NERC Critical Infrastructure Protection Committee (CIPC)
Report to Southwest Power Pool Regional Entity Trustees
Submitted by Robert McClanahan, Chair, SPP Critical Infrastructure Protection WG
October 18, 2010

- The Electric Sub-Sector Coordinating Council (ESCC) continues work on its *Critical Infrastructure Strategic Roadmap* (attached below). This roadmap provides a framework via which to identify and address risks that could significantly impact the supply of electricity to the nation. The document will be used to communicate industry critical infrastructure protection (CIP) efforts to the Energy Sector's Government Coordinating Council (GCC).
- The leadership of the NERC Technical Committees (Operating Committee, Planning Committee and Critical Infrastructure Protection Committee) is developing a report entitled *Critical Infrastructure Strategic Initiatives Coordinated Action Plan*. This plan addresses a number of issues and risks raised in the joint NERC/DOE *High-Impact, Low-Frequency Report* issued earlier this year. The Technical Committees will be establishing working groups and task forces to complete the actions defined in the plan.
- NERC has issued alerts on both the Stuxnet virus and the Aurora vulnerability. Both alerts provide information about the vulnerability, as well as requiring Registered Entities to respond to a survey. These surveys ask questions related to specific actions taken to address the vulnerability and mitigation plans for situations where specific recommendations cannot be acted upon immediately. The response for the Stuxnet advisory was due to NERC on October 15th, while the Aurora response is due by December 13th.
- The proposed changes to the CIP Standards continue to keep the industry energized. The CIP Standards Drafting Team continues to meet every other week, either face-to-face or via teleconference. Philip Huff of Arkansas Electric Cooperative Corporation is Vice Chair of the SDT. Joe Doetzel of KCP&L is also a member of the group.
- The NERC CIPC held its quarterly meeting in Denver, CO on September 15-16, 2010. The agenda for this meeting can be found at http://www.nerc.com/docs/cip/CIPC_Agenda_15Sep10.pdf.
  - Mark Weather ford, NERC's new Chief Security Officer, shared his vision for the Critical Infrastructure Protection Program at NERC. He will be stressing "reliability through security".
  - Stuart Brindley, NERC Contractor and former CIPC Chair, presented the *Critical Infrastructure Strategic Roadmap* and the *Critical Infrastructure Strategic Initiatives Coordinated Action Plan*. CIPC approved a resolution to allow CIPC leadership to work with leadership from OC and PC to refine the *Coordinated Action Plan* for presentation to the NERC Board in November.
  - CIPC elected two Executive Committee members to replace members who had recently retired or resigned.
- CIPC continues work to revisit and update its Security Guidelines for the industry. These guidelines are not guidelines in support of standards, but are intended to provide general guidance and best practices on security-related matters. The following groups are working on this endeavor:
  - Business Continuity Guideline Task Force – will be updating the *Continuity of Business Practices* guideline.

- Control System Security Working Group (CSSWG) – will be reviewing nine existing guidelines that address cyber security, with the intent of consolidating these into a concise cyber security reference document for the industry. In addition, the CSSWG will be taking on some additional work from the *Coordinated Action Plan*.
- Protecting Sensitive Information Guideline Task Force – will be developing a new guideline to assist the industry in securing sensitive information.
- Substation Guideline Task Force – will be updating the *Physical Security – Substations* guideline. This Task Force is chaired by Allen Klassen of Westar Energy. John Breckenridge of KCP&L is also participating on this task force.

➢ The next CIPC meeting is scheduled for December 8-9, 2010 in Tampa, FL.
- A classified briefing for CIPC is Members and Alternates is being planned in conjunction with this meeting.
- There will be an election at this meeting to fill the Vice Chair position left vacant by my resignation from that post at the September meeting.

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Critical Infrastructure Strategic Roadmap

Electricity Sub-Sector Coordinating Council (ESCC)

DRAFT

to ensure the reliability of the bulk power system

October 2010

116-390 Village Blvd., Princeton, NJ 08540
609.452.8060 | 609.452.9550 fax
www.nerc.com

Introduction

North America's electric power grids are not immune to severe disruptions that could threaten the health, safety, security, or economic well-being of its citizens. The North American Electric Reliability Corporation (NERC) and the electricity industry are committed to protect the electricity infrastructure and enhance its resilience in an effort to manage risks, whether natural or man-made.

This Critical Infrastructure Strategic Roadmap (Roadmap), prepared by NERC's Electricity Sub-Sector Coordinating Council (ESCC), provides the framework to identify those risks that have the potential to seriously disrupt the supply of electricity to customers, and promotes the actions necessary to enhance reliability and resilience. Particular attention is paid to severe-impact risks with the potential to impact large portions of the grid, or disrupt service for an extended period of time. Some of these risks have a low probability of occurring, or have not ever occurred. The most challenging are some of those related to physical and cyber security that are relatively new to the sub-sector, are not completely understood even by experts in the field, and continue to evolve.

Fortunately, managing complex risks is not new to the electricity industry. This Roadmap builds on century-long experience and takes an integrated approach that builds on the electricity industry's capabilities to plan and operate North America's electricity system—one of the most reliable in the world.

Table of Contents

Introduction 2
Executive Summary 4
Vision and Goals 5
Building on Existing Capabilities 5
Vision 6
Goals 6
Information Sharing and Communication 6
Physical and Cyber Security 6
Coordination and Planning 6
Public and Regulatory Confidence 6
The Risk Landscape 7
The Electricity Sub-Sector's Risk Priorities 9
Scenario 1: Physical Attack on Significant Electricity System Equipment 9
Scenario 2: Coordinated Cyber Attack 9
Scenario 3: Geomagnetic Disturbance 9
Multi-Element Approach 9
Planning Elements 9
Prevention Elements 10
Mitigation Elements 11
Recovery Elements 11
Multi-Year Roadmap 12
Mobilizing the Electricity Sub-Sector 12
Key Strategic Initiatives 13
Expected Results 14
Monitor Progress 15
Appendix – Bibliography 16
Appendix – Strategic Initiatives Plan 17
Scenario 1: Physical Attack on Significant Bulk Power System Equipment 17
Scenario 2: Coordinated Cyber Attack 17
Scenario 3: Geomagnetic Disturbance 17

Executive Summary

The role of NERC's Electricity Sub-Sector Coordinating Council is to "foster and facilitate the coordination of sector-wide policy-related activities and initiatives to improve the reliability and resilience of the electricity sector, including physical and cyber security infrastructure."

To help carry out that role, the ESCC has developed this Critical Infrastructure Strategic Roadmap (Roadmap) to recommend to NERC's Board of Trustees that NERC's Technical Committees and the industry place renewed emphasis on certain severe-impact risks to electricity system reliability.

In particular, the ESCC has identified three risks that merit increased attention by NERC and the electricity sub-sector. Each of these has the potential to severely impact large portions of the bulk power system, or disrupt electricity service for an extended period of time.

- Coordinated physical attack on significant electricity system equipment
- Coordinated cyber attack on control systems needed to manage reliability
- Severe geomagnetic disturbance

The ESCC acknowledges that significant cost and effort will be required to properly understand these risks and develop realistic and effective solutions, and has therefore prioritized initiatives that would deliver the greatest benefit to reliability as soon as possible. The ESCC encourages NERC's Technical Committees to join forces to develop work plans to assess the risks in more detail, consider alternative approaches, and recommend solutions for industry implementation.

The ESCC is committed to enhance our collaboration with government on these matters and, in coordination with the Board of Trustees, will monitor progress of the Technical Committees and provide additional guidance as necessary.

Vision and Goals

Critical infrastructures are facing increasing and unknown risks. The U.S. and Canadian governments have established programs to work collaboratively with all critical infrastructure sectors to address risks that could have widespread regional, national, or international consequences. The electricity sub-sector does not stand alone.

In the spirit of these national initiatives, this Roadmap reflects the perspective of the electricity sub-sector as envisioned by the charter of the Electricity Sub-Sector Coordinating Council. It is intended to reflect the interests of all electricity stakeholders, beyond that of NERC in its role as the electricity reliability organization. The focus of these efforts is to address severe-impact risks on the bulk power system. This includes risks affecting distribution systems that could, in aggregate, severely impact the bulk power system. While local distribution is also important, the ESCC feels that these risks are best dealt with at the state/provincial or local level with individual entities.

The bibliography appended to this Roadmap provides a number of references to government and electricity industry publications that together provide the broader context for this Roadmap.

Building on Existing Capabilities

It is not possible to completely protect the electricity system. While the bulk power system is designed with redundancy to manage planned equipment outages, and the resilience to withstand certain un-planned disruptions, it is not on a scale that would be sufficient to face the severe-impact risks described in this Roadmap. To attempt to do so would have enormous societal, environmental, and economic impacts and take years, if not decades, to study, design, seek approvals, and build. Customers would face cost increases on a magnitude never before seen.

This Roadmap provides an approach that builds on the ability of NERC and the industry to reliably plan and operate the bulk power system; a system that is designed and operated to absorb failures, avoid cascading events that would cause large-scale disruptions, and recover rapidly. The industry has arrangements in place to provide mutual support when local capabilities are exceeded—a continent-wide capability activated, for example, in the wake of major storms and hurricanes. Forward-looking reliability and adequacy assessments provide an industry-wide projection of how the electricity system is evolving and will affect future reliability. Comprehensive reviews of system disturbances and abnormal events are published in an effort to prevent similar events from occurring in the future. And to support the continuous millisecond operation of the bulk power system by individual entities, NERC facilitates communication among reliability coordinators, notifies the industry when significant events occur, and coordinates with industry and government officials. Working together, the electricity sub-sector can build on this capability to address severe-impact risks.

Vision

In 2007, the NERC Board of Trustees endorsed the U.S. Department of Energy's Energy Sector-Specific Plan that provides the framework for collaboration between government and the energy sector to mitigate risk by reducing vulnerabilities, deterring threats, minimizing adverse consequences, and enhancing recovery. This Roadmap supports the Sector-Specific Plan's vision and goals and demonstrates the electricity sub-sector's commitment to support this public-private partnership.

Vision Statement
The Electricity Sub-Sector envisions a robust, resilient electricity infrastructure in which continuity of business and services are maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between sub-sector entities and government.

Goals

Information Sharing and Communication

Goal 1: Enhance situational awareness within the electricity sub-sector and with government through robust, timely, reliable, and secure information exchange.

Physical and Cyber Security

Goal 2: Use sound risk management principles to enhance physical and cyber measures that improve preparedness, security, and resilience.

Coordination and Planning

Goal 3: Conduct comprehensive emergency, disaster, and business continuity planning. Conduct training and large-scale exercises involving electricity industry and government entities to enhance reliability and coordinated emergency response.

Goal 4: Clearly define critical infrastructure protection roles and responsibilities.

Goal 5: Enhance understanding of key interdependencies and collaborate with other critical infrastructure sectors to address them, and incorporate that knowledge in planning and operations.

Public and Regulatory Confidence

Goal 6: Strengthen public and government regulatory agency confidence in the sub-sector's ability to manage risk and implement effective security, reliability and recovery efforts.

The Risk Landscape

The challenges to adequately protect the electricity system are many. The electricity infrastructure is spread geographically across the continent, in densely populated urban areas as well as lightly populated rural areas. Generating stations, substations, and the transmission and distribution lines that connect them are a familiar and accessible part of our surroundings. While it is not possible to protect everything with absolute assurance, this Roadmap guides the electricity sub-sector toward solutions that address these risks in a responsible, realistic, and effective manner.

NERC supports an all-hazards, all-threats approach to risk management consistent with industry practices commonly used across the sub-sector. These threats and hazards can be grouped into three categories; natural, human-caused, and technological. The electricity sub-sector consistently demonstrates the ability to successfully manage many of these risks through effective business continuity planning and reliable operations, even during emergency situations.

However, certain severe-impact risks are more challenging to fully understand and address for a number of reasons, including.

- Little information is available regarding the specific nature of the risk, making it difficult to decide which preventive or mitigating actions are necessary or appropriate.
- The likelihood of occurrence is extremely low or may never have occurred, and is therefore unknown.
- The costs and resources required to comprehensively address the risk may be enormous.
- The events being prepared for may never occur.
- Risks related to national security are considered to be the responsibility of government.

As a result, there is limited agreement across the sub-sector regarding the extent to which these more severe-impact risks need to be addressed, let alone how they should be addressed. The following table provides the ESCC's assessment of the risks facing the electricity sub-sector, and highlights those requiring urgent additional attention.

- "**Plans typically in place**" means that entities generally have the ability to manage the risk depending on local needs, and have demonstrated this ability through drills, exercises, or real events.
- "**Requires further assessment**" means that limited information is available to entities regarding the relative urgency of the risk, or the risk may be considered to be beyond the responsibility of individual entities.
- "**Requires additional action**" means that while individual entities may have the ability to manage certain aspects of the risk, there is a need to consider the risk more fully, take the necessary actions to improve this ability, and ensure coordination with other entities, for example through drills and exercises.

Table 1: Risk Landscape

Risk Area	Opportunities for Improvement
Naturally Occurring Hazards	
• Geological (e.g. earthquake)	Plans typically in place
• Meteorological	
o Severe storm	Plans typically in place
o Extreme water flows (drought, flood)	Plans typically in place
o Extreme temperature	Plans typically in place
o Geomagnetic disturbance (GMD), solar magnetic disturbance (SMD)	Requires additional action
• Biological disease (e.g. pandemic)	Plans typically in place
Human-Caused (Unintentional) Hazards	
• Hazardous material spill or release	Plans typically in place
• Explosion, fire	Plans typically in place
• Interdependency (e.g. fuel shortage, telecommunications service disruption)	Plans typically in place
• Human operational error	Plans typically in place
Human-caused (Intentional) Hazards:	
• Local criminal activity or sabotage	Plans typically in place
• Civil disturbance, riot	Plans typically in place
• Strike or labor dispute	Plans typically in place
• Terrorism	Requires additional action
• Physical attack	Requires additional action
• Electro-magnetic pulse (EMP)	Requires further assessment
• Cyber security breach, coordinated cyber attack	Requires additional action
• Equipment failure	Plans typically in place
• Local information/control system failure	Plans typically in place
• Local telecommunications system failure	Plans typically in place

The Electricity Sub-Sector's Risk Priorities

The ESCC recommends to the NERC Board of Trustees that the electricity sub-sector place renewed emphasis on managing the severe-impact risks highlighted in Table 1: Risk Landscape that require additional action.

These risks were examined in the High Impact Low Frequency Risk Workshop sponsored by NERC and the U.S. Department of Energy in November 2009. While each of these risks appear to be unique, they can be grouped into a few discrete scenarios that will facilitate developing solutions that can be more readily applied under a variety of circumstances. Solutions that also serve to enhance reliability under normal circumstances would be highly desirable while those with limited application under very narrow circumstances would be less desirable.

The ESCC recognizes that the electricity sub-sector is highly diverse, and not all solutions will be applicable to all entities. As with all risk management decisions, entities will need to balance expected outcomes against costs, recognizing that all costs are ultimately borne by the customer.

Scenario 1: Physical Attack on Significant Electricity System Equipment
A coordinated physical attack on key nodes of the bulk power system critically disables difficult to replace equipment in multiple generating stations or substations and could have a significant affect on the remainder of the system. A prolonged period of time is required to fully restore the bulk power system to normal operation.

Scenario 2: Coordinated Cyber Attack
A coordinated disruption disables or impairs the integrity of multiple control systems, or intruders take operating control of portions of the bulk power system such that generation or transmission equipment is damaged or mis-operated.

Scenario 3: Geomagnetic Disturbance
A severe geomagnetic disturbance (GMD) damages difficult to replace generating station and substation equipment, and causes a cascading affect on the remainder of the system. A prolonged period of time is required to fully restore the bulk power system to normal operation.

Multi-Element Approach

The ESCC recommends that electricity sector entities consider this full spectrum of risk management elements to address these severe-impact risks; planning, prevention, mitigation, and recovery.

Planning Elements

Clarify Roles and Authorities	Establish clear responsibilities and authorities for planning and responding to an emergency or crisis, across the sub-sector, with other sectors, and with government.

Assess Risks	Establish robust situational awareness across the electricity sub-sector through timely, reliable, and secure information exchange. Assess available intelligence from government regarding threats and provide actionable information to sub-sector entities to improve protection and preparedness.
Conduct Technical Studies	Use sound risk management principles to conduct technical studies, evaluate risks and potential impacts, and identify possible improvements.
Prioritize Assets	Prioritize assets most important to reliability and identify actions that improve protection of these assets. Priorities should be developed in consultation with other stakeholders to consider the potential impacts on customers, other critical infrastructures, and government and national security infrastructure.
Identify Interdependencies	Understand key interdependencies with other critical infrastructures and collaborate with other sectors to address them, and incorporate that knowledge in planning and operations.
Evaluate and Test	Develop exercises and testing programs to probe vulnerabilities and identify opportunities to improve protection measures and evaluate preparedness. Involve neighboring electricity sector entities, government agencies, and other critical infrastructure sectors.
Develop and Promote Guidelines	Develop and promote guidelines to inform sub-sector entities and prompt protection and recovery solutions.
Communicate	Strengthen public confidence in the electricity sub-sector's ability to manage risk by communicating how the sub-sector is proactively addressing threats and vulnerabilities and prepared to respond to high impact, low frequency events. Enhance bidirectional industry-government sharing of security threat and vulnerability information.
Funding Needs	Consider options for funding and cost recovery for critical infrastructure protection, particularly as traditional cost-justification approaches may be difficult to apply, or when objectives exceed assuring the reliability of the electricity system itself.

Prevention Elements

Detect and Prevent	Develop appropriate active security policy enforcement, monitoring controls, and protections to deter or prevent severe-impact risks. Employ defense-in-depth strategies. Work with infrastructure vendors and suppliers to enhance identification of vulnerabilities, protections and recoverability.

Mitigation Elements

Improve Resilience	Identify options to strengthen the inherent redundancy, flexibility and capacity of the bulk power system to reduce the likelihood of unmitigated impacts on the system. Limit the adverse impact and preserve the reliability of the remainder of the system. Enhance, to the extent practical, the survivability of national security and critical infrastructures.

Recovery Elements

Readiness	Develop and implement plans to exercise and maintain a state of readiness to respond to events that might adversely affect reliability.
Respond	Enhance entity and coordinated bulk power system-wide response to a significant event, including the capability to communicate quickly and effectively with all affected stakeholders.
Restore the System	Ensure plans are in place, exercised and ready to be implemented to restore the system to reliable operation in the wake of a severe event. Verify and enhance plans to provide human and material resources with particular attention on equipment that may not be readily available. Enhance pre-established plans to recognize priorities during restoration with respect to customers, other critical infrastructures, and government and national security infrastructure

.

Multi-Year Roadmap

For many years, NERC and its Technical Committees have filled an important collaborative role by providing an open and inclusive forum to identify issues of concern and take action to help the industry address them. These Technical Committees are well suited to specifically address severe-impact risks. In particular, the Operating Committee, Planning Committee, and Critical Infrastructure Protection Committee have the mandate, leadership and expertise to jointly address the initiatives identified by this Roadmap. To do so, they utilize the active contribution of experts from across the electricity industry, including vendors and suppliers, and government partners.

Mobilizing the Electricity Sub-Sector

The ESCC recommends to the NERC Board of Trustees that NERC and its Technical Committees develop work plans to address these risk scenarios by more fully assessing the nature of the risks, considering alternative approaches, and recommending solutions for industry implementation. Given the breadth and complexity of these scenarios, the ESCC recommends that the Technical Committees join forces to make optimal use of their capabilities. The ESCC recognizes that significant resources will be required to effectively address some of these initiatives, and encourages the Committees to invite assistance from experts outside the Committees, and prioritize this work accordingly, including assessing the relative urgency of their other work currently underway.

Recognizing that it is not reasonable or effective for the industry-supported Technical Committees to address all these activities at the same time, the ESCC proposes a staged approach. Initiatives that will more directly enhance reliability and resilience are considered "High Priority" and should be addressed immediately. Others that yield benefits in the longer term are considered "Important". Progress will be monitored and reviewed periodically by the ESCC to provide further recommendations to the NERC Board of Trustees and guidance to the sub-sector.

Table 2: "High Priority" and "Important" Characteristics

Relative Importance	Characteristics
High Priority	• Risk has low or higher likelihood, yet high consequence • Requires immediate action to reduce the risk • Progress achievable within available resources • Action is largely within the control of sub-sector entities • Action enhances reliability during normal operations
Important	• Risk has unknown likelihood, yet high consequence • Requires action to identify options and resources required to reduce the risk

Relative Importance	Characteristics
	• Action may not be achievable within existing resources • Requires substantial coordination with other critical infrastructure sectors or government • Action has limited opportunity to enhance reliability during normal operations

The following table illustrates the relative priority to address each of the strategic goals against the three severe-impact scenarios.

Table 3: Strategic Priorities

Goal	Scenario 1: Coordinated Physical Attack	Scenario 2: Organized Cyber Attack	Scenario 3: Geomagnetic Disturbance	Enhances reliability under less severe scenarios?
1. Enhance situational assessment, coordination, and information exchange	High Priority	High Priority	High Priority	Yes
2. Enhance protective measures	Important	High Priority	Important	Limited
3. Enhance contingency planning, training, and exercises	High Priority	High Priority	Important	Yes
4. Clarify critical infrastructure protection roles with government	High Priority	High Priority	High Priority	Limited
5. Address key interdependencies with other sectors	Important	Important	Important	Yes
6. Strengthen public confidence	High Priority	High Priority	Important	Limited

Key Strategic Initiatives

To achieve these priorities, the ESCC has identified a number of key strategic initiatives that will provide NERC and the Technical Committees with a common focus to address the three severe-impact scenarios. Individually, each of these actionable initiatives provides direction to the Technical Committees regarding the actions they need to undertake. Collectively, the results of their efforts will significantly contribute to meeting the vision and goals of this Roadmap.

The “Appendix – Strategic Initiatives Plan” identifies each initiative, its relative priority consistent with the Table 3 – Strategic Priorities, and recommended timelines. The timelines

should be considered as preliminary estimates, and will require review by the Technical Committees as the scope and necessary resources are more fully understood. The ESCC is prepared to coordinate closely with the leadership of the Technical Committees to ensure a common understanding of expected results, and the appropriate commitment of resources. With this in mind, the column in the Appendix – Strategic Initiatives Plan headed "Substantial Progress" means that resources are engaged, an agreed work plan has been established, and alternative solutions to address the initiative have been drafted.

Expected Results

The results needed to address each initiative will vary according to the scope and nature of the respective initiative. Some of the initiatives are closely bounded, and a final report could provide new guidance to the sub-sector, provide solutions for entity implementation according to local needs, or identify the need to develop or revise a NERC reliability standard. Other initiatives may require a more complete analysis of the problem, and propose next steps such as greater involvement of those outside the electricity sub-sector, or substantially more specialized resources. It is anticipated that all initiatives would offer solutions at an early stage – the "low hanging fruit".

Monitor Progress

The ESCC considers the need to quickly demonstrate progress that addresses severe-impact risks to the electricity sub-sector to be a top priority for NERC and its stakeholders. Through their conference calls and in-person meetings, the ESCC will monitor progress and provide additional guidance as necessary. The ESCC appreciates that these initiatives are critical, and will require a concerted effort by the sub-sector to address them in a timely manner. To be successful, it is crucial to establish and maintain close coordination between the ESCC, NERC's Board of Trustees, and the Technical Committees. The ESCC invites the leadership of the Technical Committees to collaborate with the ESCC to develop the appropriate coordination mechanisms.

The ESCC will monitor progress on each of the strategic initiatives according to three key milestones, and NERC will keep stakeholders advised of progress.

1. **Scope and Resources**
   - Determine assumptions and limitations
   - Identify and recruit industry resources
   - Develop project plan and timelines

2. **Comprehensive Assessment**
   - Define specific objectives
   - Identify options and alternatives with pros and cons
   - Propose results and timelines

3. **Results**
   - Final report, with action items and next steps
   - Develop new or enhance existing industry guidance
   - Propose new or revised standards, where necessary and appropriate

Appendix – Bibliography

The following references provide additional context and information related to the scope and role of the Electricity Sub-Sector Coordinating Council.

1. Electricity Sub-Sector Coordinating Council (ESCC) Charter http://www.nerc.com/docs/escc/ESCC_Charter_BOT_approved_20100512.pdf
2. DHS National Infrastructure Protection Plan (NIPP) http://www.dhs.gov/files/programs/editorial_0827.shtm
3. Government of Canada's National Strategy and Action Plan for Critical Infrastructure http://www.publicsafety.gc.ca/prg/em/ci/index-eng.aspx
4. President Obama's 2009 Cyberspace Policy Review http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
5. Energy Sector Specific Plan 2007 http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-redacted.pdf
6. Roadmap to Secure Control Systems in the Energy Sector, http://www.oe.energy.gov/DocumentsandMedia/roadmap.pdf
7. NERC's Reliability Concepts paper describing the fundamentals of electricity reliability http://www.nerc.com/files/concepts_v1.0.2.pdf
8. DOE/NERC HILF "High Impact, Low Frequency Risk to the North American Bulk Power System" report http://www.nerc.com/files/HILF.pdf
9. Emergency management and business continuity standards Canadian Standards Association CSA Z1600-8 http://www.csa.ca/cm/ca/en/standards/products/public-and-community-safety/emergency-management and National Fire Protection Association NFPA 1600 http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=1600
10. U.S. National Infrastructure Advisory Council (NIAC) "Risk Management Approaches to Protection" http://www.dhs.gov/xlibrary/assets/niac/NIAC_RMWG_-_2-13-06v9_FINAL.pdf
11. NERC Reliability Metrics Working Group report "Integrated BPS Risk Assessment Concepts" http://www.nerc.com/docs/pc/rmwg/Draft_Integrated_Bulk_Power_System_White_Paper6.1.pdf
12. U.S. National Infrastructure Advisory Council (NIAC) Critical Infrastructure Resilience report http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf

Appendix – Strategic Initiatives Plan

Scenario 1: Physical Attack on Significant Bulk Power System Equipment
A coordinated physical attack on key nodes of the bulk power system critically disables difficult to replace equipment in multiple generating stations or substations and could have a significant affect on the remainder of the system. A prolonged period of time is required to fully restore the bulk power system to normal operation.

- Coordinated physical attack, suspect terrorism
- Three high voltage transmission substations are attacked, severely damaged, and rendered completely inoperable
- Initial damage assessment indicates 6-18 months to return each substation to 100% operating capacity
- Communications are disrupted and disable Transmission Operator voice and data with half their surrounding neighbors, their Reliability Coordinator, and Balancing Authority
- Substations serve large urban population (1 million +)
- Magnitude of loss of load causes BPS instability over a very large geographic area

Scenario 2: Coordinated Cyber Attack
A coordinated disruption disables or impairs the integrity of multiple control systems, or intruders take operating control of portions of the bulk power system such that generation or transmission system is damaged or mis-operated.

- Transmission Operators report unexplained and persistent breaker operations that occur across a wide geographic area (i.e. within state/province and neighboring state/province)
- Communications are disrupted and disable Transmission Operator voice and data with half their surrounding neighbors, their Reliability Coordinator, and Balancing Authority
- Loss of load and generation causes widespread BPS instability, and system collapse within state/province and neighboring state/province. However, portions of the Interconnection remain operational.
- Blackouts in several regions disrupt electricity service to several million people

Scenario 3: Geomagnetic Disturbance
A severe geomagnetic disturbance (GMD) damages difficult to replace generating station and substation equipment, and causes a cascading affect on the remainder of the system. A prolonged period of time is required to fully restore the bulk power system to normal operation.

- Evaluate geomagnetic storm impacts for multiple intensity levels, up to a maximum of 10 times that of 1989
- High voltage transformers irreparably damaged to varying degrees in northern and southern latitudes (ref. page 74-76 of DOE/NERC HILF report http://www.nerc.com/files/HILF.pdf)

Scenario	Tactic	#	Initiative	Priority	Substantial Progress[1]
Common to all Scenarios	Plan	A.	Crisis Response Plan Prepare a coordinated sub-sector-wide crisis response plan; identify roles and responsibilities, including government interfaces.	High Priority	Q1 2011
		B.	Government Interface Develop executive-level (i.e. ESCC) and Sub-Sector interfaces with government on matters related to critical infrastructure.	High Priority	Q4 2010
		C.	Communications Plan Develop a comprehensive communications plan to help ensure NERC and Sub-Sector efforts to address critical infrastructure (including HILF) risks are adequately resourced and appropriately recognized.	High Priority	Q4 2010
		D.	Information Sharing Increase the effectiveness of efforts with government to develop timely and reliable sources of information regarding threats and vulnerabilities.	High Priority	Q4 2010
Scenario 1: Physical Attack	Plan	E.	Physical Attack – Current Capability Assessment Identify opportunities to enhance existing protection, resilience and recovery capabilities of the bulk power system for this scenario, with particular emphasis on opportunities that will also serve to enhance reliability under normal conditions.	High Priority	Q2 2011
	Prevent	F.	Protect Critical Equipment Study options and practices to enhance physical protection of critical equipment requiring long recovery times (e.g. large high-voltage	Important	Q2 2011

[1] "Substantial Progress" means that resources are engaged, an agreed work plan has been established, and alternative solutions to address the initiative have been drafted.

Scenario	Tactic	#	Initiative	Priority	Substantial Progress[1]
			transformers). NOTE: May also apply to Scenario 3 GMD.		
	Recover	G.	Critical Spares Enhance the availability of critical spare equipment that may not be readily available, starting with high voltage transformers. NOTE: May also apply to Scenario 3 GMD.	Important	Q4 2011
		H.	Physical Attack – Restore the Bulk Power System. Enhance restoration plans and procedures. NOTE: Coordinate with other scenarios.	High Priority	Q3 2011
Scenario 2: Cyber Attack	Plan	I.	Cyber Attack – Current Capability Assessment Identify opportunities to enhance existing protection, resilience and recovery capabilities of the bulk power system for this scenario, with particular emphasis on opportunities that will also serve to enhance reliability under normal conditions.	High Priority	Q1 2011
	Prevent	J.	Isolate Critical Cyber Systems Isolate critical cyber systems from other business systems and the Internet.	High Priority	Q1 2011
		K.	Smart Grid Security Influence the development of smart grid technologies to ensure security needs address potential reliability impacts on the bulk power system.	Important	Q4 2011
	Recover	L.	Cyber Attack – Restore the Bulk Power System. Enhance restoration plans and procedures. NOTE: Coordinate with other scenarios.	High Priority	Q3 2011
Scenario 3: GMD	Plan	M.	GMD – Current Capability Assessment Identify opportunities to enhance existing protection, resilience and recovery capabilities of the bulk power system for this scenario, with particular emphasis on opportunities that will also serve to enhance	High Priority	Q2 2011

Scenario	Tactic	#	Initiative	Priority	Substantial Progress[1]
			reliability under normal conditions.		
	Prevent	N.	GMD Protection Determine protective enhancements needed to prevent or minimize damage to facilities. NOTE: May also apply to Scenario 1 Physical Attack.	Important	Q4 2011
	Mitigate	O.	GMD Response Determine what advance warning would be needed for system operators to take action to prevent or mitigate the impact of a GMD.	High Priority	Q2 2011
	Recover	P.	GMD – Restore the Bulk Power System. Enhance restoration plans and procedures. NOTE: Coordinate with other scenarios.	High Priority	Q3 2011