water for an extended period.
- Consider building operator-training simulators at a location independent of both the primary and back up control centers. Though the simulator will not have the complete capabilities of the primary control center or backup control center, if connected to particular data concentration hubs it may permit operators to control portions of the BPS within the parameters of the New Normal.
- Should entities consider having their Storm/Emergency Response centers at tertiary sites with some limited level of system control and information?
- Often control centers of large areas have many subordinate control centers. These subordinate control centers could range from being a local control of a large transmission owner to a small municipal operating entity. Regardless of size and particular monitoring capabilities, these subordinate entities could participate in drills where they must operate in the absence of direction and oversight. As such, if a large entity were to lose both its primary and backup control centers, efficient BPS operations

[31] A mini SCADA has less functionality and capacity than a primary SCADA, with fewer telemetry points and limited advanced applications, if any. It usually is capable of at least monitoring tie line flows with neighbors.

may have been impacted, but effective operations may still be maintained through a far more diverse group of operating entities. In order to achieve effectiveness, parties may need to consider the training and drills needed to create the confidence and capabilities to achieve reliability under this distributed model.

- If there is a warning of a possible attack or major system event, operating entities may want to consider staffing each of the sites where it has some operating capability. In the event that anyone or multiple sites are damaged the remaining facility may be able to take control, if only partially.
- From a cybersecurity perspective, both control centers could be significantly degraded if the primary and backup control centers are simultaneously exploited through the means by which entities keep the facilities synchronized. In an environment of heightened cyber threat, operating entities may consider not keeping these facilities synchronized and using different sets of cyber controls and hardware to ensure that both centers do not have common vulnerabilities to potential cyber threats.

Key Recommendation #10 | Monitoring the Bulk Power System
Consider the simultaneous loss of primary and backup control centers and how essential functions will continue to be performed.

5.0 Communications

The reliable operation of the BPS depends on a highly reliable communications infrastructure. North America's BPS has been described as the world's largest machine; generation resources, consumer load, field operations, and centralized controls are all separated by significant geographic distances and the actions of any single entity can significantly impact others. Although communication, both voice and data, is very important in normal operations, during a crisis situation it is absolutely critical[32].

During a Severe Event communications will be degraded to some extent, and entities may experience the complete loss of normal communications. Despite this, operating entities must strive to continue to monitor the system and direct operations at all times regardless of circumstances. This section discusses alternatives to address the challenges associated with degraded communications.

Assumptions

This section assumes that communications is degraded as a result of a Severe Event for a number of reasons:

- Impact on communications infrastructure from one or more of the following:
  - Loss of BPS power supply to telecommunications facilities
  - Physical damage to telecommunications facilities
  - The user volume of communications exceeds the capacity of communications facilities, especially cellular and satellite telephone networks
- New and unfamiliar communications protocols that are not required during normal operation may need to be arranged with entities or individuals.
- Electricity market functions that depend on automated dispatch will be dramatically reduced or suspended, creating the need for manual operator control and direction.

[32] A cyber attack will pose particular risks to the systems used to operate the BPS. This is addressed by NERC Cyber Attack Task Force report, currently under development.

5.1 Communications Relationships

The need for reliable communications depends on the operating relationships between entities. The following table illustrates key working relationships and the types of communications most critical to BPS operations through a Severe Event:

Table 4: Key Communications Relationships

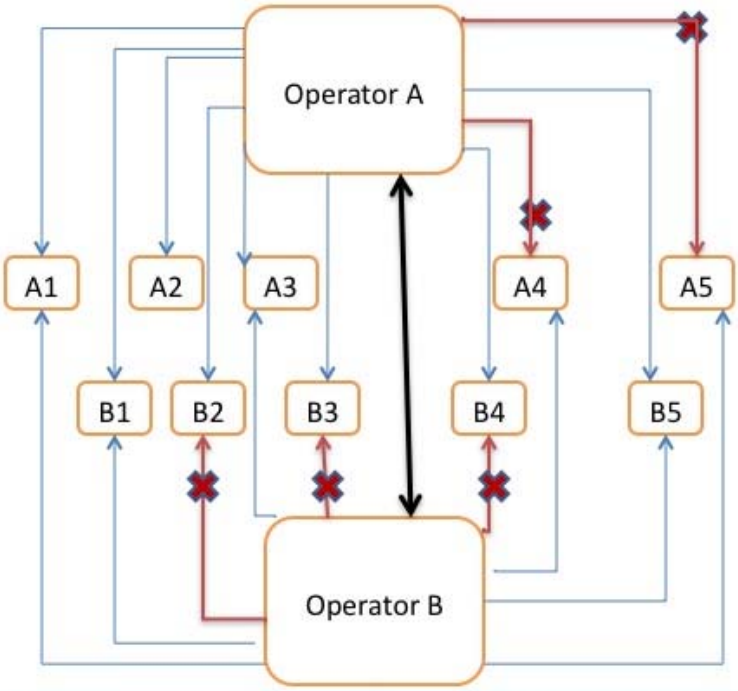
Relationship	Key Communications
1. Between field personnel, through the Distribution Provider and Transmission Operator, and the control center of the Transmission Operator	• Assess situation at remote facilities • Manually read meters and equipment status indicators • Operate equipment (e.g., opening and closing breakers)
2. Between the Balancing Area and the Generator Operator within an island	• Determine generator status and schedule, including fuel and operating limitations • Direct generation schedules (MW and Mvar) • Monitor frequency • Determine which unit could operate as the driver unit in isochronous mode
3. Between the plant Generator Operator and its connected Transmission Operator	• Determine generator status, schedule, and constraints on unit output • Determine transmission line and substation loadings • Implement restoration sequence • System configuration
4. Between the generation/transmission operators and their suppliers of equipment and services	• Determine fuel, equipment, and other resource requirements • Secure reliable delivery of essential fuel, equipment, and other resources
5. Between the control centers of neighboring but not necessarily interconnected Transmission Owners, Transmission Operators, Balancing Authorities, and Reliability Coordinators	• Confirm generation and transmission status and limitations • Methods of controlling generation to match load throughout the zone • Decide plans to synchronize islands • Identify opportunities to provide mutual assistance
6. Between the Transmission Operator control centers and the Reliability Coordinator	• Discuss and coordinate restoration and operation options and strategy • Confirm operating authorities

Table 4: Key Communications Relationships	
Relationship	**Key Communications**
7. Communications with Government entities (e.g., local and state emergency operations centers)	• Assess situation • Determine prognosis for restoration of service • Identify needs and priorities • Coordinate with other critical infrastructures • Coordinate public communications (e.g., schedules for rotating blackouts) • Identify safety and security needs and solutions • Keep informed about status and manage expectations for service
8. Between the consumer loads and the Distribution Service Provider	• Provide information regarding the nature of loads within the area such as priority loads, large or variable loads, issues related to cold load pickup • Coordinate and communicate service restoration information and rotating blackout schedules • Communicate restoration information and manage customer's expectations for service quality

5.2 General Communications Recommendations

- The *Interdependencies with Other Critical Infrastructures* section of this report suggests ways to work with telecommunications service-providers to better understand interdependencies and mitigate the risks associated with BPS and telecommunications infrastructure disruptions.
- Consider co-locating BA and TO functions within the same work center in order to reduce communication requirements and assist with the synchronization complexity of restoration.
- When examining backup communications options, minimize the number of repeater hops to reduce the number of possible failure points. Configure satellite telephones so they operate point-to-point without the need for intermediate ground stations. Entities should be flexible and prepared to create a network that may include hops to other entities in their wider area through whom they can communicate as illustrated in the figure below.

Figure 5: Alternate Communications Paths



Operator A has communications with key facilities A1, A2, and A3 but does not have communications with A4 and A5. And Operator B cannot communicate with B2-B4. When Operator A confirmed it had communications with Operator B, it found Operator B could communicate with facilities A4 and A5. As such Operators A and B developed a communications relaying relationship. While Operator A is working to restore communications to all of its facilities , it is trying to assist Operator B with getting communications with facilities B2, B3, and B4.

- Entities should consider installing mobile radios compatible with those used by neighboring entities, and developing protocols to share assigned channels.
- When preparing for the Y2K transition period, many entities implemented satellite telephones and continue to rely on them in the event primary communications facilities are unavailable. Entities should consider assessing the extent to which satellite telephones can presently be used to coordinate operations between entities within each Interconnection.
- Identify personnel in advance who have communications skills, such as HAM radio or social networking media such as Facebook or Twitter. If the Internet continues to be available these methods could be very effective in communicating rapidly to the public at large.
- Consider backup generation, wind generation, and solar cells at communications sites to prolong the power supply to these resources. Note that sources of variable generation will require significant energy storage capability.

Key Recommendation #11 | Communications
Consider installing renewable generation (e.g., wind, solar) or expanding fuel storage capabilities at critical BPS facilities to supplement standby generators.

- Prepare plans for long-term fuel delivery to backup generation at entity-owned communications sites.
- If time permits before a degradation of communications, increase the utilization of system "All-Call" and the NERC Reliability Coordinator Information System (RCIS) to notify operating entities of increased operating activity and the need to coordinate major system activities.
- If primary communication links to remote terminal units are down but other communication lines are functioning, consider how an Operating Entity could leverage sub-station security communications capabilities (i.e., radios, fiber communications) to relay critical power system flows, without significantly jeopardizing these systems.
- Local emergency management services (e.g., police, fire, military) vehicle radios may provide both physical security and communications capabilities at critical sub-stations.
- Local HAM Radio chapters often have agreements with local emergency operations centers to provide communications in times of emergencies. Consider reaching out to these chapters[33] to integrate into business continuity planning and possibly drills and exercises.
- The military once had wire telephone communications gear. If available in local armories, consider how operating entities and the military could use such wired communications between critical operating nodes within a particular island (this option would require physically laying the wire and staffing switch boards).

Key Recommendation #12| Communications
Consider alternate means to communicate when primary means of communication are completely unavailable for extended periods of time.

[33] Radio Amateur Civil Emergency Service http://www.qsl.net/races/ and Amateur Radio Emergency Service http://www.arrl.org/ares

5.3 Communication Protocol Recommendations:

Reporting Formats

- Know which are the critical data points are needed to assess the current operating state (review and refresh the protocols developed for Y2K to report critical operating data).
- If all sites are reporting during a single time period (or even staggered), prioritize which stations report first (e.g., by criticality of the information, alphabetical order, or other method). Structured and sequential communications will help manage communications volumes and delayed or missed calls.
- Develop a standardized reporting format so more information can be passed more effectively (i.e., Location, reading 1, reading 2, issues, possible opportunities, actions).
- If spreadsheets are used to record the data, consider if dedicated laptops are needed to consolidate the data, or if hardcopy forms available at data collection points would be sufficient.

- **Consistent Conference Call Protocols** – The individuals providing information will change throughout the New Normal period. Communications must be clear and concise and the leader of the conference calls must drive participants to stay focused on the essential elements of information; the information needed to identify issues and decide the necessary actions.
- **Communications Protocols for Field Personnel** – Develop, train, and exercise field personnel on the communications protocols they will use.
  - Prepare a specific reporting format and common protocols.
  - If needed, assign each critical data point a reporting time, so that the various parties are coordinated.
  - Prepare for an extended period of degraded communications with field personnel (i.e., posting these procedures at the stations with critical data points).
- **Protocols for Releasing Information to the Public** – Throughout the New Normal period, people will need to understand how restoration is proceeding so they can make their own decisions to care for themselves, their family, and their community. If there is limited information available from media outlets, entities could consider posting important information (e.g., rotating blackout schedules) at government offices such as police stations or post offices and at locations where people will congregate (e.g., food and water delivery points).
- **Standing Orders for Personnel** – Standing orders are a prescribed set of instructions for people to take action in the absence of communications or leadership direction. Standing orders could be developed to direct key personnel to report to designated locations following a Severe Event or direct a sub-station technician to clear each bus and open each breaker following a large scale blackout.
- **Validating Sources of Information** – The New Normal may create different operating relationships with operators communicating with and being directed by people they do not know. Consider establishing validation protocols to confirm identities. Develop "challenge and password" protocols or other information known only to certain

persons. Consider how these passwords would be developed, shared, protected, and periodically changed.

Key Recommendation #13 | Communications
Consider robust training, drills, and exercises to fully test critical restoration steps using alternative voice and data communications (e.g., satellite telephones).

5.4 Emerging Technology Recommendations

NOTE: The following suggestions assume the Internet is available. The diverse and distributed nature of the Internet's network infrastructure makes it highly resilient. Local Internet Service Providers and the "last mile" of connectivity to the end user may be the weakest links if they are directly affected by the Severe Event.

- **Masked websites** – Entities could each develop masked (i.e., not listed under the entity's normal domain) websites to display critical readings.
  - Coordinate the development of these websites with other entities so they are designed, secured, and tested (these may require another web presence beyond your entity's currently "secure portal").
  - These websites could support data scraping so that other entities could scrape from multiple sites and upload to spreadsheets to assist in model updates or offline analysis of system conditions. To facilitate this, decide which common data format (e.g., XML, or RSS feeds) will be used. The data scraping could potentially dump the values into PSSE models or other off line studies or analysis.
- **Alternate use of security cameras** – If there is insufficient staff to read key metering points consider using security cameras be to monitor a meter (more acceptable when the threat is not a physical attack threat).
  - Consider using the physical security monitoring center to relay the meter readings to operations personnel.
  - If multiple entities require these readings consider uploading the camera feed to a webpage. This would significantly reduce the verbal reporting burden and multiple entities could access the data as their models or processes required.
- **Mobile devices** – Smart phones and tablet computers could be used as cameras, video cameras, or for conference calls.
- **Ad hoc networks** – Consider what was done during the Arab Spring uprising in Egypt to continue communications even when the Internet was significantly limited, using for example, Mobile Ad Hoc Networks (MANET).
- **Social media** – Consider using social media such as Twitter feeds for reporting. Consider developing Twitter accounts that could be used to share critical data from sub-station to control center, and control center to neighbors. This could be an extension of an entity's existing social network, but directed to system and field operations rather than consumers.

6.0 Short-term and Long-term System Planning

This section offers guidance for both short-term (also known as operational) and long-term system planning functions through a Severe Event. While long-term system planning functions may seem less immediately impacted by a Severe Event than other functions, both short-term and long-term system planners should be equally prepared to ensure their functional resilience.

This section considers the impact on system planners of a Severe Event that damages or degrades planning resources and capabilities.

Experience from Hurricane Katrina

Following Hurricane Katrina, Entergy transmission planners were unable to enter their headquarters in downtown New Orleans for several weeks. This substantially affected their ability to provide timely support, and limited confidence and speed of restoration and reconstruction efforts.

Affected System Planners

System planners are typically divided into short-term (or operational, less than 12 months time horizon) or long-term (greater than 12 months). While there are significant differences in these functions, there is sufficient similarity in how they are affected by a Severe Event that both are considered in this section. Where appropriate, differences are noted.

System Planning Tools and Facilities

System planning engineers typically work as integrated groups in an office environment with a central computer network, telephone network, and access to real time information from operating centers.

Information and data needed for system planning is typically in several forms: traditional paper files, drawings, and maps are located in or near the planning center, records of in-progress current project work in both paper and digital form are at the planner's desk, and shared data such as system load flow base cases are likely to be located in computer servers which may be local or remotely accessible through the IT network. Maintaining backup copies of data is typically a challenge; paper records, even if duplicated, are unlikely to be maintained in a backup location. System planners may periodically create backups of in-progress work but the copies are typically maintained locally. Only the data located on servers is likely to be adequately and securely maintained with off-site backup.

System planning tools and software are typically concentrated at one or two locations. Some software such as load flow, fault analysis, stability, relay settings, and economic analysis will be installed on individual user laptop and desktop computers and many programs require software tokens or are locked to the user's computer. More complex software and associated databases may be installed on local or networked servers. Some short-term system planning software, such as an interface to a state estimator or other real-time system information, is more likely to be installed on dedicated computers in physically and electronically secure locations.

Other system planning tools such as calculators, drafting equipment, plotters, printers, & scanners, are typically located in a central planning office for general use.

6.1 Consequences of a Severe Event on System Planning Functions

The consequences of a Severe Event may include the following, discussed in further detail below and elsewhere in this report.

- Temporary loss of access to system planning offices and tools
- Temporary loss of access to protected or backed up software
- Loss of communications
- Unusual demands on system planners for studies
- A need for studies of systems with multiple BPS elements out of service
- Loss of personnel, unable or unwilling to rejoin the system planning function

Loss of Access to Facilities, Software, and Data

Loss of access to system planning offices, tools, and communications are typically addressed in business continuity plans. In the event that tools and facilities become available, but data is inaccessible, essential information will need to be developed from other sources. Operations will have backup centers where versions of system planning cases may be found. Joint and interregional studies may also be a source for replacement information.

The particular concern with loss of access is that even though it is likely that facilities and tools can often be replaced, if attention is not paid to implementing and sustaining spare equipment and data backups, a significant delay can occur before system planners are able to function again.

Key Recommendation #14 | Short-term and Long-term System Planning
Consider the potential loss of system planning resources (e.g., equipment, data) as well as damage to the system. Review business continuity plans to ensure that system planning resources are adequately considered.

Unusual Demands on System Planners for Studies

Demands on system planners will be immediate, intense, and continuous as system conditions change and configurations evolve. For example, the April 27, 2011 tornadoes affecting TVA required analysis to operate multiple unplanned islands, and study previously unconsidered configurations. Similarly, the loss of the HV transmission cables supplying the Auckland, New Zealand central business district in 2006 required planners to incorporate the temporary overhead lines.

Experience from the 2011 Japanese Earthquake

The 2011 Japanese earthquake and tsunami and the destruction of all transmission facilities supplying the Fukushima nuclear plant required rapid multiple expedient responses that placed extreme demands on planners.

The tasks of system planners will evolve through the mitigation, restoration, and New Normal phases of a Severe Event.

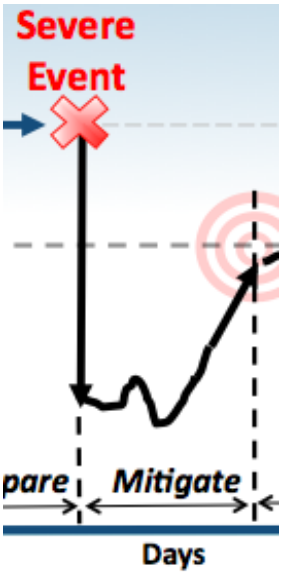
- **Mitigation Phase** – Establish and recover essential system planning facilities. Restore as much of the BPS as possible to reliable operation with a focus on supplying critical and priority loads. Perform essential studies to support BPS operation in unstudied states. Perform studies needed to support island synchronization, system reconfiguration, and potentially conflicting requirements for emergency supply to priority loads. Tasks may require only a limited number of system planners, but with specialized skills and local knowledge.
- **Restoration Phase** – Continue to recover and construct facilities adequate to support longer-term system planning. Develop the studies needed to consider options to return generation and transmission facilities to service. Begin to develop longer-term plans for new facilities. During this phase, the need for system planners may increase from a small core of specialists to a full complement of planning staff.
- **Return to Normal Phase** – Restore complete system planning capabilities. Reconcile short and long-term system planning requirements to improve BPS reliability. Resume long-term system planning functions.

Key Recommendation #15| Short-term and Long-term System Planning
Consider the appropriate use of key system planners who may be required immediately, and for prolonged periods, to perform studies not previously considered.

6.2 Planning During the Mitigation Phase

Support Real-Time Operations

The first priority for system planners will be to establish communication with essential staff and recover essential planning facilities, information systems, and data needed to begin work. Once this is done, the immediate priority will be to support system operators in their efforts to restore the BPS and supply electricity to customers to the extent possible on a prioritized basis. The initial surviving system will likely be in an "unstudied" state. Therefore, real time assessments will need to be performed and step-by-step restoration procedures confirmed by studies before control actions are taken.



The volume of work and the need for rapid response is likely to require that some long-term system planners be re-assigned to the short-term system planning effort during the mitigation phase and perhaps even into the early portions of the restoration phase.

If there is widespread damage to the system, system planning studies may need to consider using temporary configurations such as partially restored substations. Studies may include operation with less than normal margins, contingencies that may cause loss of load, reconsideration of breaker fault ratings, and reconsideration of transformer overloads. Normal design criteria such as voltage may not apply in the early stages following the Severe Event. System planners and management should re-evaluate planning requirements considering the consequences of the Severe Event.

Temporary Facility Ratings

System planners may need to consider temporary above-normal ratings in order to restore the BPS quickly. An ability to quickly calculate and integrate such ratings should be available.

Replacement Equipment

While entities have the ability to withstand normal emergencies and quickly restore their systems from existing or quickly obtained spares, a Severe Event may render purchased spares unavailable for a prolonged period. In this case continuing operation with temporary design solutions using sub-optimal equipment may be required. Maintaining records and databases of equipment characteristics as reconstruction proceeds, particularly when equipment is substituted on a contingency basis, may be a challenge. While most entities have comprehensive transformer spares programs, use of spares in expedient restoration situations may result in unbalanced configurations. Studies may be required of protection and operating limits.

Planning Following the April 27, 2011 Tornadoes

Following the multiple tornados affecting the Tennessee Valley Authority, the Browns Ferry nuclear plant had lost all but one of its seven 500kV transmission connections. As the transmission lines were successively restored to service, multiple unstudied configurations had to be reviewed in coordination with plant restoration.

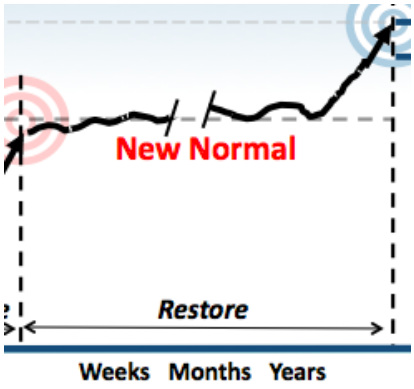
Advance System Planning

Items of advance system planning should be considered as an aid to help speed the mitigation phase. Examples include:

- Perform system studies and maintain records of equipment interchangeability.
- Perform studies to identify the islands that would likely form during a Severe Event, and their sources of generation, including sources of generation (e.g., cogeneration at an industrial plant) not normally supplying the BPS.]

Key Recommendation #16| Short-term and Long-term System Planning
Consider performing selected studies in advance (e.g., equipment interchangeability) that could help speed restoration.

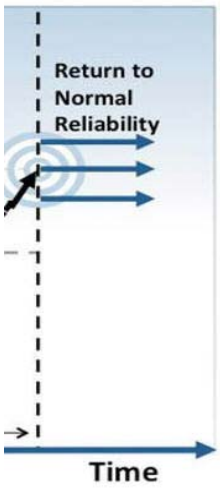
System Planning during the Restoration Phase



As immediate real-time operating demands are met, system planning will transition from the immediate mitigation phase to longer-term restoration of the BPS. Temporary staff reassignments are likely to continue. The system planning function will grow from an initial core of specific expertise and begin to approach pre-event capabilities. In study targets, it is possible that restoration and construction will be significantly different from the original BPS configuration. Factors may include:

- Long-term loss of load, e.g., industrial or residential loads that may be lost for extended periods.
- Budget limitations as operations, maintenance and capital funds are reallocated to manage more immediate priorities. This is discussed further in the section *Emergency Financing* section of this report.

6.3 System Planning during the Return to Normal Phase



By this time the restoration of system planning capabilities will be complete, although it may differ from the original. System planning efforts may be required to reconcile short and longer-term plans with the requirements of the post-New Normal system and its remaining loads. System planning will likely have achieved restoration of regular planning schedules. Entities will be reflecting on their experiences and considering significant changes in long-term plans. Factors may include:

- Permanent loss of load, in particular, industrial load
- Permanent budget changes, either lower or higher, and possibly new funding and approval mechanisms
- Loss of experienced planning staff, expertise, and resources

6.4 Design Considerations

While system planners are typically not responsible for the physical planning and design of lines and substations, they are well positioned to offer recommendations toward improving reliability, including the following.

Critical Spare Equipment

Emergency spares may not be identical to the equipment they replace and may result in unbalanced configurations that require protection and operating limits studies.

Entities have spare equipment criteria for critical equipment such as transformers, transmission line and substation, and generating unit components. However, a Severe Event may render purchased spares insufficient or unavailable for a prolonged period. In this case, operation with temporary designs may be required. To further enhance resilience, line and substation planning could include:

- **Increase Equipment Standardization** – To promote greater interchangeability of components, increase the standardization of component specifications such as physical size and electrical rating. For example, TVA has minimized the number of single-phase 500 kV transformer designs that it currently purchases, and has extensive studies on file of the interchangeability of differing designs. Others have established standard sizes and ratings for transformers, breakers, conductors, and other equipment.

Standardized 500 kV Transformers used by Tennessee Valley Authority

Following two 500 kV transformer failures in 2001, TVA developed an approach that reduced costs and procurement time, and increased interchangeability of spares by limiting transformer purchases to seven standard designs, and using external rather than internal reactors.

- **Location of Spare Equipment** – The location of spare equipment may be important. The spare equipment should be readily assessable, but a physical distance from the equipment being replaced to minimize the possibility of damage as a result of collateral or intentional actions. In higher voltage substations using banks of 3 single phase transformers, a 4th spare transformer is typical and physical separation of the spare should be part of the station design.
- **In-Situ Spares** – It is common practice to situate spares (such as high voltage transformers) adjacent to in-service equipment within same station to minimize restoration times due to equipment failure. Again, physical separation of these transformers should be maximized and otherwise protected from the potential of collateral damage caused by the destruction of the other. Other means to separate in-service spares could include using blast walls, complete redundancy in switching devices (breakers) and relay protection.
- **Use of Adjacent Substations** – Maintaining a safer distance between in-service spares could also be accomplished, depending on application and location, through storage at adjacent substations.
- **NERC Spare Equipment Database**[34] – Consider contributing spare high-voltage transformer data as part of the NERC Spare Equipment Database program being implemented in 2012.

Key Recommendation #17| Short-term and Long-term System Planning
Consider the spare equipment critical to BPS restoration and ways to improve availability of these spares.

Use of Rights-of-Way

Utilities that operate in areas prone to tornados recognize the possibility of simultaneous loss of all transmission lines on a single right-of-way. Other Severe Events such as earthquakes,

[34] Ref. NERC Spare Equipment Database Task Force report http://www.nerc.com/filez/sedtf.html

unusually extreme ice storms, and physical or cyber attacks may also threaten multiple facilities using a common right-of-way.

- While it is common practice to concentrate multiple circuits onto a single right-of-way, consider minimizing the impact of a single mode failure on the facilities. For example, single circuit towers may be less vulnerable to disruption and facilitate energization when crews are working on adjacent structures.
- Some circuits could be built underground to reduce the vulnerability of all circuits along the right-of-way.

Station Design

The implementation of the NERC Critical Infrastructure Protection (CIP) standards[35] have helped enhance physical and cybersecurity at substations. However, many substations are often not staffed and monitoring is limited to visual security cameras and alarms and control devices used for electrical operation. Suggestions to improve resilience include:

- Install electronic surveillance to facilitate remote visual inspection and assist in setting priorities for operation, repair, and identifying alternatives for restoration.
- Harden structures and control houses to minimize damage and improve restoration efforts.
- To reduce exposure to explosions, use physical separation or blast containment techniques.
- Standardize the use of protection and control devices and schemes to ease repair or replacement. Consider using alternate technologies for backup systems that are simple yet effective.

Use of Modular Control Houses by American Electric Power

AEP is working with suppliers to develop modular control houses with Faraday cage shielding of devices and protection cables that would harden critical cyber assets serving large metropolitan areas.

[35] NERC CIP-002 – CIP-009: http://www.nerc.com/page.php?cid=2|20

7.0 Protection and Control

This section identifies challenges associated with protection and control systems used to support the reliable operation of the BPS following a Severe Event and a prolonged period of New Normal operation. It is important to understand the differences between a power system protection engineer's two competing objectives.

Dependability and Security		
Power system protection engineers must optimize the balance between the two conflicting goals of dependability and security. In general, enhancing dependability implies an intrinsic loss of security and vice versa.		
Dependability is "the degree of certainty that a relay or relay system will operate correctly"[36].		**Security** is "the degree of certainty that a relay or relay system will not operate incorrectly"[37].

Protection and control plays a major role in BPS reliability. An analysis of historical NERC outage reports indicates that hidden failures[38] are involved in over 70% of cascading outages. The probability of a hidden failure occurring is likely greater under the stressed system conditions following a Severe Event. Therefore, the severity of the event and the prolonged duration of the New Normal justify a thorough assessment of protection and control systems to help ensure reliable operation.

Protection schemes depend entirely on the local configuration of the BPS and vary significantly from utility-to-utility and region-to-region. While this section does not provide step-by-step

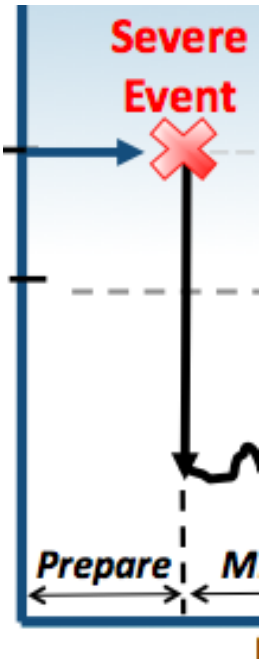
[36] Ref. IEEE Standard for Relays and Relay Systems Associated With Electric Power Apparatus," *IEEE Std C37.90-2005 (Revision of IEEE Std C37.90-1989),* pp. 0_1-19, 2006. [1]
[37] Ibid.
[38] A hidden failure is defined as a permanent defect on a relay system that will cause the incorrect removal of a circuit element as a direct consequence of another event [2] Tamroglak, "Analysis of Power System Disturbances due to Relay Hidden Failures," ECE, Virginia Tech, Blacksburg, VA, 1994. As conveyed by the definition, hidden failures remain dormant until a particular event causes its manifestation and associated relay miss-operation.

instructions or guidance on specific protection schemes, it does emphasize key considerations and potential mitigation actions to enhance reliable protection and control systems.

7.1 Preparation Phase

The NERC cybersecurity standards[39] require that critical cyber assets such as certain protection and control devices and systems be protected. The following offers industry practices best employed prior to a Severe Event.

Physical and Cybersecurity



- Instead of using manufacturer default passwords, consider using strong[40] passwords, change them periodically, and use different passwords for each control house and/or each protection relay.
- Consider performing periodic comparisons between "as-left" relay setting files in the field with setting files at the main office.
- Consider monitoring access into substation, control house, and protection relays.
- Consider enhancing physical security of equipment in the switchyard.
- Emphasize "need-to-know" and restrict access to critical assets and information.
- Consider encrypting communications of all critical data.
- Consider having redundant secure communication paths to critical assets to decrease the impact of denial of service attacks and to provide an alternative path for alarm and mitigation action.
- Consider developing procedures to disable bi-directional data flow in substations to prevent network access to protection relays. The intent is to prevent intruders from being able to remotely log into relays and alter relay settings, yet still allow the relays to perform their normal protective function. The procedure should not compromise SCADA data; disable communications from the communication processor to relays, and therefore only allow uni-directional data flow from the relays to the communications processor.

Power Supply to Protection and Auxiliary Systems

- Determine battery backup power requirements for substation loads such as the control house and station service under a Severe Event scenario.
- Consider installing permanent or portable backup generation to charge batteries at critical substations.

[39] NERC Cybersecurity standards CIP-002 – CIP-009 http://www.nerc.com/page.php?cid=2|20
[40] US-CERT Cyber Security Tip ST04-002 http://www.us-cert.gov/cas/tips/ST04-002.html

- Understand the interdependencies between stored energy in circuit breakers and substation off-site power. For example, spring-spring circuit breakers have stored energy for an open-close-open (O-C-O) operation. The motor to charge the spring mechanism may be AC or DC driven, or both. If the motor is AC driven and the station service transformer is out of service, then only an O-C-O operation is allowed.

Communications Infrastructure

- It may not be possible to operate equipment remotely. Consider the logistics required to dispatch staff to multiple critical substations to monitor and manually operate equipment.
- Understand the interdependencies between protection systems and the communication infrastructure. As an example, consider a Direction Comparison Blocking (DCB) scheme. If the communication between substations is compromised, the scheme will lack security (i.e., the relay may misoperate for a fault outside the protected zone). However, the dependability of the scheme will not be affected.

Control House

- Consider a mobile control house for rapid restoration of critical substations [3]. The design of a mobile control house should address transportation, flexibility to adapt to multiple protection schemes, battery and generator backup power, test and control switches, communication equipment, etc.

Organizational Resilience:

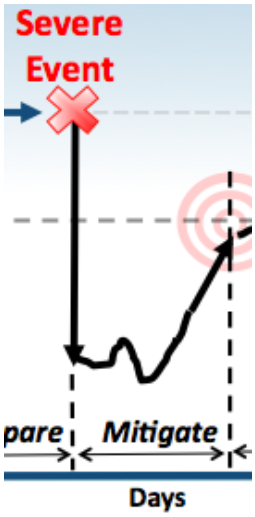
- Consider developing contacts and communication protocols to request the assistance of relay technicians and engineers from neighboring utilities that may not be as affected.
- Consider developing procedures to designate responsibilities to optimize protection and control under the New Normal. Consider tasks such as:
  - Creating a new system model for protection studies
  - Identifying personnel to assess the adequacy of protection settings considering local circumstances under the New Normal
  - Identifying personnel to update relay settings
  - Developing a priority list for protection relays
- Ensure that appropriate communication channels exist between protection systems engineers and power system operators.

Particular Considerations

- Assess the potential impact of a geomagnetic disturbance[41] on protection schemes. Harmonic distortion[42] may cause misoperations [4]. For example, certain shunt capacitor unbalance protection schemes may misoperate as a result of system harmonics. A potential mitigation is to use a voltage differential scheme to protect shunt capacitor banks. Consider the impact on the security-dependability balance on schemes that use harmonic restraint (e.g., transformer differential). Consider the potential impact of harmonic distortion on power system equipment such as harmonic filters, capacitor banks, SVC, communication equipment, generators.
- Assess the potential impact of a coordinated cyber attack on protection systems. A potential mitigation is to isolate systems, including any remote access to these systems, during periods of heightened concern.
- Assess the vulnerability of communications infrastructure to ensure data availability, integrity, and confidentiality: point-to-point fiber, power line carrier, synchronous optical networking (SONET) ring, third party provider network, etc.

7.2 Mitigation Phase

Immediately following the Severe Event, protection systems will respond according to predefined settings; adjusting protection relay settings as the event is evolving is not feasible. Response may be limited to confirming the status of protection systems.



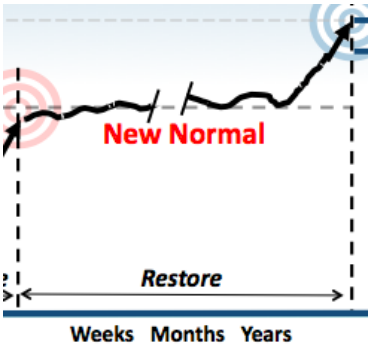
- If a cyber attack is suspected, compare "as-left" setting files in the field with setting files at the main office.
- Taking into consideration potential new islanded configurations, prioritize assessments at critical substations and generation facilities (ref. *Operations, Island Stability* section).

[41] Ref. *Interim Report: Effects of Geomagnetic Disturbances on the Bulk Power System* http://www.nerc.com/files/2012GMD.pdf. This report concluded that the loss of reactive power is the most likely outcome from a severe solar storm centered over North America.

[42] Consider the operating quantity measured by protection relays: fundamental component (digital vs. analog filter), RMS values, etc.

7.3 Restoration Phase

A highly stressed system should be expected during the New Normal period, characterized by islanded operation, rotating blackouts, lower system inertia and higher network impedance (i.e., reduced synchronizing torque), different short circuit currents and critical clearing times, and reduced stability margins. Through the New Normal, protection relay settings may not be optimal and unwanted operations may occur.



System Restoration and Control

- Consider station service at substations along restoration paths to be critical loads.
- Assess physical damage on protection and control communication channels: wave traps, fiber channels, microwave, etc. Non-pilot distance protection of transmission lines may become primary protection until infrastructure for pilot schemes (that require a communications channel) is provided.
- Remote power system control may be compromised. Dispatch personnel to critical substations for manual operation of equipment.
- Assess physical damage to substation control houses. Ensure adequate protection relay equipment is readily available.
- No damage to protection relay devices is expected after a GMD event. Current transformers may have remanence flux, which can shorten the time-to-saturation; this should not be a problem for high speed protection [4].
- If traditional telemetry or access to SCADA/EMS is compromised, consider using monitoring and control capabilities embedded in microprocessor-based protection relays.

Reliability of Protection Schemes

- Consider revisiting protection settings to enhance the security-dependability performance of the protective equipment. Protection relay settings are developed based on an assumed system state. Such settings may become unreliable under the New Normal; critical clearing times may be reduced, short circuit currents may change, and stability margins may be reduced. It may be possible to optimize the reach of protective zones.
- Consider a reliability bias towards security [7]. Traditionally, protection systems have been biased towards dependability. Under normal conditions, system topology and good stability margins justify such a design. For example, multiple transmission lines provide a number of alternate paths for power to flow and the BPS can withstand losing a single line as a result of conservative protection security provided the remaining transmission lines have sufficient loading margins. Under such conditions, not clearing a fault with primary protection has a greater impact on the system than a relay mis-operation due to lack of security. However, under New Normal conditions, the power system may be in a highly "stressed" state. Unnecessary line trips may further

exacerbate system conditions, contribute to the geographical propagation of the disturbance, and may even lead to cascading events and subsequent blackout.

- Consider studying cascading outages. The BPS may not be secure enough to withstand the next contingency (N-1); consider reviewing existing and developing new SPS and RAS schemes.
- If rotating blackouts are implemented, consider studying the impact of cold load pick-up on distribution protection with Distribution Service Providers.
- Assess source strength for distribution circuits. If short circuit currents do not allow protection coordination, consider implementing voltage supervision.
- With stability margins significantly reduced, under frequency load shedding (UFLS), under voltage load shedding (UVLS), and special protection schemes (SPS) may be essential to ensure a reliable operation of the power system. Review and ensure the appropriateness of existing UFLS, UVLS, and SPS schemes [8-14]. Consider deploying additional schemes to better suit the prevailing system state. The main three parameters involved in designing UFLS and UVLS schemes are:
  - When to shed load (threshold setting)
  - How much load to shed
  - Where to shed load

Importance of Relay Setting Parameters

All three parameters are important. During the July 1996 WSCC blackout, [12] load was shed at the power sending side which caused several tie-lines to become overloaded which in turn led to a loss of synchronism. In the 1977 New York blackout [15] generator excitation protection tripped several machines after a voltage rise caused by load shedding.

Key Recommendation #18 | Protection and Control
Consider ways to implement large-scale changes in system protection schemes to support islanded operation and changing BPS configurations, and what decision points would be needed.

Key Recommendation #19 | Protection and Control
Consider ways to quickly reconfigure relay settings in the event large-scale changes are needed.

Distribution System Impacts and Mitigations

Large magnitude geomagnetically induced currents are not expected to flow in the distribution system. However, the impact of harmonic distortion on any distribution-level protection systems should be considered.

7.4 Training

Due to the challenges posed by operating the power system under the New Normal, personnel training is a critical factor to ensure a resilience power system. Training opportunities may include:

- Consider cross training between distribution and transmission relay technicians and engineers to allow flexible reallocation of personnel.
- Consider developing an instruction manual describing the system protection philosophy. The intent is to facilitate the learning process in case system protection personnel are shared among utilities. The manual should address protection scheme designs, protection relays used, communication equipment needed, etc.
- Before attempting to synchronize islands, ensure that mechanisms are in place to identify and coordinate any changes to protection systems (i.e., SPS, UFLS, UVLS schemes) that could affect neighboring entities.

References

[1] "IEEE Standard for Relays and Relay Systems Associated With Electric Power Apparatus," *IEEE Std C37.90-2005 (Revision of IEEE Std C37.90-1989),* pp. 0_1-19, 2006.

[2] Tamroglak, "Analysis of Power System Disturbances due to Relay Hidden Failures," ECE, Virginia Tech, Blacksburg, VA, 1994.

[3] R. Mazzatto, M. Leschuk, R. Glass, R. Brown, and D. Schmidt, "Case Study: Mobile Protection Unit for Rapid Power Restoration," *65th Annual Georgia Tech Protective Relaying Conference,* May 2011.

[4] "Geomagnetic disturbance effects on power systems," *Power Delivery, IEEE Transactions on,* vol. 8, pp. 1206-1216, 1993.

[5] UCTE, "Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy," ed, 2004.

[6] NERC, "Final Report on the August 14, 2003 Blackout in the United States and Canada," ed, 2004.

[7] E. Bernabeu, "Methodology for a Security-Dependability Adaptive Protection Scheme based on Data Mining," Ph.D., ECE, Virginia Tech, Blacksburg, VA, 2009.

[8] NERC, "Assessment of the Design and Effectiveness of UVLS Program," 2005.

[9] NERC, "UVLS System Maintenance and Testing," 2005.

[10] NERC, "Assuring Consistency with Regional UFLS Program Requirements," 2005.

[11] NERC, "Underfrequency Load Shedding Equipment Maintenance Programs," 2005.

[12] NERC, "Review of Selected 1996 Electric System Disturbances in North America," 2006.

[13] NERC, "Under-Voltage Load Shedding Program Data," 2006.

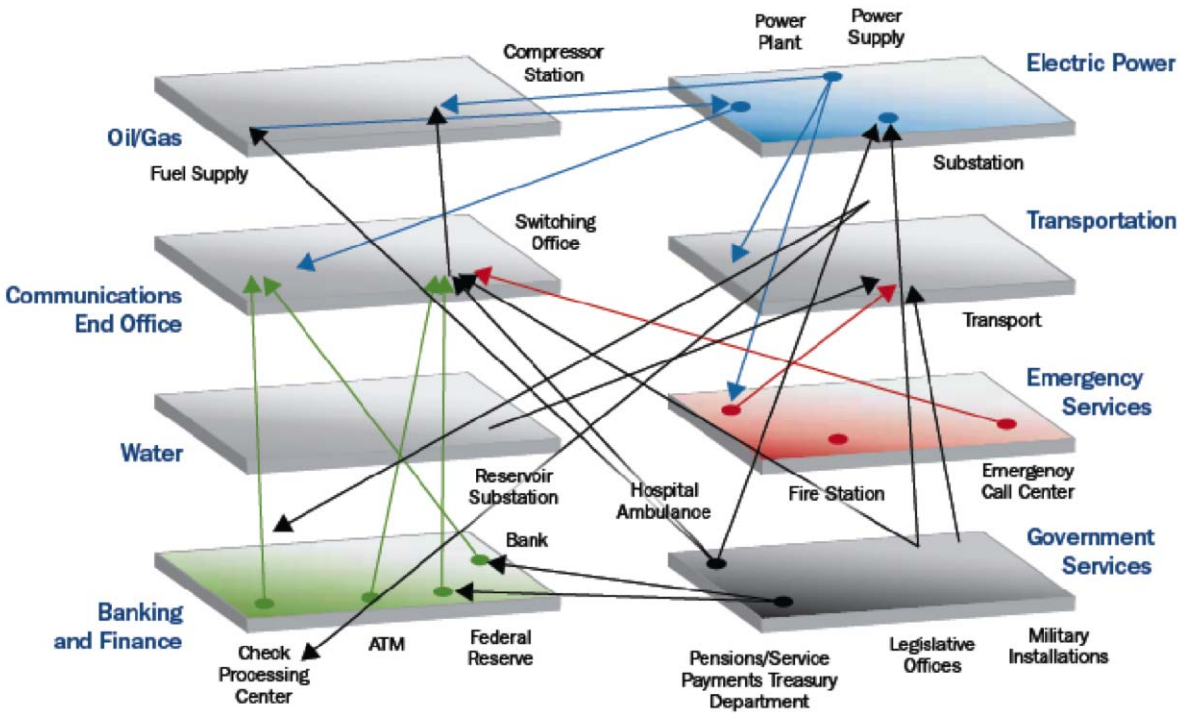
[14] NERC, "Under-Voltage Load Shedding Program Performance," 2006.

[15] FERC, "The Con Edison power failure of July 13 and 14, 1977: final staff report," ed. Washington, 1978.

8.0 Interdependencies with Other Critical Infrastructures

A Severe Event that broadly affects the BPS will in all likelihood have a significant impact on other critical infrastructures that depend on the reliable and continuous supply of electricity. Similarly, the BPS relies on other critical infrastructures that are necessary to support BPS restoration and operation. This section considers both aspects of these interdependencies.

Figure 6: Critical Infrastructure Interdependencies[43]



The U.S. and Canadian governments have programs in place to encourage greater protection and resilience of our nations' critical infrastructures. In Canada, "The *National Strategy and Action Plan for Critical Infrastructure*[44] establishes a risk-based approach for strengthening the resiliency of Canada's vital assets and systems such as our food supply, electricity grids, transportation, communications and public safety systems." Similarly, in the United States, the *National Infrastructure Protection Plan*[45] prepared by the U.S. Department of Homeland Security identifies 18 critical infrastructures.

[43] Source: Department of Energy, Energy Sector Specific Plan http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf
[44] Public Safety Canada: http://www.publicsafety.gc.ca/prg/ns/ci/index-eng.aspx
[45] DHS Critical Infrastructure: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

The table below illustrates the extent to which electricity is interdependent with many other infrastructures. These are discussed more fully in later sections.

Table 5: Key BPS Interdependencies

Critical Infrastructure	BPS Depends on Infrastructure for:	Infrastructure Depends on Electricity for:
Banking and Finance	Funds transfer	Funds transfer, cash distribution, functioning of the economy
Communications	Voice and data services	Voice/data centers and networks, internet providers
Dams (hydroelectric)	Energy source	Station service
Defense Industrial Base	-	Military bases and defense production facilities
Energy – Coal, Oil & Natural Gas	Electricity generation fuel source Backup generators, service vehicle fuel	Fuel production and transportation (pumping)
Energy – Electricity	Station service	Station service
Food and Agriculture	Food production (staff well-being)	Irrigation and food production
Government Facilities	-	Facility service
Healthcare	Staff well-being	Facility service
Information Technology	Automated tools	Facility service
Nuclear	Electricity generation fuel source	Station service, including safety systems
Transportation	Staff and equipment transportation	Communications and control systems operation
Water	Electricity generation cooling Staff well-being	Pumping and processing

The following describes some of the significant dependencies of the BPS on other critical infrastructures needed to support mitigation and restoration through a Severe Event.

8.1 Communications Sector

In addition to affecting the BPS, a Severe Event may also degrade the communications infrastructure. System operators may not be able to rely on telephone, cellular, email or dedicated broadband networks to communicate with entity staff, other entities, and key stakeholders. Alternative communications facilities need to be in-place and tested in advance of a Severe Event.

Effective BPS restoration and continued operation is highly dependent upon the ability to communicate, both voice and data, at all times. The highly interdependent aspect of BPS recovery and the communications infrastructure cannot be over-emphasized. Communications infrastructure and protocols are discussed in further detail in the Communications section.

Recommendations:

Entities should work closely with their communications service-providers to better understand mutual dependencies, identify priorities, and seek ways of mitigating the impact of severe disruptions.

- Identify specific interdependencies between telecommunication infrastructure and BPS infrastructure, such as voice and protection circuits, SCADA, remote terminal units and smart grid devices, necessary for BPS operations (e.g., key telecommunications facilities and their power system restoration paths and priorities).
- Ensure that critical telecommunications users are registered for priority wireless and land-line services such as:
  - U.S. Government Emergency Telecommunications Service[46] (GETS)
  - U.S. Government Wireless Priority Service (WPS)[47]
  - Industry Canada's Wireless Priority Service[48] (WPS).
- Identify risks and hazards such as failures, attacks, High Impact Low Frequency Events and/or congestion etc., that could impair the quality of service continuity, readiness, performance and time response of telecommunications.
- Explore opportunities and needs associated with emerging technologies (e.g., future 700 MHz, 1.8 GHz bandwidth frequencies, WIMAX, wireless priority services).
- Take mitigation measures (e.g., operational procedure changes, changes to priorities and procedures in restoration plans, design considerations, inter-entity information exchange).

[46] U.S. GETS http://gets.ncs.gov/
[47] U.S. WPS http://wps.ncs.gov/use.html
[48] Canadian WPS http://www.ic.gc.ca/eic/site/et-tdu.nsf/eng/h_wj00016.html

Key Recommendation #20 | Interdependencies with other Critical Infrastructures
Consider working with communications service providers to identify which of their facilities are critical to BPS operations. Determine which BPS and distribution facilities supply them and what backup power capacity is in-place (e.g., batteries, standby generators).

8.2 Dams (hydroelectric) Sector

Hydroelectric dams provide substantial generation in many regions of North America, and often provide critical blackstart services, as well as control water flows for irrigation, navigation, and elevation. Failure of key dams could have a significant effect on BPS operations.

Recommendations:

- Operators should develop a comprehensive understanding of the location and characteristics of hydroelectric facilities in their area and consider their ability to restart these facilities following a blackout.
- Some dams may be of more critical importance in their role of navigation, such as enabling coal supply via barge to key generating stations. Operational plans should identify the generators dependent upon navigable inland waterway supply for fuel transport or cooling water.

8.3 Energy Sector

The energy sector, in addition to electricity, includes natural gas, petroleum, and coal. Disruption to any of these fuel infrastructures could seriously impede BPS restoration.

Recommendations – Coal

- According to the U.S. Energy Information Administration, coal currently accounts for almost half of U.S. electricity generation[49]. Coal-fired generators are dependent upon frequent, in some cases daily, supply of coal from mine to power plant.
- Operators should ascertain and maintain cognizance of on-hand fuel supplies and storage capacity at coal fired generators.
- Operators should understand the coal transport routes in their area, consider possible supply disruption points, and explore alternate routes or transport modes.
- Operators should develop contingency plans around “out of fuel” scenarios in the coal fleet. What would New Normal operation look like in a short coal supply scenario?

Recommendations – Natural Gas

- Entities should understand[50] the gas pipeline networks and arrangements in place to supply gas-fired generators in their footprint (e.g., gas-fired generators and pipelines

[49] http://www.eia.gov/energyexplained
[50] Ref. NERC Natural Gas and Electric Power Interdependency report http://www.nerc.com/files/Gas_Electric_Interdependencies_Phase_I.pdf

that supply them, operator communications protocols during normal operations and emergencies).

- System operators should know which pipeline compressor facilities are gas versus electric powered and what gas pressure drops might be in the event of a sustained BPS outage. System operators will need to work with gas counterparts to understand power outage impacts on gas supply, and vice versa, and identify which are priority loads.
- In the event of a physical or cyber attack on gas infrastructure (including gas SCADA systems), system operators should consider the impact on gas-fired generation, and encourage their gas counterparts to share their plans to respond and restore operation.
- System operators should coordinate with gas operations personnel concerning their load shedding priorities.

Recommendations – Oil

- Oil is a relatively minor fuel source for the BPS, however system operators should assume these units will be unavailable due to unprecedented demand for diesel and gasoline fuel for standby and backup generators.
- Diesel fuel is needed for emergency standby generators at all critical BPS facilities that are without a reliable supply of power from the BPS during restoration. Entities should review contractual arrangements and establish priorities with fuel suppliers.
- Diesel and gasoline fuel is needed for transportation purposes. Regional Entities may wish to consider establishing regional fuel reserves for use in severe emergencies when normal fuel delivery channels may not be available for extended periods or when competing fuel demands (e.g., National Defense) take precedence for available supplies.

Key Recommendation # 21 | Interdependencies with Other Critical Infrastructures
Consider alternate suppliers, transportation paths, and agreements to support generating station fuel supply chains (e.g., coal, natural gas).

8.4 Information Technology Sector

Reliable operation of the BPS is highly dependent on the IT sector. IT is in turn heavily dependent upon electricity. Over the past decade, many entities have chosen to purchase or lease commercially available IT[51] systems and networks rather than build and support their own. Cyber attacks continue to increase in frequency and sophistication. System operators should be aware of the extent to which they rely on IT infrastructure, and should develop plans and procedures to enable recovery and New Normal operations in the event of significant disruption to the IT infrastructure.

Recommendations:

- Operations staff should work with entity IT staff to develop a comprehensive understanding of the IT infrastructure on which BPS operations are dependent. Consider elements of the infrastructure outside entity direct control, network interfaces

[51] In the context of this section, IT refers to entity business systems, rather than operational EMS or SCADA systems.

(if any) with operational systems such as EMS and SCADA, redundant systems and backup plans.

- Consider developing detailed operational plans in the event of major disruption to the internal or external IT infrastructure and Internet.
- Develop backup plans for telemetry that is critical to BPS operations in the event of a major IT infrastructure disruption.

Key Recommendation #22 | Interdependencies with Other Critical Infrastructures
Consider working with information technology service providers that are critical to BPS operations and consider augmenting the subject matter expertise of staff and suppliers to support these systems.

8.5 Nuclear Sector

Nuclear power plants are a key part of the generation infrastructure, providing 20% of electricity in the U.S. and about 15% in Canada. This segment of the power sector has long been heavily regulated from a safety and security perspective. Because of its unique nature and national security importance in the U.S., the nuclear sector was designated as its own critical infrastructure by the U.S. Department of Homeland Security, and has its own Sector Specific Plan under the National Infrastructure Protection Plan (NIPP). System operators are well versed in handling nuclear plant outages, and in the dependence of nuclear plants on BPS-supplied electricity. However, recent incidents, such as Fukushima, have focused renewed attention on the interdependencies of nuclear plants, the grid, backup fuel supply for cooling, and the transportation infrastructure to move that fuel. BPS restoration and New Normal operation should take into account the disruption of and potential long-term unavailablility of key nuclear power plants.

Recommendations:

- The industry is extensively studying the lessons learned from Fukushima. These lessons should be incorporated into BPS restoration and recovery plans.
- Nuclear plant operators and system operators should carefully calibrate plans and procedures[52] in the event of major disruption to either infrastructure.
- As has been learned from the Fukushima event, emergency cooling for nuclear plants highlights several key interdependencies: water, fuel, and transportation. Recovery plans and procedures should take account of these infrastructure interdependencies.
- Once off-line, nuclear plants can be out-of-service for extended periods. Recovery and New Normal operational plans should consider these implications carefully, particularly if nuclear generation provides a substantial source of energy to the area.

[52] NERC standard NUC-001 Nuclear Plant Interface Coordination http://www.nerc.com/page.php?cid=2|20

Key Recommendation #23 | Interdependencies with Other Critical Infrastructures
Consider alternate means to supply BPS power to nuclear plants and confirm these loads as critical to restoration and public safety.

8.6 Transportation Sector

The transportation infrastructure is highly complex. It includes rail, waterborne transport, surface transport, and aviation as well as pipelines that transport natural gas, crude oil, petroleum products, and water. All of these infrastructures are critically important to BPS operations. Almost half of generation is dependent upon coal that is transported via rail and barge. (Barge transport can be very dependent upon river/navigation conditions, including flooding, low water, and accidents.) Pipelines move the natural gas that fuels a quarter of the generation fleet, and is forecast to increase over time. Surface transport moves fuel for backup generation and mobility. In the future, electric vehicles will introduce new interdependencies as they consume electricity and may provide new demand response opportunities. Disruptions to any of these infrastructures can heavily impact BPS restoration and New Normal operations.

Recommendations:

- Emergency plans should be developed that "work backward" to inventory the transport dependencies affecting BPS operations, including basic requirements such as transporting workers to and from work locations.
- Emergency plans should identify suppliers of diesel fuel and gasoline for service vehicles and emergency backup generation and review how these supplies will be prioritized through a Severe Event.
- Backup and re-routing plans should be developed in the event of major disruption to primary transport networks. This could include secondary and tertiary routing plans to move coal, gas, and petroleum products. Disablement of a key river lock or railroad bridge, or key pipeline, could seriously affect BPS restoration. Alternative routing/sourcing should be planned for in advance.
  - In addition to evaluating existing stockpiles at generating stations, Operators should consider re-establishing coal inventory needs if operating in an islanded configuration for a considerable period of time, and consider if coal can be re-dispatched to more critical generators.
  - Operators should work with rail service providers and government to consider how to prioritize the shipment of coal or other fuels to priority generators.
- Operators should consider consulting with government to consider establishing strategic reserves of key fuels to be used in the event of significant supply disruption. This could be a shared regional system, modeled on the U.S. Strategic Petroleum Reserve.
- Transportation dependencies go beyond fuels. The transportation of key pieces of equipment, such as transformers[53], and other spare parts essential to BPS restoration. The same planning should be considered for these other items, to include alternative sourcing and transport mechanisms.

[53] Ref. NERC's Spare Equipment Database program http://www.nerc.com/filez/sedtf.html

8.7 Critical Infrastructure Sectors that Depend on Electricity

All critical infrastructures depend on electricity to varying degrees. System operators, working in consultation with other critical infrastructures and possibly local, state/provincial, or federal government authorities will need to prioritize loads and understand the extent to which they will be supplied through the mitigation and restoration phases following a Severe Event. Some of these infrastructure sectors and their importance in a Severe Event are briefly described below.

- **Government and Emergency Services:** In a Severe Event affecting the BPS, priority loads may include certain government loads, particularly those with no backup emergency power source. This may include police/fire, emergency services, command centers, and key military facilities. This will be critical to ensuring law and order and effective governance.
- **Defense Industrial Base:** Should a Severe Event be associated with an act of war, or a substantial threat to the National Security, supplying key elements of the defense community and its industrial base would become a priority load.
- **Water:** Water is essential for life. Failure to treat wastewater could result in widespread disease. Hence, supplying electricity for water and wastewater treatment plants and pumping stations will likely be a high priority load for restoration.
- **Healthcare:** Hospitals and healthcare facilities are always a high priority in an outage situation, and will be in any Severe Event to handle injuries or disease.
- **Agriculture and Food:** Food supply will be an important priority in a Severe Event. Electricity for irrigation pumping, food processing, and related purposes will be essential.
- **Banking and Finance:** An important priority will be to restore and maintain commerce. Thus the banking sector will be a priority load.

System operators should work with government authorities and other stakeholders to develop a plan for addressing these critical infrastructure sectors in the event of a severe BPS disruption. Most operators know their critical and priority loads under normal recovery operations, such as hurricanes and ice storms. However, new protocols may need to be developed to address these loads in the context of BPS restoration and New Normal operation after a Severe Event.

Training and Exercises

Training will be an absolutely critical element for personnel at all levels in order to gain an understanding of what types of conditions may be encountered in all phases of an emergency, and what the key interdependencies could look like. System Operators, field, and support staff will need this training as will senior management and other key stakeholders, including Government officials, law enforcement, defense, etc. Representatives of interconnected infrastructures should also be included so that information can be shared on key interdependencies and likely response patterns (this can avoid recovery procedures working against each other). The concept of a multi-sector New Normal should be a main theme of this training.

The training cannot envision every possibility. A major part of the training (like survival training) is to engender resourcefulness and flexibility in operational personnel. They understand the outlines of the problem and can then react to the situations at hand.

Realistic exercises should be a key part of the program. Exercises should include BPS personnel at all levels, plus key government representatives, and subject matter experts from other critical infrastructures. The exercises should be carefully documented and thorough after action reports prepared so that learning can be factored into planning and continuous improvement.

These activities should also be coordinated with the National Infrastructure Protection Plan, the National Response Plan and similar coordination elements of the federal and state/provincial governments of both countries.

9.0 Coordination with Government

Local, state/provincial and federal governments (government authorities) are key stakeholders in the electricity industry's response to a Severe Event. These government authorities are responsible for emergency planning and response, developing energy security and reliability policies. In the event of a Severe Event that spans a broad geographic area, government authorities – and perhaps the military – will have a large role to play. Just as the response by electricity entities to any Severe Event will be driven through local and regional entities first and foremost, the response from government will also likely be foremost a local and state/provincial response. As such it is important to be prepared to work with government authorities at all levels:

- Plan for a Severe Event, share your plan with government authorities, and know their plans.
- Understand local and state/provincial government concerns and provide them with information that will help address these concerns.
- Understand in advance how government may be able to assist during a Severe Event. Government authorities may be able to assist by providing resources or information.

This section provides a number of recommendations to enhance communication and coordination on the following topics:

- Overview of government authorities
- Coordination and communications prior to a Severe Event: planning, exercising, and training
- Initial communication and coordination
- Coordination and communication during restoration

9.1 Overview of Government Authorities

In order for entities to determine the government agencies they will need to coordinate with, entities need to understand the roles that government and first responders play, as well as their authorities and legal responsibilities. This will avoid potential conflicts, enhance coordination, and help each other understand respective needs. Entities charged with directing response and restoration should be familiar with government procedures for declaring emergencies at the local, state/provincial and federal levels. The laws, regulations, and plans for declaring emergencies and invoking emergency authorities are readily available on government websites. Entities should review the relevant emergency-related legislation and plans, understand the roles and responsibilities, and determine in advance of a Severe Event their points of contact with the appropriate government authorities. Involving these points of contact in entity emergency exercises will enhance entity understanding of the role of government authorities and help build positive relationships.

Some examples of government authorities involved in managing emergencies include:

- **Local and state/provincial emergency management** agencies and first responders, who prepare for and respond to all emergencies, especially those with responsibilities for the

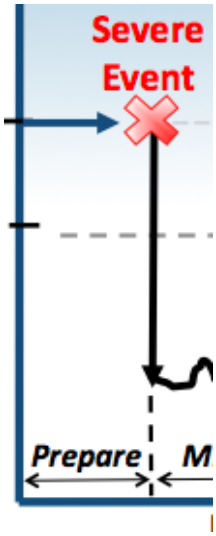
energy sector. These organizations are on the front line of emergency response at the local and state/provincial levels.

- **The lead authority for emergencies (usually activated at the Emergency Operations Center)**. State/provincial governments have a designated primary contact for managing emergencies.
- **State Governors** and provincial Premiers possess emergency authorities that they can exercise to mitigate the impacts of emergencies. Increasingly, state/provincial authorities (e.g., **State Homeland Security Directors)** have protection and vulnerability assessment programs in place involving the critical infrastructure sectors.
- **State/Provincial regulators, such as public utility commissions**, who oversee and regulate multiple sectors and systems, such as natural gas, telecommunications, and water systems, as well as important elements of the transportation infrastructure. This provides them with the capability to connect information between interdependent systems, and may also provide a nexus of infrastructure information that crosses a number of sectors at once. **State/provincial energy offices** typically serve many energy-related functions at the state/provincial level, including coordinating responses to energy emergencies, developing state energy emergency plans, and developing practices to improve energy security and reliability at the state-level.

Key Recommendation #24 | Coordination with Government
Confirm the roles, authorities, and points of contact between BPS entities and as appropriate, local, state/provincial, and federal governments.

9.2 Coordination and communications prior to an event: planning, exercising, and training

Critical and priority loads: Entities should work with government at all levels to inform them of the power system loads considered critical to power system restoration. Entities should also consult with government to identify priority loads that are essential to public health and safety. Establishing a common understanding of these loads prior to a Severe Event will help provide a basis to confirm or adjust these priorities, depending on the specific circumstances following a Severe Event.



Key Recommendation #25 | Coordination with Government
Coordinate with local and state/provincial government authorities and consumer stakeholders to identify priority loads to mitigate the impact on public health and safety.

Requesting regulatory exemptions and waivers: Entities understand that its operations need to comply with all applicable international, federal, state/provincial, local laws, standards (e.g., NERC Reliability Standards, OSHA, and Department of Transportation), codes, executive orders

and regulations. However, during a Severe Event, entities should consider seeking exemptions from certain regulations if this helps improve overall public safety.

Entities should identify waivers they may request from state/provincial and federal agencies to continue operations under stressed conditions (e.g., environmental emissions, truck driver hours). Identify entity and agency emergency contact information and know each waiver's limitations (i.e., expiration and renewal terms). Work with government authorities to confirm detailed procedures. Keep any required forms available and completed in advance to the extent possible, and review them annually.

Key Recommendation #26 | Coordination with Government
Consider developing a list of regulatory exemptions or waivers that will materially improve restoration and operation (e.g., plant emissions, truck driver hours) and consult with state/provincial and federal agencies.

Credentialing: Government first responders (e.g., police, fire, ambulance) have become more aware in recent years of the need to provide access to critical infrastructure work crews. Access to the affected area will be important as soon as it can be provided safely. If possible, access policies should be established with government authorities prior to a Severe Event. Areas with a history of reliance on mutual assistance for recurring disasters (such as for hurricane response) may have protocols in place; in the event of a Severe Event some protocols (depending on communications systems that may not be operational) may need to be available for use without transmittal, or a working access and credentialing protocol may be needed.

Recommendations:

- Consider consulting with government authorities to understand what access policies may be in place during a Severe Event.
- Consider having entity staff meet with local law enforcement personnel to discuss access requirements and build a cooperative relationships.

Considerations:

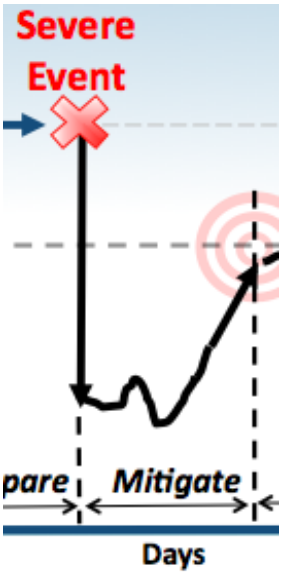
- Do you know what kind of documentation would be needed to reenter affected areas?
- Is there a plan in place to procure and disseminate the necessary documents if communications systems are down?
- Have you discussed an access plan with government authorities that cover you, your mutual aid, and contractors? Consider alternatives in case information technology is compromised.

Building Trust with Decision Makers: Realistic exercises that involve entity personnel at all levels, key government staff, and other critical infrastructures are essential to preparedness. Following exercises, participants should identify action items and next steps for future planning and continuous improvement.

Budgets: Governments have the means to declare a state of emergency and invoke the authorities needed to respond to the situation. Entity emergency management plans should recognize government roles and responsibilities when they exercise that authority, and how they will become aware of changes that may impact entity operations. Entities should engage with government to help ensure a common understanding of mutual needs.

9.3 Initial Communication And Coordination

It will be very important that entities begin communicating with the appropriate government authorities at a very early stage of a Severe Event to provide updates both on a scheduled basis, and as urgent developments occur. This will help ensure that decisions are made using the best available information.

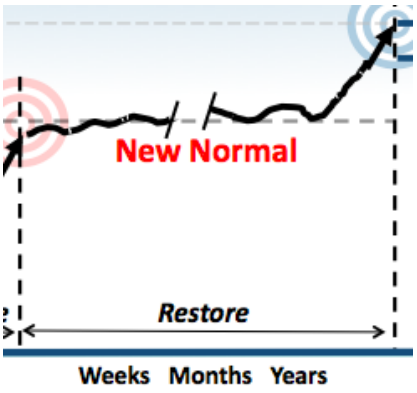


Some of the key issues that should be communicated with government authorities, especially with local and state/provincial emergency operations centers, include:

- Restoration assessment and prognosis
- Share needs and priorities
- Coordinate with other critical infrastructures
- Coordinate public announcements and schedules for voluntary and mandatory load shedding, including rotating blackouts
- Requests for protection and security

Recommendation: Entities should consider establishing crisis management teams that consist of broad stakeholder and technical representation and establish clear lines of communication with government. Similar to what many entities do during major weather events entities should consider co-locating at their state/provincial emergency operations centers 24/7 for as long as necessary.

9.4 Coordination and Communication During Restoration



Restoration and operation through the New Normal period will require scarce resources to be continuously reprioritized and reallocated. Government is ultimately the locus for determining public health and safety priorities for resource allocation, and as such, government authorities will need information about what supplies, resources, and materials are available, as well as the prospects and progress of restoration in order to make informed decisions.

Electricity entities in Canada and the U.S. have a long history of sharing resources and work crews to aid restoration following hurricanes and severe floods. In an effort to facilitate crossing the U.S. and Canadian border during emergencies, the Canadian Electricity Association is working with the Canadian Border Security Agency and the U.S. Department of Homeland Security. A *Cross-Border Mutual Aid Assistance Agreement* has been prepared and is expected to be implemented in the near future.

Government authorities and electricity entities should have primary, alternate, and possibly tertiary contacts and means of contact, including provisions for 24x7 contact. Hard-copy contact information lists should be maintained and reviewed at least annually.

Entities need to be familiar with government emergency management structures. For examples, entities in the U.S. should be familiar with the government's Incident Command System [ICS]/National Incident Management System [NIMS] principles[54]. Requests by entities should be referred through the appropriate channels.

Continual Review of Legal Authority: Legislation and supporting regulations define the role of government agencies during emergencies. Entities should be familiar with these and understand how emergency authorities may affect entity operations. During a Severe Event, government may revise these or enact new authorities. Entities will need to stay abreast of these changes, understand how they may affect the entity, and have mechanisms in place to communicate them quickly across the entity as appropriate.

Understanding Impacts: It is important for the government to understand the role played by BPS entities and vice versa. Requests for information should not distract or impede those who are engaged in operational roles such as restoration and crisis response. It is also important that government understand the actions that asset operators will be taking, and that actions will be underway independent of any emergency declaration by government. However, as the days add up to weeks after a Severe Event, decisions regarding changing priorities will be required.

[54] Ref. http://training.fema.gov/IS/NIMS.asp

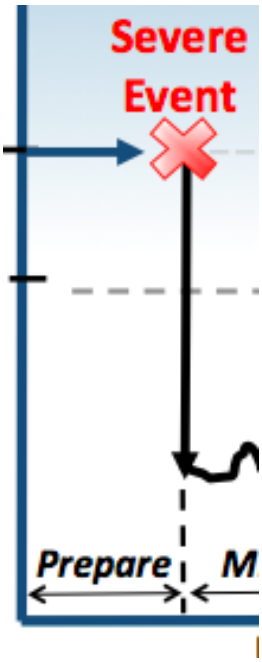
Recommendation: Government authorities and electricity entities should coordinate closely so they are prepared to explain the actions they are taking or are about to take, and why. Decision-makers will need to understand the second and third order effects of making such priority selections. For example:

- The sequence of electricity service restoration to consumers in different geographical areas or regions will vary depending on circumstances such as the availability of resources and the nature of any damages to equipment.
- If the cause of the Severe Event is continuing, restoration may need to be halted, or re-started.
- If fuel is not prioritized to communications facilities, the ability to operate portions of the BPS will be severely limited.

References

- http://disaster.ifas.ufl.edu/PDFS/CHAP03/D03-07.PDF
- http://www.nyu.edu/intercep/businesscase/index.html - New York University / International Center for Enterprise Preparedness
- http://www.fema.gov/privatesector/preparedness/
- http://www.oe.energy.gov/our_organization/iser.htm - Department of Energy
- http://www.fema.gov/pdf/about/stafford_act.pdf
- http://www.naruc.org/cipbriefs/ - NARUC briefs on critical infrastructure protection
- http://www.naseo.org/eaguidelines/ - NASEO and NARUC Energy Assurance Planning guidance

10.0Taking Care of People



The electricity sector has extensive experience planning for emergencies. While these plans often focus on repairing or replacing physical assets and taking the necessary operating actions, success is highly dependent on our most important asset – knowledgeable, capable, and available personnel. Without question, a Severe Event will put great stresses on personnel throughout the New Normal period.

This section provides guidance on topics that should be included in an entity's disaster recovery plan or business continuity plan. Much of this information is based on past experience in disaster response operations and also includes lessons learned in everyday operations. While many of the suggestions might seem obvious, past experience indicates they may not be achievable if not planned in advance of an event. This guidance is provided in the context that can easily be modified for inclusion in entity plans.

This section discusses the following topics that should be considered as part of an entity's plans.

- Accommodation
- Safety considerations
- Employee and family Issues
- Respite facilities
- Counseling

10.1 Accommodation

Consider alternate housing arrangements that would be suitable during the Mitigation Phase as well as the longer Restoration Phase. Traditional support infrastructure such as hotels, restaurants, and grocery stores will most likely not be available or unable to support the influx of personnel and displaced residents of the affected areas.

An example of an extended restoration event is the recovery of Entergy's system after the catastrophic damage caused by Hurricane Katrina and the subsequent failure of the levy system around New Orleans. Because of its experience, Entergy modified its existing plans to include many of the recommendations provided in this section.

Recommendations

Housing options could include rental housing, apartments, hotels, tent cities, campgrounds, employee travel trailers or campers, cruise ships or military vessels, and federal, state/ provincial shelter facilities. Identify points of contact to determine how these options would be acquired and implemented.

10.2 Safety Considerations

Maintaining operations through the New Normal period can be stressful and hazardous. There is never a good time for an accident or operating error, but this is especially true during a Severe Event. Paradoxically, experience has shown that safety rates can be better during major disaster response and restoration than during routine operations. This may in part be due to the initial increase in adrenalin and commitment to tasks that are of immense value to their peers and the general public. But it is not reasonable to assume that this will continue through the weeks or months of a Severe Event. The onset of fatigue and stress will contribute to increased errors. Accidents or operating errors can delay or even halt restoration efforts.

Entergy's Experience from Hurricane Katrina

Entergy's headquarters and nearly 1,000 employee homes were initially uninhabitable. Entergy secured office space to replace its New Orleans area work locations and arranged interim housing for displaced employees for 7 months. Entergy has since implemented long-term office relocations as an integral part of its disaster recovery strategy.

For entity incident and disaster planning, safety for personnel families and personnel performing operational restoration is a primary consideration. While many of these apply to "normal" emergencies, they can become particularly important during a Severe Event.

Recommendations

- **Advanced warning** – If the Severe Event is preceded with advance warning, provide guidance on when and where to evacuate.
- **Proper permits** – Many entities require specific certifications and permits. Procedures should be documented on what permits and certifications may be waived through a Severe Event.
- **Safety teams to oversee work conditions** – Safety teams should monitor for signs of fatigue and stress and have the authority to stop work when conditions are unsafe. This may require an increased role for the entity's internal health and safety oversight organization.
- **Transportation** – Transporting personnel safely and reliably between work and rest centers will decrease stress.
- **Stock of supplies** – For shorter-term events, experts recommend having a minimum of a seven-day supply that will need to be adjusted for a Severe Event, but the same considerations for health and nutrition are applicable. Entities should consider stocking non-perishable foods and food in pouches; proteins, fruits and vegetables; and foods that do not require extra cooking and can be eaten cold if necessary. Store water, at least one gallon per person per day. Remember to have on-hand manual can openers, cooking utensils, pots and pans. Include aluminum foil, paper towels, garbage bags and disposable cleaning wipes. Have sufficient rotated stocks of batteries for flashlights and radios. Make up a good first aid kit and stock up on cleaning supplies, especially bleach, gloves and heavy-duty garbage bags. Keep freshly stocked emergency kits with vitamins and over-the counter medications that might be needed, such as pain relievers, antacids and cold-relief medications.

- **Notification of well-being** – Entities should provide communication options to allow personnel to contact family. Personnel should be patient as communication systems are likely to be disrupted. Typically, personnel will establish a family communication plan that establishes a time frame for contacting family after the event.
- **Encourage personnel to develop an individual or family Emergency Medication Plan** – Entities could develop and provide a sample plan to its employees. This may include the following:
  - Consult an individual's healthcare provider, especially for complicated or difficult-to-administer medications, such as those requiring pumps or nebulizers.
  - All medications should be kept in one location in the home, to expedite any evacuations or ease in retrieving medications after an event. Along with your prescription identification card, individuals should keep a list of their medications and those of other family members, including drug name, strength, dosage form and frequency.
  - If there is a shortage of medications for personnel, entities may consider helping to secure medications or work to have key personnel placed on a priority list for medications.
  - Keep the names and phone numbers of your doctor and the pharmacy that filled your prescriptions in your wallet. If possible, the entity should work with a local pharmacy or its mail-order service to help personnel address any prescription needs.
- **Personal protective equipment** – Ensure that an entity has and provides to field personnel the appropriate personal protective equipment.
- **Personnel in new roles** – When redirecting personnel into new roles which require more physical effort, leaders must take into consideration any health issues a staff member may have been able to control in under normal circumstances, but may be further exacerbated after a Severe Event.
- **Plan for medical response** – Enhance first-aid packs, and prepare for on-site medical care teams.
- **Worker rest** – Manage worker rest based on conditions and tasks. Ensure appropriate rest time between and during work shifts and provide safe, comfortable, and quiet facilities.
- **Security** – Provide security in areas where potential civil unrest may erupt that includes personnel guidance on how to manage such unrest.

10.3 Employee and Family Issues

Every employee and their family should have a personal emergency plan that recognizes and mitigates the risks faced in a given community. An entity's business continuity or disaster recovery plan should identify the relative criticality of each job function and inform employees potentially affected. As part of this planning, the entity should clearly communicate the level of support it will provide in situations covered by business continuity plans or disaster recovery plans so that employees in non-critical job functions may also plan appropriately. Employees who do not fill critical job functions should be instructed to check-in for reassignment.

During an event, health and safety concerns are a primary consideration. During a Severe Event, this concern extends to all personnel and their families. The success of restoration for an entity could hinge on whether the families of employees are safe and able to get back to some semblance of a normal set of activities.

Operating Iraq's Grid in an Unstable Security Environment

With Iraq's unstable security situation and a shortage of system operators, generation, transmission and distribution station staff were expected to live on site. Given the high levels of sectarian and personal violence many families of staff were moved into the stations as well. Often the station staff would provide the residents surrounding the station with scarce electricity and create a friendly buffer around the station.

Recommendations

Some key topics that should be considered in disaster recovery plans that may need to be in place for months following a Severe Event include the following:

- Supplies and respite
- Communications
- Transportation
- Safety
- Education
- Child/elder care
- Secure homes
- Relocating employee's family to safety as necessary
- Food and necessities
- Continuity of pay and banking services

10.4 Respite Facilities

Immediately following a Severe Event, basic needs need to be met to help reduce personnel and family stress. Although the following recommendations appear to address the immediate need after a Severe Event, the human factor related to respite to prevent burn-out is something that will need to be addressed throughout the New Normal period.

Recommendations

Rest Area

- Provide an area that is covered and dry
- The area should contain heating and cooling with good ventilation
- Provide for personnel to sit or lie down
- Provide an area suitable for activities and discussions, and a separate quieter area for rest

Water

- Ensure personnel stay well hydrated.

Respite Facilities following the 9/11 Terrorist Attacks

During the search and rescue and the subsequent clean-up at Ground Zero after the 9/11 terrorist attacks on New York, respite centers remained in the work-zone for an extended period of time.

- Reserve potable water for the essentials of drinking and food preparation. Other treated water may be suitable for showering and hand washing.
- Ensure water is treated and managed properly; serious diseases can be transmitted by untreated water.
- Properly dispose of or recirculate gray water to protect the potable water supply.

Food

- Ensure adequate supplies of healthy food. Consider long shelf-life foods, stock-piled in advance.
- Maintain clean and comfortable meal facilities.
- Store perishable foods below 45 ºF and serve heated food above 140 ºF.
- Dispose of perishable foods not properly stored after 4 hours.
- Consider weather conditions and temperatures to determine whether hot or cold foods should be served.

Hygiene

- Provide hand washing or disinfecting facilities at all food service areas, rest rooms, and disposal areas. Disinfecting and hand washing is the single-most important measure in preventing food-borne illness and must be enforced at all times.
- Provide individual hand cleansers and liquid hand sanitizing gel to personnel.
- Provide for bathing and clothes washing at respite facilities.

Rest Rooms and Waste Disposal

- Ensure portable latrines are available, cleaned regularly, and located in appropriate areas.
- Ensure waste is managed appropriately and designate storage locations away from living and work areas.

10.5 Counseling

Everyone involved in maintaining operations during an event are dealing with increased stress and anxiety. In certain events, there is a potential of the tragic loss of life and material possessions that will affect each person involved. Personnel must seek care from a stress management team or other options provided by the entity when they feel overwhelmed or unable to cope with maintaining operations. Many times during stressful situations personnel need someone to talk to that is not involved in the situation so they are not burdening their relationships with others close to them.

Recommendations

During normal business operations, Human Resource (HR) departments usually have the responsibility of benefits that may include various types of counseling programs. HR may want to consider expanding their business continuity plan to include counseling programs for

incidents. An entity may consider establishing a counseling center at a respite location. Because situational stress and loss of life could include personnel (internal and external) and personnel's family members, the business continuity plan should establish a process to expand the needs of its typical employee assistance program to deal with needs of those individuals outside its organization. Remember personnel performance can be affected by the problems of an employee's immediate family members. In addition to the services provided by the entity, personnel may seek guidance from local religious leaders.

Key Recommendation #27 | Taking Care of People
Consider ways to support the health, safety, and well-being of personnel and their families in the face of extraordinarily demanding circumstances.

References

National Rural Electric Cooperative Preparedness Plans, Building Operations Plans

Communities of the National Capital Region, Be Ready Make a Plan, www.makeaplan.org

PUBLIC ASSISTANCE PROGRAM (Public Assistance, Emergency, Fire Suppression) DCA/DEM/BRM Recovery Office STANDARD OPERATING GUIDLINES the Florida Division of Emergency Management web site is: http://www.FloridaDisaster.org

Preparing Makes Sense Get Ready Now Brochure, United States Department of Homeland Security www.ready.gov/.../Ready_Brochure_Screen_EN_20040129.pdf

A Guide to Business Continuity by James C. Barnes, 2001, Wiley Press, ISBN: 0-471-53015-8.

Security Planning & Disaster Recovery by Eric Maiwald and William Sieglein, 2002, McGraw-Hill/Osborne Press, ISBN: 0-07-222463-0

Business Continuity Planning edited by Ken Doughty, 2001, Auerbach Publications, ISBN: 0-8493-0907-7

Business Resumption Planning by Edward S. Devlin, Cole H. Emerson, Leo A. Wrobel, Jr, and Mark Desman, 2001, Auerbach Publications, ISBN: 0-8493-9945-9

11.0Logistics and Self Sustained Operations

This section identifies the challenges associated with the logistics of acquiring, delivering, and replacing or repairing assets damaged in a Severe Event and provides guidance on effective logistics to support operations through the New Normal period.

The key to identifying the best use of resources is dependent on the entity's ability to respond and think "outside the box" of normal planning for emergencies. Many of the items suggested are counter-intuitive to operating in a normal environment. Of necessity, many decisions will be spur of the moment decisions and may have un-intended consequences later as restoration progresses from the New Normal period to pre-event reliability. For example, suppose early in the restoration process a decision is made to cannibalize a substation for parts to rebuild other substations. As load continues to be restored over the New Normal time period, eventually the substation that was cannibalized will need to be rebuilt.

Decision-makers will need to understand the current operating situation and prioritize logistical needs in the absence of much of the information normally available. Initially, the efforts will focus on dispatching existing inventory to restore the critical loads essential to BPS restoration. Efforts will then rapidly shift to dispatching inventory to support priority loads, many of which will be on the distribution network.

Procurement processes suitable for normal operations to meet an entity's policies or government requirements may need to change to provide the flexibility and responsiveness needed during a Severe Event.

11.1 Specialized Equipment

Specialized equipment such as high voltage transformers, circuit breakers, turbines, phase shifters, and series capacitors often take a year or longer to procure and build. Consider the following:

- Participate in spare equipment consortiums that allow the use of other's spare inventory (e.g., NERC's Spare Equipment Database program[55]).
- Locate spare equipment at a site that is more secure than the sites where they may be needed.
- Develop agreements with other utilities to share spare or redundant equipment. If agreements already exist, discuss the implications of a Severe Event with the participating entities and consider how decisions would be made to appropriately allocate spare equipment. This is important because those owning the spare equipment will increase their operational risk by releasing spares.

[55] Ref. NERC Spare Equipment Database Task Force report http://www.nerc.com/filez/sedtf.html

- Maintain a list of suppliers and service level agreements for highly specialized installation or transportation equipment such as cranes for heavy equipment and Schnabel rail cars for large high voltage transformers.
- As opportunities arise to replace transformers that are aging or have insufficient capacity, convert substations operating at non-standard voltages to more common voltages.

11.2 Standard Equipment

While standard equipment such as structures, hardware, insulators, distribution components, etc. may be more readily available; replacement inventory will still be constrained. Consider the following:

- Compile a list of regional and national suppliers with around-the-clock contact information, and ensure the list is readily accessible during a Severe Event.
- Review existing spare equipment and material inventories under a Severe Event scenario and identify opportunities to improve these inventories.
- Create a salvage control center which could amass materials to be re-dispersed to key restoration areas. Cannibalize spare parts from damaged equipment or from less critical plants and substations.
- Siphon fuel from inoperable equipment.
- Re-allocate tools such as compressors, chargers, lifts from in-operable equipment.
- Re-allocate redundant equipment to facilities that need them.
- Use temporary design standards that use less material (e.g., wood and steel beams in lieu of concrete foundations, increase span distances between towers without sacrificing public safety).
- Remove obstacles from beneath transmission lines to increase clearance. Increase clear-cut corridors to manage vegetation growth with fewer resources.

Wal-Mart and Home Depot Hurricane Response

Wal-Mart and Home Depot, valuable sources of many different consumables that may be required, have emergency response plans that have proven very effective during hurricane response.

11.3 Fuel for Transportation and Backup Generators

Entities have contracts in place with suppliers to provide fuel for vehicles and generators. However, during a Severe Event the fuel suppliers may also be impacted and normally used delivery systems or routes may be unavailable. Entities should enhance their arrangements with suppliers in advance of a Severe Event to consider alternative delivery systems. Regardless, entities need to consider how they would prioritize their allocation of limited fuel supplies.

Table 6: Sample Fuel Priorities for Critical Equipment

Critical Load	Rationale for Priority
Backup generators at nuclear stations	In the event of a loss of BPS power supply, enhance recovery, prevent extended unavailability, or maintain safe shutdown
Backup generators at non-nuclear generating stations	In the event of a loss of BPS power supply, enhance recovery and prevent extended unavailability
Backup generators at transmission substations	Supply station service auxiliaries (e.g., compressed air for breaker operation, protection systems, station monitoring devices and systems)
Backup generators power plant and system control centers	Supply critical operations at Reliability Coordinators, Transmission Operators, Generator Operators
Backup generators at telecommunications centers	Supply communications facilities and systems needed to operate the BPS
Vehicles	Transport personnel and resources needed for BPS restoration and supply to critical loads and priority loads

Key Recommendation #28 | Logistics and Self-Sustained Operations
Consider with fuel suppliers ways to prioritize the supply and delivery of fuel for emergency standby generators and essential work vehicles.

11.4 Transportation Routes

Evaluate alternative transportation routes. It is likely that the transportation sector (e.g., airlines) would be heavily impacted. This occurred with September 11th and with recent volcano eruptions shutting down air traffic into Europe, South America, Australia, and New Zealand. Natural disasters combined with terrorist activity could easily impact the railroad or highway system to large parts of the continent.

Seasonal issues such as ice storms, blizzards, hurricanes, and flooding can compound the impact of the Severe Event on transportation. Consider alternate transportation modes (e.g., rail, air, water, truck) that may not be appropriate during normal circumstances.

Establish contact with and develop relationships with state and local government transportation authorities who can help identify transportation routes and approve any transportation permits that may be required by utilities, transportation service-providers, or mutual assistance partners.

11.5 Personnel and Facility Resources

Whether using entity employees or external resources, a Severe Event will strain the entity's ability to respond to a Severe Event. Planning to effectively use human resources during a Severe Event will optimize the utility's ability to respond.

Entity Employees

Business continuity and disaster recovery plans should identify the key personnel needed to restore and maintain critical operations, and recognize the increased intensity associated with filling these roles through the New Normal period. Plans should address scheduling additional personnel to assume these critical roles or provide operational support. Plans should address issues related individuals who are unwilling or unable to report for work. The plans should also consider how to supplement these key roles with personnel who can be shifted from lower priority work and quickly trained to fill critical roles. For every critical role, there should be at least one individual with primary responsibility and a fully trained and experienced backup. Identify, train, and explicitly recognize individuals to fill these roles.

Plans should identity the initial work shift hours and team or crew composition. For example, during the first few days of an event shift durations may be different than later in the event when circumstances may be more predictable. Consider changes that may be required to employee work arrangements (e.g., collective agreements) such as work schedules and alternate roles and responsibilities.

- **Management Personnel** – Management will need to be ready to make important decisions to support personnel operating in unusual situations, including working out of their normal scope of responsibilities or levels of authority.
  - With the necessary refresher or certification training, a manager with experience in the field and technical trades could assist as an equipment operator, control center operator, or foreman.
- **Field Personnel** – Field personnel will play front-line operational roles to identify damage and repair or replace damaged equipment.

  - With suitable training, a groundman may perform certain duties as a line hand on a de-energized line.
  - Journeymen linemen may provide support in roles such as relay technician assistants or substation assistants.
  - Warehouse staff may provide groundman support for line crews.
- **Operating Personnel** – Operating personnel are typically the first to recognize an event has occurred and are instrumental in activating their entity's plans. They will need to maintain situational awareness, make decisions and direct operations clearly and concisely at all times.
  - Back office engineering staff may support system operator functions.
- **Office Personnel** – Office personnel will not likely be directly involved in the front-line of restoration activities, yet the most important aspects of their roles will still need to be carried out and they may be re-deployed to new tasks.
  - Engineering or office staff may fill needed roles in logistical operations such as procurement or warehousing.

Leadership and Succession Planning

During a Severe Event, it is particularly important that personnel know at all times the manager or supervisor who will provide them with direction and operational support. Circumstances will require these leaders to change roles through the New Normal period, and succession planning will be a critical element of an entity's strategic direction and operational success. It is vital that leaders at all levels continue to find, assess, develop, and monitor the personnel resources needed to manage New Normal conditions. As the New Normal period progresses, working conditions may become more stable, and entity leaders may resist losing competent personnel to other roles, and having to train their replacements. Leaders themselves may be reluctant to move into new areas of responsibility. Leaders need to understand that succession planning must continue to match rapidly evolving organizational needs with employee competencies and capabilities. Effective succession planning will form the basis for continued success through the New Normal period. The succession planning process for the organization should:

- Define the skills and competencies needed through the New Normal period.
- Identify leadership and personnel competency gaps.
- Observe and periodically assess how leaders and personnel are coping in their roles.
- Identify personnel who are demonstrating an ability to assume increased responsibilities.
- Foster a growing sense of responsibility for personnel to display leadership characteristics at all levels in the organization.

Clearly Define the New Roles

It is important that personnel understand their new roles and who their manager or supervisor is at all times. Personnel need to know who provides them with technical direction and who they can rely on when they need to seek help or advice. Personnel roles and responsibilities should be clearly defined and documented and include:

- **Reporting structure** – present and new role, new work locations, new manager or supervisor, working hours and shifts
- **Expectations of the new role** – personal equipment provided by the individual (e.g., tools, personal protective equipment), equipment that will be provided at the work location, professional qualifications, certifications, or licenses required.

External Resources (Contractors, Mutual-Aid providers)

Entities often rely on externally contracted resources to fill roles similar to those of entity employees, for example for major projects. Entities need to consider that these contracted resources may not be available during a Severe Event, as other entities will have similar incremental needs to respond to the Severe Event. Prior to a Severe Event, entities should consider establishing contracts with these resources that explicitly address what may or may not be provided through a Severe Event (e.g., force majeure).

Mutual aid arrangements with other entities allow entities to quickly supplement their existing workforce. Recognizing that neighboring entities may be similarly stressed, consider making arrangements with a number of geographically dispersed entities to help ensure that assistance can be obtained from areas outside the affected region. Similarly, consider how you may be able to assist other entities, particularly with personnel other than the work crews historically familiar with working in new work locations (e.g., system operators, system planners, control room support staff). The terms of these arrangements should be reviewed periodically.

Key Recommendation #29 | Logistics and Self-Sustained Operations
Consider how your business continuity or disaster recovery plan would change if you are unable to rely on mutual support arrangements.

Alternate Work Locations

During a Severe Event, it is possible that the primary work location may be unavailable and personnel will need to work from backup or other temporary locations. Personnel should be trained on how to deploy to the alternate location and start work safely and efficiently.

Alternate work locations, which may include fields for staging work, empty warehouses, or schools should be identified and tested periodically. Plans should consider:

- Alternate backup facilities if both primary and backup operations centers are unavailable.
- A communications plan to quickly and reliably direct personnel to backup facilities.
- Van pools to safely transport employees and conserve fuel.
- If working from home is viable, ensure personnel have the tools to effectively work prior to any event.

12.0 Preventing and Responding to Physical Attacks

While this report provides generally applicable guidance for entities to prepare, mitigate, and respond regardless of the cause of the Severe Event, this section specifically addresses a coordinated physical attack scenario.

It is impossible to completely prevent a determined physical attack on BPS infrastructure. However, steps can and should be taken to prepare to make such an attack more difficult and/or less effective.

This section discusses the following topics:

- **Challenges** – The challenges of preventing and preparing for physical attacks.
- **Prevention** – Steps that should be considered to protect facilities in a way that will discourage attacks, make attacks more difficult to accomplish, or minimize the damage.
- **Preparation** – Steps that should be considered in advance, to prepare to respond to a physical attack.
- **Response and Recovery** – Steps that should be considered to effectively respond to a physical attack, and how security might change to support operations through the New Normal.

Assumptions

This section assumes the following scenario:

- A simultaneous and coordinated physical attack directly impacts the BPS. Equipment at multiple generating stations and high voltage transmission substations are severely damaged.
- Subsequent attacks days or weeks later will continue to impact BPS equipment and place field personnel at risk. Law enforcement and National Guard support to protect field personnel and equipment is very limited due to the priority to protect the communities they serve.
- Voice and data communications are disrupted due to equipment damage (microwave towers, fiber cuts, etc.). Cell phone systems are jammed due to excess traffic.
- Transportation is disrupted due to widespread power outages.

12.1 Challenges to Protecting the BPS

In order to provide some insight into why some prevention and preparation strategies are suggested and others are not, the following provides context for subsequent sections.

Asset Protection

BPS assets are dispersed widely across the continent, usually in remote areas, making complete protection infeasible. Protection is often limited to fencing and padlocks at facilities that are operated remotely and not staffed.

Mixed Environments

Some BPS assets are in rural, remote locations while others are in urban, densely populated areas. This makes protection difficult and the resulting procedures complex.

Multi-Jurisdictional

Because service territories rarely align within a single municipality, it is typical for entities to need to deal with many different local law enforcement agencies to address security issues. This multi-jurisdictional nature is not limited to the geographic location of the assets, but also involves understanding the various different government agencies and their roles.

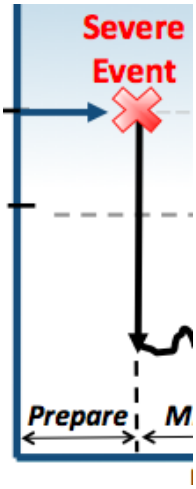
Replacement Assets

Many BPS assets are difficult to replace or repair – some require purchasing lead-time of many months. This suggests that greater protection is needed for these assets.

Ease of Asset Identification

Due to the size, accessibility, and visibility of high voltage power lines, identifying equipment that is part of the BPS is relatively easy.

12.2 Recommended Prevention Strategies



While it is impossible to completely prevent a determined physical attack on BPS infrastructure, actions should be considered to implement prevention measures that will deter or limit an attack by making it difficult to locate, enter, and damage a facility.

Obfuscation

A facility that 'blends' into its surroundings is more difficult to identify and decreases the chance it will be targeted. This can be accomplished by:

- **Security by Environmental Design** – Where possible, establish visual barriers such as trees, mounds, and bushes.
- **Security by Architectural Design** – Where possible, use matching building material that blends the asset into the neighboring buildings.
- **Fly Zones** – Do NOT identify locations as 'no fly zones' to the Federal Aviation Administration and Transport Canada. The resulting maps available to all pilots are widely published and will clearly identify the location of the facilities.

Hardened Facilities

Design facilities, particularly those that are critical assets, to increase the effort required to damage the facility or make it difficult to gain access. Install equipment to detect and report a security breach. This can be accomplished using:

- Basic construction techniques, such as:
  - Higher and stronger walls
  - Fewer windows and doors
  - Reinforced gates
- Install monitoring and sensing equipment, such as:
  - Cameras
  - Vibration Detection
  - Motion Detection
- Involve the local community, for example by enhancing Neighborhood Watch programs to raise awareness regarding the local BPS facilities that they rely on.

Key Recommendation #30 | Preventing and Responding to Physical Attacks
Consider actions that can be taken to protect BPS assets by involving local communities and law enforcement (e.g., reinforcing their awareness of BPS facilities that are critical to operations).

Key Recommendation #31 | Preventing and Responding to Physical Attacks
Consider ways to improve security when designing or refurbishing existing BPS facilities.

12.3 Recommended Preparation Strategies

The strategies suggested in this section pertain to preparatory actions that may be taken prior to an attack to manage likely consequences. These actions will help ensure that assets are prioritized, vulnerabilities and risks are understood, law enforcement support is coordinated, and plans and teams have been developed and exercised.

Consequence Assessments

Consider conducting consequence assessments to evaluate and prioritize BPS assets. Consequence assessments should consider the impact on the entity, as well as impacts on society and other critical infrastructures within the entities footprint of operation. Criteria to identify critical assets for NERC Reliability Standard CIP-002-1 are provided in the *NERC Security*

Guideline – Identifying Critical Assets[56]. Additional information is available in Section 3 of the DHS National Infrastructure Protection Plan[57] that provides a generic methodology for consequence assessments.

Physical Vulnerability Assessments

Conduct physical vulnerability assessments to identify threats, vulnerabilities, loss impacts, prioritize risks, and identify cost effective controls. Assume that critical assets will be targeted.

Strategies

Identify strategies for emergency response, operations recovery, and system restoration.

Site Security Plans

Develop, exercise and maintain site security plans that provide for the protection of assets and personnel from physical attacks. Site security plans should be based on the results of consequence assessments as well as risk and vulnerability assessments. The countermeasures documented in the plans should be implemented according to the alert levels declared by the entity.

Emergency Response Plans

Develop, exercise, and maintain incident and emergency response plans that provide for life safety (e.g., evacuation, shelter-in-place, bomb threat) and limit initial property damage.

Business Continuity Plans

Develop, exercise, and maintain business continuity plans that initially recover business operations to minimally acceptable levels for the New Normal period, then later resume operations to normal business operation levels.

Incident Management Plan

Develop, exercise, and maintain an incident management plan that addresses command, control, communications, and coordination with entity operational response, crisis communication (e.g., media, consumers), and government.

Training

Train and exercise teams in the activation and execution of the above plans and other response, recovery, and restoration strategies.

Local Law Enforcement Agency Days

Collaborate with local law enforcement agencies to build relationships. Foster an environment of cooperation and participate in joint exercises. Coordinate planning and preparedness activities with local and state/provincial government.

---

[56] NERC Security Guideline – Identifying Critical Assets
http://www.nerc.com/fileUploads/File/Standards/Critcal_Asset_Identification_2009Nov19.pdf

[57] Ref. NIPP, National Infrastructure Protection Plan

Key Recommendation #32 | Preventing and Responding to Physical Attacks
Consider ways to improve local coordination and cooperation with local/state/provincial law enforcement.

Replacement Equipment

Essential equipment that is difficult to obtain should be identified, acquired, and stored in secure locations. See the *Logistics and Self-sustained Operations* section of this report for additional information.

Adaptability and Continuous Improvement

Periodically perform post-exercise reviews to identify and document preparedness successes, areas for improvement, and lessons-learned. Develop an action plan for improvements, develop enhancements, and implement identified improvements.

Possible Threats

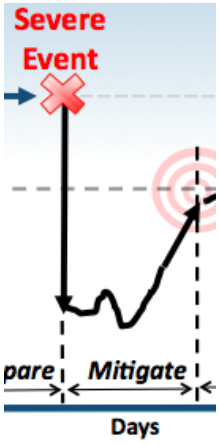
Physical attacks on the BPS may appear in several forms. Threats could come from internal (e.g., disgruntled employee, contractors) or external (e.g., disgruntled customer, terrorist) sources. The table below shows possible threats that should be considered when performing a risk assessment. The threats shown could be part of the initial attack or could be part of subsequent attacks designed to stop, slow, or divert response and recovery efforts.

Controls Overview

Controls (countermeasures, safeguards) may come in many forms. Before an appropriate control can be identified the nature of the threat must be understood as well as the vulnerability of the asset being protected. Threat and vulnerability information is identified and documented in a risk assessment. When assessing controls it is useful to classify them into 'control types'. The table below shows possible controls separated into control types. The examples shown are not limited to a physical attack scenario.

Table 7: Control Types and Examples		
Control Type	**Definition**	**Control Examples**
Prepare	Controls that prepare for threat occurrence or expected losses.	Risk assessments, impact assessments, plans (response, recovery, restoration, preparedness), backup data, alternate sites, backup equipment, awareness, training, exercises, drills, control maintenance
Prevent	Controls that prevent threat occurrence or resulting losses.	Prevention procedures, site security plans, fences, access control, passwords, safety measures, fire prevention measures, hide asset, security guards
Detect	Controls that detect threat occurrence or resulting losses.	Smoke detectors, heat detectors, motion sensors, vibration sensors, cameras, security guards
Minimize	Controls that reduce or minimize losses as the threat occurs.	Activate emergency response procedures, water sprinklers, CO2, halon, fire extinguishers, exit signs, stairwells, emergency lighting, first-aid kits, flood wall, deterrence measures, security guards, backup generators
Recover	Controls that recover resources, operations, and reputation lost as a result of threat occurrence.	Activate business recovery and restoration procedures, heal/replace injured personnel, rebuild/replace damaged equipment and facilities, restore data from backups

12.4 Recommendations for Response and Mitigation Strategies



The strategies suggested in this section pertain to actions taken immediately after the physical attack to notify appropriate response teams, assess the nature and magnitude of the attack, and review the status of BPS assets in order to make decisions on the physical security and incident management actions to be implemented.

Site Security Plans

Activate appropriate site security plans according to the alert levels (e.g., Elevated, Imminent per U.S. National Terrorism Advisory System[58]) to protect critical assets and personnel from additional attacks.

Emergency Response Plans

Activate appropriate emergency response plans (evacuation, shelter-in-place, bomb, threat, etc.) that provide for life safety and limit initial property damage.

Business Continuity Plans

Activate appropriate business continuity plans that recover time-sensitive, high priority business operations to minimally acceptable levels for the New Normal period.

Incident Management

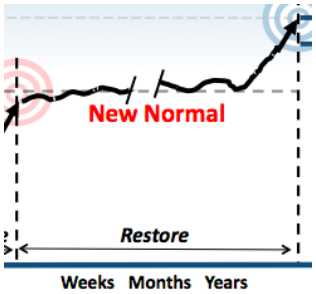
Activate an incident management system that includes the execution of crisis management plans, the activation of emergency operations centers and incident command posts, as well as the coordination of emergency response and business continuity. Also, activate crisis communication plans, and coordination with government and industry authorities.

Additional response actions are shown in the Mitigations for Physical Attack section in *Appendix 3* of this report.

[58] Ref. NTAS http://www.dhs.gov/files/publications/ntas-public-guide.shtm

12.5 Recommendations for Restoration Strategies

The strategies suggested in this section pertain to actions that should be taken after response actions are underway to notify appropriate recovery and restoration personnel, implement the incident management system, recover business operations according to prioritized lists of BPS assets, and implement physical security plans and procedures.



Site Security Plans

Continue implementation of site security plans according to the alert levels (e.g., Elevated, Imminent per U.S. National Terrorism Advisory System[59]) to protect critical assets and field personnel from additional attacks.

Business Continuity Plans

Continue implementation of business continuity plans that recover time-sensitive, high priority business operations. Activate plans to recover less time sensitive, lower priority business operations to minimally acceptable levels. Later, resume operations to normal business operation levels.

Incident Management

Operate an incident management system where crisis management teams in emergency operations centers and incident command teams in the field provide command, control and coordination of restoration activities, communication, physical security, and coordination with government and industry authorities.

Adaptability and Continuous Improvement

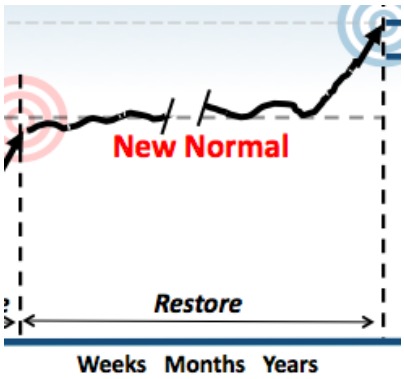
Perform after action reviews to identify and document successes, failures, and lessons-learned. Develop an action plan for improvements; follow the action plan, and implement actions to improve preparation, response, and restoration plans and procedures. Share non-proprietary after action review results with NERC, as appropriate.

Additional restoration actions are shown in the *Mitigations for Physical Attack* section in *Appendix 3* of this report.

[59] Ref. NTAS http://www.dhs.gov/files/publications/ntas-public-guide.shtm

13.0Financing Emergency Operations

During a routine emergency and recovery (e.g., storm damage), entities normally have sufficient cash and related financial mechanisms in the form of reserves, lines of credit or other financial instruments to deal with immediate needs. Consumer rates approved through the tariff approval process and various forms of industrial insurance are used to finance restoration work and the return to normal operations is possible through rate recovery. A more serious event[60] can be financially devastating.



A Severe Event will certainly have financial impacts that exceed anything that North America has experienced. The recent nuclear tragedy in Japan hints at the seriousness of the potential problem. This is a look into crippling financial problems as severe as the event itself.

The requirement for cash immediately after the event and for months during recovery through the New Normal period will be significant. Conservative estimates may place this cash requirement at ten times that of normal operations. Given this cash flow requirement, the duration of liquidity is short lived. An entity's ability to acquire and properly allocate funds will largely influence the degree to which recovery is successful, or even possible. Effective cost-tracking and audit processes will still need to be in place to demonstrate that restoration actions are financially prudent under the circumstances.

Each entity will react somewhat differently to the financial reality of a Severe Event depending on the financial structure of the entity and cash flows and lines of credit diminish. State/provincial and federal intervention will be inevitable during a Severe Event.

The goal of this section is to provide guidance and information to all entities faced with these financial challenges under the following assumptions.

- The Severe Event is regional and affects several BPS entities
- Existing banking and insurance institutions are still functioning, but are outside the area affected by the Severe Event.
- The entity's executive and financial functions are able to operate.

[60] Ref. Edison Electric Institute, *After the Disaster: Utility Restoration Cost Recovery* http://www.eei.org/ourissues/electricitydistribution/Documents/Utility_Restoration_Cost_Recovery.pdf

13.1 Getting Prepared for Emergency Financing

Some would argue there is little that can be done in advance to prepare for emergency financing that would be required through a Severe Event. Increasing consumer electricity rates through the normal tariff and regulatory approval process would be extremely difficult if not impossible. The carrying cost for large lines of credit is similarly difficult to secure and would soon become unsustainable. It is expected that the need to manage costs will place increased pressures on everything from staffing levels to warehouse inventories and reduce bench strength of needed equipment and resources.

However, much can be done to prepare to manage the financial pressures that would arise soon after a Severe Event. Entities should consider bringing together those responsible for financial matters to discuss the issue. The insurance, procurement, risk management, and financial functions share a significant part of the responsibility and may already have much of the information needed to prepare a plan. Discussions with suppliers, financial institutions, and labor unions will increase awareness of the challenges that would be faced in a Severe Event, and help identify options to address them.

Key Recommendation #33 | Emergency Financing
Consider how extreme financial challenges will be addressed in consultation with financial institutions, suppliers, and government agencies.

The following links provide references that may aid these discussions.

Public Safety Canada: http://www.publicsafety.gc.ca/prg/em/index-eng.aspx

- Resources for Emergency Management Planning
  - Emergency Management Planning Guide to support the Federal Policy for Emergency Management and the Emergency Management Act (2007)
  - All-Hazards Risk Assessment
- Emergency Preparedness
  - Canadian Emergency Management College
  - Guides for business and first responders
  - Joint Emergency Preparedness Program
- Joint Emergency Preparedness Program (JEPP) http://www.publicsafety.gc.ca/prg/em/jepp/index-eng.aspx

Canadian Centre for Emergency Preparedness: http://www.ccep.ca/

U.S. Federal Emergency Management Agency (FEMA): http://www.fema.gov/privatesector/preparedness/

- References, news and information

- Robert T. Stafford Relief and Emergency Assistance Act
  http://www.fema.gov/pdf/about/stafford_act.pdf

U.S. Department of Energy: http://www.oe.energy.gov/our_organization/iser.htm and http://energy.gov/oe/office-electricity-delivery-and-energy-reliability

University of Florida: http://disaster.ifas.ufl.edu/PDFS/CHAP03/D03-07.PDF

- Outlines the role of U.S. government agencies in a disaster
  - Describes the difference between a Declaration of an Emergency and a Declaration of a Major Disaster
  - Outlines the types of assistance that a state governor may request
  - Describes the role of FEMA if engaged

New York University, International Center for Enterprise Preparedness:
http://www.nyu.edu/intercep/businesscase/index.html

- Provides links to research papers on the financial impacts of emergency preparedness:
  - Corporate balance sheet, impact on assets and liabilities
  - Profit and loss, impact on revenue and expenses

U.S. Emergency Management Assistance Compact: http://www.emacweb.org/

- State-to-state mutual aid system

Public Entity Risk Institute:
https://www.riskinstitute.org/peri/index.php?option=com_bookmarks&task=detail&id=588

Appendix 1: Task Force Scope

Purpose

This document defines the scope, objectives, organization, deliverables, and overall approach for the SIRTF.

The purpose of the SIRTF is to provide guidance and options to enhance the resilience of the bulk power system to withstand and recover from severe-impact scenarios, specifically:

- Coordinated physical attack
- Coordinated cyber attack
- Geomagnetic disturbance

Background

The NERC and DOE *High Impact, Low Frequency Risk to the North American Bulk Power System* report described a number of severe-impact scenarios and their potential impact on the reliability of the bulk power system. Subsequent to this report, the Electricity Sub-sector Coordinating Council's (ESCC) *Critical Infrastructure Strategic Roadmap* identified a number of strategic initiatives to mitigate these impacts. Several of these initiatives (i.e., items E, F, H, L, and P) identify the need to assess the current capability of the bulk power system to withstand these severe-impact scenarios and to enhance restoration plans and procedures.

NERC staff and the leadership of the NERC technical committees (Planning, Operating, and Critical Infrastructure Protection Committees) have developed a Coordinated Action Plan to address the initiatives identified in the Strategic Roadmap. This scope document elaborates on the Coordinated Action Plan to establish and provide direction to the SIRTF.

Scope

The SIRTF will provide guidance and options to enhance the resilience of the bulk power system to withstand and recover from three severe-impact events as described in the Coordinated Action Plan.

- Coordinated physical attack
- Coordinated cyber attack
- Geomagnetic disturbance

The SIRTF will propose approaches, practices, and plans to reduce the impact of these events through effective emergency operations and timely restoration of the BPS.

The SIRTF will consider what aspects of emergency operation and restoration will be particularly challenged through these severe-impact events, and consider options to enhance the resilience of the BPS. Preferred solutions will be flexible and based on heuristic methods applicable under a wide variety of circumstances, as opposed to fixed procedures. The SIRTF will recommend solutions for broad implementation across the electricity sector, and propose drills or exercises to reinforce this capability. These solutions could be in the form of industry

guidelines that describe practices that may be used by individual entities according to local circumstances.

The SIRTF may consider establishing sub-teams to address the planning /operational and tools/systems issues that may be unique for each of the three severe-impact scenarios.

Assumptions and Limitations

The three scenarios described in the Coordinated Action Plan are intended to describe extreme conditions that would make operation and restoration much more challenging than would normally be considered by electricity entities through their usual planning and preparedness activities. While solutions that offer material improvements are preferred, it is recognized that more modest enhancements that are readily implemented are also valued.

It is expected that any solutions proposed to enhance existing capabilities would be broadly applicable to other severe-impact scenarios, and certainly applicable to smaller scale events.

Goals and Objectives

Goals	Objectives
Review current situation and capabilities	1. Recognizing that priorities will vary depending on local circumstances, consider priorities to restore critical power system loads along restoration paths (e.g., communications, nuclear units), and priority customer loads (e.g. oil refineries, military bases, hospitals, water treatment plants, public telecommunications). Consider how these priorities might differ through a range of outage durations (e.g., days, weeks, and longer). 2. Consider operating capabilities and voice and data communications tools and energy management systems, with a focus on identifying minimum essential functional needs for reliable operation. 3. Consider restoration plan elements such as blackstart, islanded operation, synchronization, rotational load shedding. 4. Assess operational staffing levels and unique safety considerations under these scenarios.
Perform needs assessment	5. Identify elements of current operating and restoration capability that would be particularly challenged under these severe-impact scenarios.
Develop alternative solutions	6. Propose a range of alternative solutions and options to enhance current operating and restoration capability, including estimated costs and effort to develop and maintain this capability. Identify the residual risks that may be associated with each of these solutions.

Coordinate Solutions	7. Coordinate with NERC staff to integrate these solutions with the NERC Crisis Response Plan with special emphasis on areas where local, state, and Federal resources may be required to support such efforts.
Recommend solutions	8. Recommend specific practices or programs for use by NERC or individual entities. Create scalable drill templates that registered entities could be used to train personnel and enhance current restoration and operating protocols through existing drill and exercise programs.

Task Force Reporting Structure and Coordination with Other Related Initiatives

The Task Force will:

- Report to the Operating Committee. Seek Planning Committee endorsement prior to Operating Committee approvals.
- Provide periodic status reports to the Operating Committee and Electricity Sub-Sector Coordinating Council
- Coordinate closely with the Critical Infrastructure Protection Committee that will provide expertise to address Coordinated Action Plan Item F – Protect Critical Equipment
- Coordinate closely with the Spare Equipment Database Task Force
- Coordinate with other NERC and industry resources that may be able to contribute, such as the, Reliability Coordinator Working Group, North American Transmission Forum
- Leverage from other recent initiatives in this area (e.g., the National Infrastructure Advisory Council's Stress Test exercise)

Resources Required

The Task Force requires expertise in the following areas:

- Experience with the real time operation of the bulk power system, including the communications and energy management systems and tools typically used by reliability coordinators, transmission operators, and generator operators.
- In-depth experience with bulk power system restoration plans and procedures, including designing and conducting restoration drills and exercises.
- Familiarity with developing situation assessment reports used to inform senior management or government.

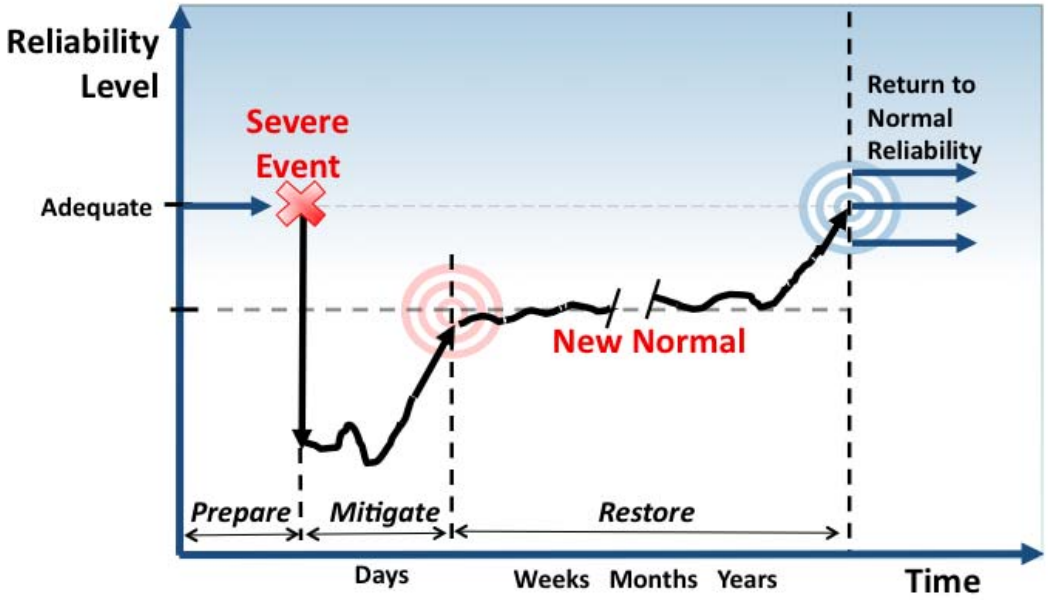
It is anticipated that 2 conference calls per month, and a total of 4 face-to-face meetings will be required, in addition to the time required to contribute to this effort. This work is expected to begin in December 2010 and end by December 2011.

References

Name	Link
DOE/NERC HILF "*High Impact, Low Frequency Risk to the North American Bulk Power System*" report	http://www.nerc.com/files/HILF.pdf
Critical Infrastructure Strategic Roadmap	http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf
NERC Technical Committees' Report – *Critical Infrastructure Strategic Initiatives Coordinated Action Plan*	http://www.nerc.com/docs/ciscap/Critical_Infrastructure_Strategic_Initiatives_Coordinated_Action_Plan_BOT_Apprd_11-2010.pdf

Appendix 2: Mitigations for Monitoring the BPS

This Appendix builds on the recommendations in the *Monitoring the BPS* section of this report and highlights the different actions that may be taken, prior to, during, and after a Severe Event.



MONITORING Resilience Considerations		Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
		Robustness The ability to absorb shocks and keep operating	**Resourcefulness** The ability to manage a disruption as it unfolds	**Rapid Recovery** The ability to get back to Normal as quickly as possible
Generator Output				
1.	**Fixed Schedules**		Develop and Modify as required MW and MVAR output schedules of available units	As the situation becomes more stable the variability and flexibility of the schedules will be broader.
2.	**Block Loading**		Using a block loading schedule reduce the need for communications	

	MONITORING Resilience	Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
3.	**Operating Ranges**	Review with GOP's particular operating ranges that if a directive is outside of the GOP needs to confirm the directive with its own call	Within the response and New Normal adjust and communicate new ranges as required by the new system.	
	LIMITS			
4.	**Hard Copies of Limits**	On a periodic basis print out BPS limits and maintain copies in primary and back-up control centers	During a cyber event routinely sample displayed limits with printed limits	
5.	**Referencing Guides**	Consider developing distribution factor spreadsheets that act as quick references to better understand the effects of possible actions and contingencies	After an event and particularly in islanded operations and when PSSE tools are not available these tables may need to be recalculated.	
6.	**Standing Orders and Temperature Sets**	Consider a standing order which states following an event to ease communications particular triggers will be used to go from one temperature set to another.	Based on communications capabilities may want to go to a seasonal set of ratings – making it easier to ensure all parties are always using the same set of ratings	
7.	**Conservative Limits**	Define a conservative set of limits which could be implemented after a large event (could be as simple as a percent back-off)		As the system becomes more stable and operators will need to continually reassess if these limits are too conservative for the community's needs.

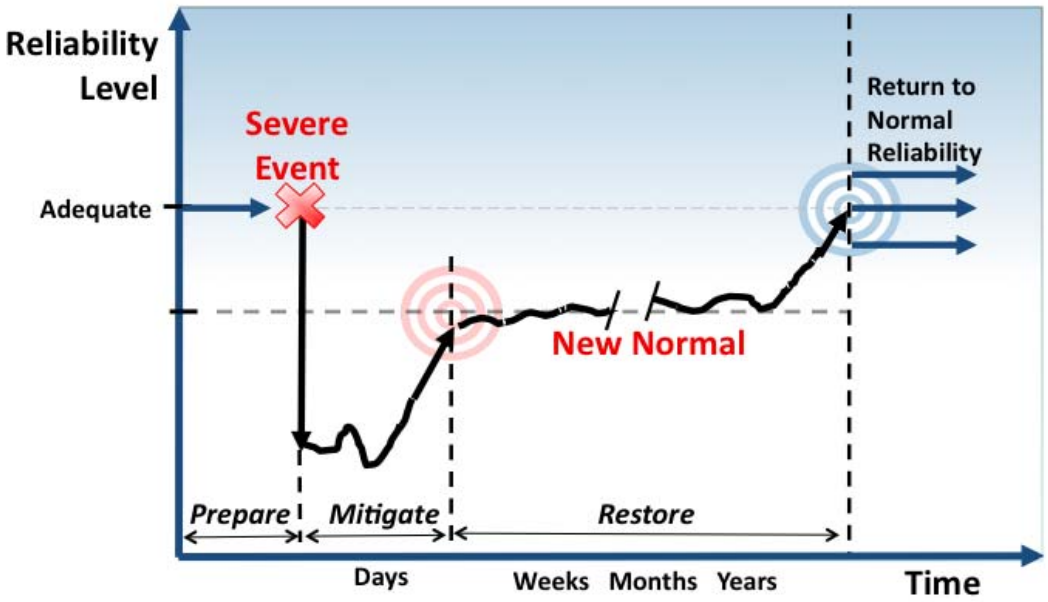
	MONITORING Resilience	Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
8.	**Revisit Design Assumptions**		A continual re-assessment and implementation cycle of adjusting operating limits to the realities of the current topology and not the original design assumptions. As islands are interconnected these differing operating assumptions will need to be communicated to the joining entities.	
9.	**Operate to the Most Conservative Limit**	Have discussions with operators and engineers when operating to the most conservative reading may not be in the best interest of reliability.	Continually work with other critical infrastructures to determine whether operating to a less conservative rating is in the greater good of keeping multiple critical infrastructures available.	
	MONITORED FLOWS ON BPS FACILITIES			
10.	**Prepare for Large Amounts of Data Loss**	1. Conduct studies of the minimum amount of data needed. 2. Assess how greater aggregation might reduce some of the reliance on this data. 3. Develop practices for operating without any SE/SA capability for months. 4. Develop a list of the most critical data points.	Based upon the list of most critical data points prioritize which stations will be staffed with the communications available at that time.	Train additional personnel to assist in the 24/7 needs to report data.
11.	**Loss of Primary & Back-Up EMS**	Understand which portions of your system are independently monitored by neighbors.	Consider how off-line study packages and applications (operator training simulator) could be leveraged.	

	MONITORING Resilience	Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
12.	**Phasors**	Continue to develop the operational capabilities of the PMUs. As these capabilities and systems are developed, consider keeping their data feeds and platforms independent of EMS capabilities.	1. Redefine the operating parameters of the PMU applications as procedures/decision points may be based upon pre-crisis topology. 2. Continue to evolve operating procedures around operating experience.	
Loss of Both Control Centers				
13.	**Back Up Location Considerations**	Consider both sites are sufficiently distant so as not to be affected by single events which would render a control center unusable.	Backup sites should have considered the issues of personnel feeding, hygiene, security, backup power, and transportation needs.	Recovery from an event would be facilitated if a common event would not render both primary and backup control centers unusable.
14.	**Agreements with Others**	Consider if other entities might be able to share control centers and telemetry.	Contracts should be in place for security, fuel delivery, sewage, and food supplies. Following an event prioritize contacting these suppliers and arrange deliveries.	Contract revisions will be necessary during the period of reconstruction. In some cases assistance from neighboring utilities may be necessary.
15.	**Diversely routed telemetry**	Design and plan telecommunications paths such that both sites are not exposed to single points of failure.	Multiple telemetry routes should be available from all sources, especially the RC, as operation from the alternate could extend for a significant time.	Diversely routed telemetry would more readily enable operation for an extended duration after the event is over while the previously disabled or destroyed control centers are rebuilt.

MONITORING Resilience		Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
16.	**Use of EOC or OTS as possible tertiary sites**	Anticipate possible use of emergency operations centers (EOC) or operator training simulators (OTS) as backup control centers and design them with the appropriate telemetry.	Dispatcher familiarity with the EOC and OTS from drills & exercises should facilitate and help recognize the need for various facilities for long term operation.	An EOC or OTS are more likely to have the necessary facilities to operate for an extended duration during the New Normal.

Appendix 3: Mitigations for Physical Attacks

This Appendix builds on the recommendations in the *Preventing and Responding to Physical Attacks* section of this report and highlights the different actions that may be taken, prior to, during, and after a Severe Event.



		Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
		Robustness The ability to absorb shocks and keep operating	**Resourcefulness** The ability to manage a disruption as it unfolds	**Rapid Recovery** The ability to get back to Normal as quickly as possible
Communicate				
1.	**ES-ISAC**	Develop and maintain procedures to report suspicious activity to ES-ISAC.	Report incidents to the ES-ISAC and monitor ES-ISAC alerts or advisories.	Continue updating ES-ISAC as appropriate.
2.	**Local, State Authorities**	Develop, maintain, and exercise communication plans with local, state authorities.	Communicate with local, state authorities during response.	Continue communicating with local, state authorities during recovery.

		Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
3.	**NERC**	Share prevention and preparedness phase lessons-learned.	Share mitigation phase lessons-learned.	Share recovery phase lessons-learned.
4.	**Alternative Communications**	Develop, maintain alternative communication methods.	Execute alternative communication methods, as required.	Continue execution of alternative communication methods, as required.
5.	**Crisis Communication Plan**	Develop, maintain, and exercise Crisis Communication Plan.	Activate Crisis Communication Plan.	Continue execution of Crisis Communication Plan.
6.	**Public Reporting**	Develop, maintain, and exercise communication with the media to share information with the public in order to increase observations in the field (the public reporting strange happenings/sightings).	Use communication with the media to share information with the public in order to increase observations in the field (the public reporting unusual events).	Continue using communication with the media to share information with the public in order to increase observations in the field (the public reporting unusual events).
7.	**Reliability Coordinator (RC)**	Utilities develop, maintain, and exercise communication plans with relevant RC.	Execute communication plans with relevant RC. Rapidly share lessons-learned with other entities.	Continue execution of communication plans with relevant RC, as required.
Monitoring & Situational Awareness				
8.	**Vulnerability Assessments**	Perform risk/vulnerability assessments and review at least annually.	Implement lessons-learned from other entities into security or operations plans.	Review vulnerability assessments for ability to estimate the actual threat, vulnerabilities, and impacts experienced.

		Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
9.	**Controls**	Install, maintain, test, and monitor controls. For example: • fences, gates, walls, berms • access control systems/methods • make assets less visible • security guards and patrols • smoke/heat detectors, motion sensors, cameras, etc.	Increase and adapt monitoring of implemented controls. Consider random changes to security plans to reduce predictable actions.	Continue increased monitoring of implemented controls.
10.	**Law Enforcement/ Military**	Develop and maintain coordination.	Increase coordination and adapt to current situation.	Continue increased coordination.
11.	**SCADA Monitoring**	Review expansion of use of SCADA to monitor and report inappropriate activity.	Use SCADA to monitor and report inappropriate activity. Work with IT to monitor SCADA for possible disruption.	Continue use of SCADA to monitor and report inappropriate activity.
12.	**Situational Awareness by the Public**	Develop and implement programs to support situational awareness of facilities by the public.	Remind public of situational awareness and where to submit reports, provide for disruptions in routine communications.	Continue reminding public of situational awareness and where to submit reports. Share intelligence and lessons-learned with communities.
13.	**Monitoring Plans**	Train, exercise, maintain plans and teams to perform monitoring.	Activate appropriate monitoring plans and teams.	Continue execution of appropriate monitoring plans and teams.
14.	**Intelligence**	Implement thorough intelligence gathering and reporting. (e.g., through ES-ISAC, RCs)	Increase intelligence gathering and reporting.	Continue increased intelligence gathering and reporting.

		Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
15.	**Security Threat Levels**	Develop, maintain, and exercise a system of Security Threat Levels which is compatible with the National Terrorism Advisory System. Have procedures to be prepared to move to a different level based on perceived threats; and report the current level to authorities as appropriate.	When credible, specific, and impending terrorist threats to electric infrastructure becomes evident, change the Security Threat Level to IMMINENT and activate appropriate response and crisis management plans. When a credible terrorist threat becomes evident, change the Security Threat Level to ELEVATED, and monitor threats as appropriate. Report the current level to authorities as appropriate.	Continue monitoring threats and the current situation. Change the Security Threat Level, as appropriate. Report the current level to authorities as appropriate.
Command & Control, Operate				
16.	**Incident Response Plans**	Develop, maintain, and exercise Incident Response Plans.	Activate appropriate Incident Response Plans to protect facilities and personnel.	Continue execution of appropriate Incident Response Plans to protect facilities and personnel.
17.	**Crisis Management Plan**	Develop, maintain, and exercise crisis management plans and crisis communication plans.	Activate crisis management plans and crisis communication plans.	Continue execution of crisis management plans and crisis communication plans.

		Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
18.	**Crisis, Operations, Incident Teams**	Train, maintain, and exercise crisis management, crisis communication, emergency operations, and incident response teams. Align and train teams in the National Incident Management System (NIMS) and the Incident Command System (ICS).	Activate appropriate crisis management, crisis communication, emergency operations, and incident response teams.	Continue activation of appropriate crisis management, crisis communication, emergency operations, and incident response teams.
19.	**Protect Critical Infrastructure**	Develop, maintain, and exercise response plans with law enforcement to have them protect critical infrastructure when initiated by the operator owner.	Activate appropriate response plans to have law enforcement protect critical infrastructure. Inform law enforcement as priorities regarding critical assets change.	Continue execution of response plans to have law enforcement protect critical infrastructure.
20.	**Protect Field Personnel**	Develop, maintain, and exercise plans for the protection of field personnel after an attack. Protection strategies could include: • Protection provided by local and state law enforcement and the National Guard • Protection provided by a contractor with armed personnel • Protection provided by field personnel themselves (armed?)	Activate appropriate plans for protection of field personnel after an attack.	Continue to implement and update plans for protection of field personnel during recovery and restoration.

		Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
21.	**Mobile Control Center**	Develop, maintain, and exercise a mobile control center for use by security and crisis/incident management teams. Could be used as a security control center, emergency operations center, and/or incident command post.	Deploy and protect mobile control center where needed.	Continue deployment and protection of mobile control center where needed.

Appendix 4: Resilience Discussion Worksheet

Introduction

The SIRTF report provides a framework to help entity management and subject matter experts review their plans and preparations and consider a Severe Event that is much greater in terms of impact and duration than current plans envision.

This Appendix provides a worksheet that could be used by business continuity and emergency preparedness personnel, system operators, and management to prompt creative thinking about the possible challenges they might face through a Severe Event. The worksheet builds upon the ideas and recommendations found within the SIRTF report and poses questions that may prompt new resilience ideas, mitigation responses, and other courses of action. The worksheet is not intended to require that a new and detailed response plan be developed for a Severe Event; instead, personnel are encouraged to challenge themselves to consider substantially worse scenarios to help ensure they and their organization will be in a better position to respond.

As such, the SIRTF recommends that entities use this worksheet to facilitate discussions involving personnel at all levels, including executive leadership, to enhance the entity's overall crisis preparedness and response capability. This worksheet is not exhaustive, and entities are encouraged to build further on the concepts and ideas offered.

Decision Making

1. If many members of the organization's senior leadership team were unavailable because of travel restrictions, communications failures, or other post event challenges how would decision making authority be established?

Possible Challenges Requiring Decisions	If this decision should fall to a few people – who?	If this decision should be made up of a team, who should comprise this team?
Priority Load Designation		
Changes to Operating Limits		
Procurement Decisions		
External Communications (Messaging)		
Reassignment of Personnel		

2. What might be the triggers for re-evaluating certain decisions or the assumptions or both underlying these types of decisions?

Decisions which may require periodic reevaluation:	What are the Triggers for reevaluation? (i.e., Time Based, Changes in Operating State, External Requirements)
Priority Load Designation	
Changes to Operating Limits	
Procurement Decisions	
External Communications (Messaging)	
Reassignment of Personnel	

Business Continuity and Restoration Plans

3. How would your current **Business Continuity and Restoration plans** be disrupted if your organization had little to no communications? Which of these disruptions most troubles the following personnel?

	What is most troublesome?	What makes this concern so critical?	What are possible mitigations?
System Operator			
Field Personnel			
Procurement Team			
Executive Leadership			

4. Another way of examining the critical communications interdependence is to list each of your communication capabilities and prioritize the importance of these capabilities to your business continuity or restoration plans or both. Walk through how your organization would adapt its plans if you were to lose these capabilities, from the most critical to the least.

Communications Capability	Possible Mitigations
Phone Lines	
EMS/GMS Signals	
Cell Phones	
Satellite Phones	
Internet	
Radio	
Hand-Carried Messages	
Other	

5. What resource limitations create time constraints for portions of your business continuity or restoration plans or both?

Possible Examples of Time Restraints	Possible Mitigations
Nuclear Power BPS-supplied Power (six hours)	
Nuclear Power Back-up Diesels (7 days)	
Control Room Back-Up power (3 days?)	
Data Aggregation Points	
Communications Repeating Stations	
Sub-station Breakers	
Other	

6. For energy-related limitations how could the investment of renewable generation (e.g., wind, solar) extend these time restrictions? What would be other financial justifications beyond greater system resilience for making such an investment?

Operations

1. If only limited data points are available, how would studies be performed?
2. If the Balancing Authority and Transmission Operator no longer have visibility of their systems:
   a. Who would become the new system operator and how would this be established?
   b. How would the extent (boundaries) of any resulting islands be determined?
   c. How would you implement the system restoration plan?
   d. What independent actions would equipment operators take? How are these actions known, coordinated and trained?
   e. What system information (e.g., generator characteristics, load characteristics, limits) would be shared with the new system operator and how?
   f. What communication methods and protocols would be used to keep the Reliability Coordinators, Balancing Authorities and Transmission Operators updated on local system conditions and restoration progress?
   g. How will variable generation resources be managed during restoration and New Normal timeframes?

3. How would the following system parameters be managed immediately following the Severe Event and during the New Normal?

Challenge	Possible Mitigations to determine MW, MVAR output and resulting frequency
BA has No Communications with Market/Generation Operation (MOC/GOP) Centers	
BA has no communications with units but can communicate with MOC/GOP	

4. How would your organization consider its operating assumptions and limits? At what point is it appropriate to revisit, and possibly revise, protection settings on relay settings, UFLS and other protection schemes?
5. What rules of thumb should be provided to system operators for operating in the New Normal?
6. Assuming a total blackout with no outside assistance and no expectation to interconnect in the near term:
   a. What units are most essential to the restoration plans?
   b. How many days of fuel do generating stations typically have on hand? Are there contracts regarding fuel on hand for important sources of generation, especially those needed for blackstart? How does such a number of MWh define the load to be served, the rotating blackout schedule, and the amount of reserves carried?
   c. What concerns do you have about units that do not have station power and lighting needs served?
      - How many days before a unit might be damaged? What ways could resources be committed to protect such units?
      - What if the Severe Event prevents BPS supply to the nuclear units and is expected to last beyond the technical specification requirement to have seven days fuel on hand for the back-up diesels?

7. How will new load patterns be established? What are the critical and priority loads that need to be served? Do these change based on different event outcomes and timeframes? If so why?
8. What loads are not essential and do not need to supplied over the long term?
9. Will Operating reserve requirements be met by load shedding or by reserving generation capacity? Why? What are factors that may change this assessment?
10. In the event that there are no market mechanisms and tools available to dispatch generation, what alternative mechanisms can be used?

Logistics and Interdependencies

11. What infrastructures are your critical facilities most dependent on?

Critical Infrastructure	What is most troublesome?	What makes this concern so critical?	What are possible mitigations?
Communications			
Energy			
Water & Dams			
Information Technology			
Other			

12. Of these infrastructures, which have critical facilities (those facilities essential to bulk power system operation) within your zone (and maybe in your neighbors' zones)?

Facility & Contact Info	Critical Infrastructure	Location	Impacts & Time to Impact
1.			
2.			
3.			
4.			
5.			

13. What are the energy needs of these critical facilities?
14. How would a total blackout restoration plan address these facilities' energy needs?

15. What hard-stop time limits can these facilities endure without power before there is damage or second or third order impacts to other infrastructures and/or the bilk power system. How are these time limits factored into your own plans?

People

1. For each of the major functions within your organization related to the reliability of the bulk power system, which are most critical?

Critical Organizational Function	Point or Primary Person/Department	Secondary Person/Department	Tertiary Person/Department
1. Operations			
2. Communications - Hardware			
3. Communications - Messaging			
4. Emergency Liaison			
5.			

2. Based on the assessment of critical functions, how would personnel within these functions be directed?
   a. When should they report to work following a Severe Event?
   b. Do they all report at once, and then a schedule is created, or is there a standing set of instructions?
   c. How would transportation challenges be addressed under the following scenarios?
      - State/provincial or local travel restrictions
      - Gas pumps are not working, and personnel's private vehicles have insufficient fuel to get to work.
      - Consumers wanting to know when their power will be restored routinely interrupt and delay utility personnel engaged in restoration efforts.
   d. How would you address personnel concerns about their families?
      - In the first couple of days following a Severe Event
      - 10 days after a Severe Event
      - One – six months after a Severe Event
   e. How would you house, feed, and care for these personnel?

Financing

1. How can each corporate function best prepare and respond to a Severe Event?

Critical Organizational Function	What can you do to prepare for a Severe Event? What resources are available?	How will you function during the new normal?	How will your area facilitate the return to normal BPS reliability levels?
1. Insurance			
2. Procurement			
3. Risk Management			
4. Finance			
5. Collections			
6. Labor Relations			
7.			

Appendix 5: Severe Event Response Checklist

This Appendix provides a checklist of questions that may be used by entities through a Severe Event to periodically assess the situation and decide new courses of action as system conditions and circumstances evolve through the New Normal period.

Date: _____ **Time**: _____

System Topology

What are the current island boundaries?

1. Are these being operated in an unstudied state?
2. Depending on the electrical configuration of the island(s), which operating security limits may no longer be appropriate?
    a. Why are these limits inappropriate?
    b. Conversely, why are other limits still appropriate?
    c. Of those limits which require additional study
        - Which limits should be prioritized?
        - What decision criteria are used to determine this priority?
3. Is the system configuration suitable for restoration?
    a. How do we know this?
    b. Have breakers been opened along the restoration path?
    c. Who is working on this confirmation?
4. Will the current protection schemes/SPS/UFLS/UFLS settings impede or assist with the current system's operations?
    a. What protection changes are practical at this time?
    b. How are the decision criteria for "practical" defined?
        - If changes are merited, with the limits in the current workforce, communications, and other resources how will the priority of these changes be determined?
        - How will these changes be coordinated as connections are made with other islands?

Generation

1. What generation is damaged and what is fully capable and available?
    a. What is keeping the unavailable units in this state?
    b. Are the fixes that are required under the organization's control, or what assistance is needed?
2. Which units in the island are blackstart capable and available?
3. What is the fuel availability for each unit within the island?
4. Do any of these units have regulatory restrictions that are limiting their capacity?
    a. How can these restrictions be addressed?
    b. Who is the decision maker?

Transmission Lines and Substations

1. What is the status of key substations?
    a. How critical is the key substation in the current system configuration?
    b. What is the status of key elements within the substation (transformers, busses, breakers, reactive elements)?
    c. Can the substation be reconfigured to use good equipment and bypass bad equipment
2. What equipment can be cannibalized to restore key substations?
    a. Can redundancy (per standard requirements) be minimized/eliminated to provide a larger restoration footprint such as moving redundant transformers to key substations or creating radial configurations on breaker and a half configurations to free up additional breakers for key substations)?
    b. In what timeframe can the cannibalization occur?
    c. What is the availability of specialized equipment (railcars, cranes etc.)?
3. What is the status of key transmission lines?
    a. Breaker status, operable, etc.
    b. If line is out of service, has a line inspection been completed and any potential faults resolved?
    c. Can lines be re-configured to by-pass damaged substations?

Key Equipment

1. What is the status of key equipment?
    a. Damaged equipment (repairable or not)
    b. Replacement equipment
    c. Cannibalization

Load

1. What are the critical loads needed to operate the bulk power system?
   a. Within an island?
   b. Beyond the island, that may drive restoration priorities
2. What are the priority loads needed to support public health and safety?
   a. Within an island?
   b. Beyond the island that may drive restoration priorities
   c. What are the decision criteria for ranking these priority loads?
   d. Who are the decision makers for the current priorities?
      - Are we able to communicate with these decision makers?
      - If there are no communications with this decision maker, who will make the decision?
      - How do we share and coordinate these priority load decisions?

Communications

1. Who am I able to talk to in my role as a _____?
2. Who must I talk with in my role as a _____?
3. What are the means to mitigate these communication gaps?

People

1. Are key personnel available to perform their role?
   a. How can they best be used?
   b. What key personnel gaps need to be filled, and from where?
2. What extraordinary safety concerns need to be addressed?
   a. How will personnel be kept informed of any security-related risks?
   b. How will field changes be documented so field operating and system operators are kept informed?

Monitoring

1. What is the organization's situational awareness of the current island?
2. Why can this situational awareness be trusted?
3. Are there other entities that might help provide additional situational awareness?
4. Based upon current topology – what are the most essential data points
    a. Which of these essential data points is missing?
    b. What are the possible mitigations to acquire these essential data points?
5. What other mechanisms can be used to gain some visibility of the system, no matter how limited or rudimentary?

Financing

1. What funding is available to support continued operations in the short term? How will operations be funded in the long term?
2. What funding can be shifted away from low and medium priority projects given the new normal configuration?
3. How will employees be paid if electronic transactions are not available?
4. How will customers pay bills if electronic transactions are not available?
5. How will your revenue stream be impacted? Will customers be willing to pay given the expected decrease in reliability? Will customers be able to pay given the expected economic impacts?
6. How widespread is the event? How much state or provincial aid will be available? Is federal assistance available?

Appendix 6: NERC SIRTF Roster

Chairman	Tom Bowe Executive Director of Compliance	PJM Interconnection, L.L.C. 955 Jefferson Avenue Valley Forge Corporate Center Norristown, Pennsylvania 19403-2497	(610) 666-4776 (610) 666-4287 Fx bowet@pjm.com
Vice Chairman	Paul B. Johnson, P.E. Managing Director - Transmission Operations	American Electric Power 8400 Smith's Mill Road New Albany, Ohio 43054	(614) 413-2200 (614) 413-2652 Fx pbjohnson@aep.com
	Sandy Bacik Principal Consultant	EnerNex Corp 6008 Tundra Lane Fuquay Varina, North Carolina 27526	(865) 696-4470 sandy.bacik@enernex.com
	Emanuel Bernabeu Engineer III	Dominion Technical Solutions, Inc. 2400 Grayland Avenue Richmond, Virginia 23220	(804) 432-8780 emanuel.e.bernabeu@dom.com
	Stuart Brindley President	S. J. Brindley Consulting Inc. 4177 Vermont Cr. Burlington, Ontario Canada L7M 4A6	(905) 464-4211 stuart.brindley@gmail.com
	Julie Couillard Director	CTC Cable Corporation 2026 McGaw Avenue Irvine, California 92614	(949) 428-8500 (949) 428-8515 Fx jcouillard@ctccable.com
	Sean Eagleton Section Manager	Con Edison 4 Irving Place New York, New York 10003	(212) 460-2898 (212) 529-4828 Fx eagletons@coned.com
	Ian S Grant Senior Manager, NERC Planning Coordinator	Tennessee Valley Authority 1101 Market Street MR-5G-C Chattanooga, Tennessee 37402-2801	(423) 751-8721 isgrant@tva.gov
	David Grubbs Director of Regulatory Affairs and Compliance	City of Garland 217 N. 5th St. Garland, Texas 75040	(214) 802-9045 (972) 205-2822 Fx dgrubbs@garlandpower-light.org
	Jose Guzman Junior Policy Analyst - Government Services Division	Schweitzer Engineering Laboratories, Inc.	(703) 647-6241 (703) 647-6259 Fx jose_guzman@selgs.com
	Frederick P. Heller Engineer/Analyst	U.S. Department of Defense 18372 Frontage Road Suite 318 Dahlgren, Virginia 22448	(540) 653-2929 (540) 284-0143 Fx frederick.heller@navy.mil

Bradley Hofferkamp Senior Analyst	PJM Interconnection, L.L.C. 955 Jefferson Avenue Norristown, Pennsylvania 19403	(610) 666-4688 (610) 666-4287 Fx hoffeb@pjm.com
Jennifer Hubbs Infrastructure Policy Analyst	Homeland Security Infrastructure and Reliability Division Public Utility Commission of Texas	(512) 936-7233 Jennifer.Hubbs@puc.state.tx.us
Nicholas Ingman Manager, Operational Excellence	Independent Electricity System Operator 655 Bay Street Suite 410 Toronto, Ontario M5G 2K4	(905) 855-6108 (905) 855-6129 Fx nicholas.ingman@ieso.ca
Wallace Jensen Director Electrical Engineering	Emprimus 1660 South Highway 100 Minneapolis, Minnesota 55416	(651) 341-2090 (952) 545-2216 Fx wjensen@emprimus.com
Michael D. Johnson Lead Engineer	Florida Power & Light Co. 700 Universe Boulevard TLD/JB Juno Beach, Florida 33408	(561) 691-7548 (561) 694-4161 Fx mike_johnson@fpl.com
Miles Keogh Director of Grants and Research	National Association of Regulatory Utility Commissioners 1101 Vermont Avenue N.W. Suite 200 Washington, D.C. 20005	(202) 898-2217
Matthew Light Infrastructure Systems Analyst	Department of Energy 1000 Independence Ave., SW Washington, D.C. 20585	(202) 316-5115 matthew.light@hq.doe.gov
Toni Lineberger NERc CIP Program Manager	U.S. Bureau of Reclamation P.O. Box 25007 (84-45000) Denver, Colorado 80225-0007	(303) 445-2912 (303) 445-6573 Fx tlineberger@usbr.gov
Matthew Luallen Consultant	Sph3r3, LLC 19873 Oakwood Drive Suite A Bloomington, Illinois 61705	(312) 375-4715 m@sph3r3.com
Michael Lynch Chief Security Officer, Corporate Security and Investigations	Detroit Edison Company One Energy Plaza Detroit, Michigan 48335	(313) 235-7733 (313) 965-3853 Fx lynchm@dteenergy.com
Patricia E Metro Manager, Transmission and Reliability Standards	National Rural Electric Cooperative Association 4301 Wilson Blvd. Mail Code EP11-253 Arlington, Virginia 22203	(703) 907-5817 (703) 907-5517 Fx patti.metro@nreca.coop

Philip Mihlmester Senior Vice President	ICF International 9300 Lee Highway Fairfax, Virginia 22031	(703) 934-3560 (703) 934-3968 Fx pmihlmester@icfi.com
John G. Mosier, Jr. Assistant Vice President of System Operations	Northeast Power Coordinating Council, Inc. 1040 Avenue of the Americas, 10th Floor New York, New York 10018-3703	(212) 840-1070 (212) 302-2782 Fx jmosier@npcc.org
Gale Nordling President/CEO/Consultant	Emprimus 1660 S. Hwy 100, Sutie 130 Minneapolis, Minnesota 55416	952-545-2051 952-545-2216 Fx gnordling@emprimus.com
Steven Norris Director Transmission Operations	APS 502 S. 2nd Avenue M.S. 2259 Phoenix, Arizona 85003	(602) 250-1644 (602) 250-1155 Fx Steven.Norris@aps.com
Thomas V. Pruitt Consulting Engineer	Duke Energy Carolina 526 South Church Street Charlotte, North Carolina 28202-1006	(704) 382-4676 (704) 382-3230 Fx tom.pruitt@duke-energy.com
Michael L. Puscas Manager Critical Infrastructure Protection	Northeast Utilities 107 Selden Street Berlin, Connecticut 06037	(860) 665-2615 (860) 665-6001 Fx puscaml@nu.com
Ken Shortt Director, Compliance	PacifiCorp 70 N. 200 East American Fork, Utah 84003	(801) 756-1237 (801) 756-1318 Fx ken.shortt@pacificorp.com
Michael T. Tallent Manager Cyber Security Solutions	Tennessee Valley Authority 1101 N. Market Street Chattanooga, Tennessee 37402	(423) 751-3413 mttallent@tva.gov
Terry Volkmann Consultant	Volkmann Consulting, Inc. 14240 55th Street, NE St. Michael, Minnesota 55376	(612) 419-0672 terrylvolkmann@gmail.com
Luke Weber Project Manager Operational Support	We Energies W237 N1500 Busse Road Waukesha, Wisconsin 53188	(262) 544-7393 (262) 544-7099 Fx luke.weber@ we-energies.com
Charles A. White Vice President SCE&G Electric Transmission	South Carolina Electric & Gas Co. 220 Operations Way Cayce, South Carolina 29033	(803) 933-7242 (803) 933-7242 Fx cwhite@scana.com
Bruce Wollenberg Professor	University of Minnesota Keller Hall 200 Union Street S.E. Minneapolis, Minnesota 55455	(612) 625-4583 (612) 625-4583 Fx wollenbe@umn.edu

	Bradley C. Young	LG&E and KU Services Company TBD Lexington, Kentucky 40507	(859) 367-5703 (502) 217-2249 Fx Brad.Young@lge-ku.com
Observer	David Batz Manager, Cyber & Infrastructure Security	Edison Electric Institute 701 Pennsylvania Ave NW Washington, D.C. 20004	(202) 508-5064 (202) 508-5445 Fx dbatz@eei.org
Observer	Steven Belle Power Supply Reliability Specialist	South Carolina Electric & Gas Co. 601 Old Taylor Road Cayce, South Carolina 29033	(803) 217-1978 steven.belle@scana.com
Observer	Larry Camm Policy Analyst	Schweitzer Engineering Laboratories, Inc. 500 Montgomery Street Suite 400 Alexandria, Virginia 22314	(703) 647-6221 (703) 647-6259 Fx larry_camm@selgs.com
Observer	David A. Casey Security Lead	Consumers Energy 1935 West Parnall Road Jackson, Mississippi 49201	(517) 788-0956 dacasey@cmsenergy.com
Observer	Carl J. Eng Manager, System Operations-Engineering	Dominion Virginia Power Innsbrook Technical Center - 2 North 5000 Dominion Boulevard Glen Allen, Virginia 23060-3308	(804) 273-3305 (804) 273-2405 Fx carl.eng@dom.com
Observer	Thomas R. Flowers President	Flowers Control Center Solutions 9338 Clark Road Todd Mission, Texas 77363	(936) 894-3649 flowersccs@att.net
Observer	Jeffrey Fuller Corporate Security/CIPManager	Dayton Power & Light Co. 1065 Woodman Drive Dayton, Ohio 45432	(937) 259-7144 jeffrey.fuller@dplinc.com
Observer	John Helme Technical Analyst	Utility Services, Inc. 25 Crossroads Suite 201 Waterbury, Vermont 05676	(802) 552-4022 (802) 214-8632 Fx john.helme@utilitysvcs.com
Observer	Charles John Hookham Vice President	HDR Engineering, Inc. 5405 Data Court Ann Arbor, Michigan 48108	(734) 332-6496 (734) 761-9881 Fx chuck.hookham@hdrinc.com
Observer	Anthony Jankowski Manager, Electric System Operations	We Energies W237 N1500 Busse Road Waukesha, Wisconsin 53188	(262) 544-7117 (262) 544-7099 Fx tony.jankowski@we-energies.com
Observer	Jack Kerr Consulting Engineer	Dominion Virginia Power 5000 Dominion Blvd. IN-2N Glen Allen, Virginia 23060	(804) 273-3393 (804) 273-2405 Fx jack.kerr@dom.com

Observer	Paul D. Kure Senior Consultant, Resources	ReliabilityFirst Corporation 320 Springside Drive Suite 300 Akron, Ohio 44333	(330) 247-3057 (330) 456-3648 Fx paul.kure@rfirst.org
Observer	Michael Mertz FERC Regulatory Compliance	PNM Resources Alvarado Square Albuquerque , New Mexico 87158	(505) 241-0676 michael.mertz@pnmresources.com
Observer	Melvin Miller IASO/Wireless Analyst	Nulink Wireless, LLC 15483 Murray Hill Detroit, Michigan 48227-1945	(313) 350-9129 (313) 838-6669 Fx techservices@nulinkwireless.com
Observer	Thomas Pearce Senior Utility Specialist	Public Utilities Commission of Ohio 180 East Broad Street Columbus, Ohio 43215	(614) 466-1846 (614) 752-8353 Fx thomas.pearce@puc.state.oh.us
Observer	Alan J Rivaldo Cyber Security Analyst	Public Utility Commission of Texas 1701 N. Congress Ave. Austin, Texas 78711-3326	(512) 936-7162 (512) 936-7328 Fx alan.rivaldo@puc.state.tx.us
Observer	Michael Sanders Manager, Energy Management Systems Engineering	Southern Company 600 North 18th Street 7S8220 P.O. Box 2641 Brimingham, Alabama 35291	(205) 257-3388 msander@southernco.com
Observer	Dan R Schoenecker Vice President of Operations	Midwest Reliability Organization 2774 Cleveland Avenue North Roseville, Minnesota 55113	(651) 855-1753 (651) 632-8572 Fx dr.schoenecker@midwestreliability.org
Observer	Jason Shaver Reliability Standards and Performance Manager	American Transmission Company, LLC W234 N2000 Ridgeway Pkwy. Ct. Waukesha, Wisconsin 53187-0047	(262) 506-6885 jshaver@atcllc.com
Observer	Robert V. Snow, P.E. Senior Electrical Engineer, Office of Electric Reliability	Federal Energy Regulatory Commission 888 First Street, NE Room 91-13 Washington, D.C. 20426	(202) 502-6716 robert.snow@ferc.gov
Observer	Ed Tymofichuk Vice President, Transmission	Manitoba Hydro 820 Taylor Avenue P.O. Box 7950 Winnipeg, Manitoba R3C 0J1	(204) 360-4280 (204) 360-6149 Fx tetymofichuk@hydro.mb.ca
Observer	Scott Watts Senior Compliance Specialist	Duke Energy Carolina 526 South Church Street Mail Code: EC02A Charlotte, North Carolina 28202	(704) 382-2260 (704) 382-6938 Fx scott.watts@duke-energy.com

Observer	Bruce D. Wertz Senior NERC Compliance Consultant	Public Service Electric and Gas Co. P.O. Box 54865 Hurst, Texas 76054	(817) 498-0310 (801) 383-9772 Fx brucewertz@sbcglobal.net
Observer	Daniel J. Zaragoza Director - Electric Distribution Operations	San Diego Gas & Electric P.O. Box 129831 San Diego, California 92112-9831	(619) 725-5171 (619) 725-5196 Fx dzaragoz@semprautilities.com
NERC Staff	Brian M. Harrell Manager of CIP Standards, Training, and Awareness	North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, D.C. 20005-3801	(202) 393-3998 (202) 393-3955 Fx brian.harrell@nerc.net
NERC Staff	Jordan Erwin	North American Electric reliability Corporation 3353 Peachtree Rd, NE Suite 600 Atlanta, GA	Jordan.Erwin@nerc.net
NERC Staff	Larry J Kezele Manager of Operations	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx larry.kezele@nerc.net

Appendix 7: NERC SIRTF Report Drafting Team

Chairman	Tom Bowe Executive Director of Compliance	PJM Interconnection, L.L.C. 955 Jefferson Avenue Valley Forge Corporate Center Norristown, Pennsylvania 19403-2497	(610) 666-4776 (610) 666-4287 Fx bowet@pjm.com
Vice Chairman	Paul B. Johnson, P.E. Managing Director - Transmission Operations	American Electric Power 8400 Smith's Mill Road New Albany, Ohio 43054	(614) 413-2200 (614) 413-2652 Fx pbjohnson@aep.com
	Sandy Bacik Principal Consultant	EnerNex Corp 6008 Tundra Lane Fuquay Varina, North Carolina 27526	(865) 696-4470 sandy.bacik@enernex.com
	Emanuel Bernabeu Engineer III	Dominion Technical Solutions, Inc. 2400 Grayland Avenue Richmond, Virginia 23220	(804) 432-8780 emanuel.e.bernabeu@dom.com
	Stuart Brindley President	S. J. Brindley Consulting Inc. 4177 Vermont Cr. Burlington, Ontario Canada L7M 4A6	(905) 464-4211 stuart.brindley@gmail.com
	Ian S Grant Senior Manager, NERC Planning Coordinator	Tennessee Valley Authority 1101 Market Street MR-5G-C Chattanooga, Tennessee 37402-2801	(423) 751-8721 isgrant@tva.gov
	David Grubbs Director of Regulatory Affairs and Compliance	City of Garland 217 N. 5th St. Garland, Texas 75040	(214) 802-9045 (972) 205-2822 Fx dgrubbs@garlandpower-light.org
	Bradley Hofferkamp Senior Analyst	PJM Interconnection, L.L.C. 955 Jefferson Avenue Norristown, Pennsylvania 19403	(610) 666-4688 (610) 666-4287 Fx hoffeb@pjm.com
	Jennifer Hubbs Infrastructure Policy Analyst	Homeland Security Infrastructure and Reliability Division Public Utility Commission of Texas	(512) 936-7233 Jennifer.Hubbs@puc.state.tx.us

Nicholas Ingman Manager, Operational Excellence	Independent Electricity System Operator 655 Bay Street Suite 410 Toronto, Ontario M5G 2K4	(905) 855-6108 (905) 855-6129 Fx nicholas.ingman@ieso.ca
Miles Keogh Director of Grants and Research	National Association of Regulatory Utility Commissioners 1101 Vermont Avenue N.W. Suite 200 Washington, D.C. 20005	(202) 898-2217
Michael Lynch Chief Security Officer, Corporate Security and Investigations	Detroit Edison Company One Energy Plaza Detroit, Michigan 48335	(313) 235-7733 (313) 965-3853 Fx lynchm@dteenergy.com
Sean Eagleton Section Manager	Con Edison 4Irving Place New York, New York 10003	((212) 460-2898 (212) 529-4828 Fx eagletons@coned.com
Michael D. Johnson Lead Engineer	Florida Power & Light Co. 700 Universe Boulevard TLD/JB Juno Beach, Florida 33408	(561) 691-7548 (561) 694-4161 Fx Mike_johnson@fpl.com
Patricia E Metro Manager, Transmission and Reliability Standards	National Rural Electric Cooperative Association 4301 Wilson Blvd. Mail Code EP11-253 Arlington, Virginia 22203	(703) 907-5817 (703) 907-5517 Fx patti.metro@nreca.coop
Philip Mihlmester Senior Vice President	ICF International 9300 Lee Highway Fairfax, Virginia 22031	(703) 934-3560 (703) 934-3968 Fx pmihlmester@icfi.com
Steven Norris Director Transmission Operations	APS 502 S. 2nd Avenue M.S. 2259 Phoenix, Arizona 85003	(602) 250-1644 (602) 250-1155 Fx Steven.Norris@aps.com
Thomas V. Pruitt Consulting Engineer	Duke Energy Carolina 526 South Church Street Charlotte, North Carolina 28202-1006	(704) 382-4676 (704) 382-3230 Fx tom.pruitt@duke-energy.com

	Michael L. Puscas Manager Critical Infrastructure Protection	Northeast Utilities 107 Selden Street Berlin, Connecticut 06037	(860) 665-2615 (860) 665-6001 Fx puscaml@nu.com
	Ken Shortt Director, Compliance	PacifiCorp 70 N. 200 East American Fork, Utah 84003	(801) 756-1237 (801) 756-1318 Fx ken.shortt@pacificorp.com
	Luke Weber Project Manager Operational Support	We Energies W237 N1500 Busse Road Waukesha, Wisconsin 53188	(262) 544-7393 (262) 544-7099 Fx luke.weber@we-energies.com
	Bradley C. Young	LG&E and KU Services Company TBD Lexington, Kentucky 40507	(859) 367-5703 (502) 217-2249 Fx Brad.Young@lge-ku.com
	Jack Kerr Consulting Engineer	Dominion Virginia Power 5000 Dominion Blvd. IN-2N Glen Allen, Virginia 23060	(804) 273-3393 (804) 273-2405 Fx jack.kerr@dom.com
NERC Staff	Jordan Erwin	North American Electric reliability Corporation 3353 Peachtree Rd, NE Suite 600 Atlanta, GA	Jordan.Erwin@nerc.net
NERC Staff	Larry J Kezele Manager of Operations	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx larry.kezele@nerc.net