

The background features a large, semi-transparent image of a high-voltage electrical transmission tower on the right side. The tower is a lattice structure with multiple cross-arms. The overall color palette is light blue and white, with a dark blue curved shape in the top right corner. A thick orange horizontal bar runs across the middle of the page.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Technical Committee Report

Critical Infrastructure Strategic Initiatives Coordinated Action Plan

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

Table of Contents

Introduction.....	1
Background.....	1
Roles – Coordinated Action Plan.....	2
Next Steps.....	2
Severe-Impact Scenarios.....	4
Scenario 1: Physical Attack on Significant Bulk Power System Equipment	4
Scenario 2: Coordinated Cyber Attack	4
Scenario 3: Geomagnetic Disturbance.....	5
Scenario 4: Pandemic.....	5
Organization.....	6
Action Plan.....	7
Common to All Scenarios.....	7
Scenario 1: Physical Attack	10
Scenario 2: Cyber Attack	14
Scenario 3: Geomagnetic Disturbances	17
Scenario 4: Pandemic.....	21
Appendix 1: Letter from NERC’s BOT	24
Appendix 2: Scope Development Process	25
Technical Committee Leadership Roster.....	28
NERC Staff Roster.....	29

Introduction

Background

On May 17, 2010, NERC's Board of Trustees (BoT) approved the report, entitled "*High Impact, Low Frequency Event Risk to the North American Bulk Power System*"¹ outlining the results of a joint NERC/DOE workshop on these event risks and outlined nineteen proposals for actions. In a letter from NERC's Board of Trustees Chair, Mr. John Q. Anderson (*Appendix 1: Letter from NERC's BOT*), the Planning, Operating, and Critical Infrastructure Protection Committees were directed to consider these nineteen proposals for action and to "*work with NERC staff to develop such an action plan and submit that plan to the Board of Trustees for its consideration within a reasonable time frame.*"

Further, at the Member's Representative Committee and NERC Board of Trustees meetings on August 4-5, 2010, members discussed the Electricity Sub-Sector Coordinating Council's (ESCC) draft "*Critical Infrastructure Strategic Roadmap*."² This Roadmap provides a framework to address severe-impact risks, including those identified in the High Impact, Low Frequency (HILF) report. The Roadmap provides the NERC Board of Trustees with advice on what should be done to enhance electricity reliability and resilience from an "*all-threats, all-hazards perspective,*" and provides direction for the sub-sector and NERC's Technical Committees. The current version of the Roadmap addresses feedback received at the August 4-5, 2010 meeting as well as that received through the public comment period that closed October 1, 2010. In particular, a new Appendix was added describing a Strategic Initiatives Plan, including strategic initiatives and timelines needed to address the Roadmap's vision and goals. The ESCC Roadmap recognizes that the proposed "*timelines [for the strategic initiatives] should be considered as preliminary estimates prepared by the ESCC, and will require review by the Technical Committees as the scope and necessary resources are more fully understood*".

The leadership of NERC's Planning, Operating, and Critical Infrastructure Protection Committees and NERC Staff, developed the initial approaches for *Critical Infrastructure Protection Coordinated Action Plan* (Action Plan) starting in late June 2010. The development reflected NERC's BoT and ESCC guidance that emerged in mid-2010. At their September 14-16, 2010 meetings, the Operating, Planning, and Critical Infrastructure Protection Committees each approved the general direction of the Action Plan, and authorized the technical committee leadership to finalize the plan for presentation at the November 4, 2010 Board of Trustees meeting.

The Technical Committee leadership and NERC Staff prepared the Action Plan that identifies:

- Four (4) severe-impact scenarios as an approach to address high impact low frequency events
- Defined strategic initiatives that will use these scenarios to formulate recommendations, that reflect relative priorities and lead Technical Committee for each

¹ *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*, <http://www.nerc.com/files/HILF.pdf>

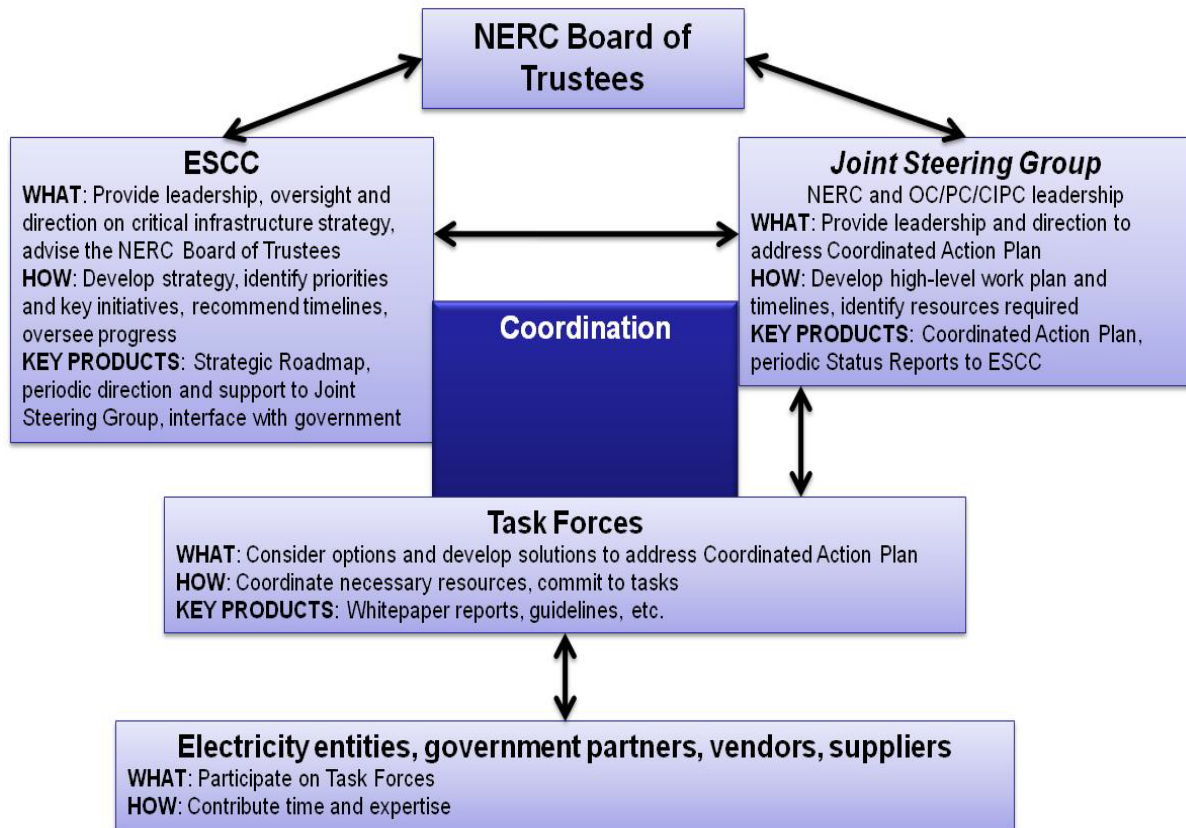
² ESCC Strategic Roadmap – http://www.nerc.com/docs/escc/ESCC_Strat_Roadmap_V3_31_Aug2010_clean.pdf

- A detailed Action Plan for each strategic initiative, including key deliverables and projected milestones

Roles – Coordinated Action Plan

Since these initiatives are unique in crossing among planning, operations, cyber security, communications, and government coordination subjects, a strong coordination organization is considered essential to the successful implementation of the Action Plan. The Technical Committees, the ESCC and NERC Staff have formulated a demonstrated approach to ensure coordination and effectiveness in long-term implementation. Figure 1 below provides the roles, coordination points, and responsibilities of this coordination effort to support this Coordinated Action Plan.

Figure 1: Roles – Coordinated Action Plan



Next Steps

NERC staff will draft Scope/Charter documents for each of the identified Task Forces to address the Action Plan, with input from the Joint Steering Group. Through their usual processes, the Technical Committees will review, refine, and approve the Task Force Scope/Charters, considering the needed resources, deliverables and milestones. The figure below describes the scope development and approval process. *Appendix 2: Scope Development Process* provides a template of the information essential to effectively initiate and oversee these Task Forces.

Figure 2: Scope Development and Approval



Severe-Impact Scenarios

A scenario-based approach has been formulated and endorsed by the ESCC as an effective approach to address high-impact, low-frequency events. Scenario approaches provide guidance and direction in considering practical range of risks and responsive actions, which increase the preparedness and resilience to address them. In addition, a scenario-based approach facilitates the development of coordinated risk management aspects, in part building on existing capabilities that can be extended to address these circumstances. NERC staff and the leadership of the Technical Committees have further developed these scenarios to form a basis for the Action Plan. These scenarios are meant to be broadly representative of severe-impact scenarios and are not intended to provide a design basis threshold.

From a priority vantage point, addressing Scenarios 1-3 are considered high priority, which is consistent in the ESCC Roadmap. Scenario 4, Pandemic, is considered a lower priority that requires continued monitoring as identified in the HILF report, in view of the existing extensive preparations already in place.

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 effect 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 in nature
- 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 disables Transmission Operator voice and data with half their surrounding neighbors, their Reliability Coordinator (RC), and Balancing Authority (BA)
- 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 operation that occurs across a wide geographic area (i.e. within state/province and neighboring state/province)
- Communications are disrupted and disables Transmission Operator voice and data with half their 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 distribution supply 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 effect 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 the 1989 event.³
- High voltage transformers irreparably damaged to varying degrees in northern and southern latitudes.⁴

Scenario 4: Pandemic

A severe pandemic reduces the availability of staff due to illness and taking care of family members.

- 40% of staff unavailable over a 2-week peak wave period
- 20% of staff unavailable over a 2-month period
- No assistance available from neighbors

³ <http://www.nerc.com/files/1989-Quebec-Disturbance.pdf>

⁴ Refer to pages 74-76 of DOE/NERC HILF report (<http://www.nerc.com/files/HILF.pdf>)

Organization

The Technical Committee leadership and NERC staff have formulated an encompassing organization to address the strategic initiatives using the scenario approaches outlined. Table 1 identifies the strategic initiatives associated with each scenario, its relative priority, and assigned leadership (i.e. Operating Committee, Planning Committee, Critical Infrastructure Protection Committee, or NERC staff). The Joint Steering Group has proposed a number of separate Task Forces be established, identified by the colors.

Table 1: Proposed Organization by Subject Area

Scenario	Item	Strategic Initiative	Priority	Lead	Task Force	Scope
Common to all Scenarios ⁵	A	Crisis Response Plan	High	NERC Staff	Not required	
	B	Government Interface	High		Not required, part of ESCC's mandate	
	C	Communications Plan	High		Not required	
	D	Information Sharing	High		Not required	
1 – Physical Attack	E	Current Capability Assessment	High	OC	Severe-Impact Resilience and Physical Security TF	
	F	Protect Critical Equipment	Important			
	G	Critical Spares	Important	PC	Spare Equipment Database TF	Approved by PC, OC Sep-2010
	H	Restore Bulk Power System	High	OC	Severe-Impact Restoration TF	
2 – Cyber Attack	I	Current Capability Assessment	High	CIPC	Cyber Systems Protection TF	
	J	Isolate Critical Cyber Systems	High			
	L	Restore Bulk Power System	High	OC	Control System Security Working Group (CSSWG)	
3 – GMD	M	Current Capability Assessment	High	PC	Geomagnetic Disturbance TF	
	N	GMD - Protection	Important			
	O	GMD- Response	High			
	P	Restore Bulk Power System	High	OC	Severe-Impact Restoration TF	
4 – Pandemic ⁶	Q	H1N1 Lessons-Learned	Monitor	NERC Staff	Not required	
	R	Pandemic Severity	Monitor		Not required	
5 – Smart Grid Cyber Security	K	Smart Grid Security	Important	PC	Smart Grid Task Force	

⁵ NERC staff will lead and be accountable for addressing these initiatives, in coordination with the Technical Committees

⁶ NERC staff will lead and be accountable for addressing these initiatives, in coordination with the Technical Committees

Action Plan

The following Action Plan builds on the strategic initiatives described in the ESCC Roadmap, and provides key deliverables and projected milestones.

Common to All Scenarios

Scenario	Tactic	#	Initiative
Common to all Scenarios	Plan	A.	<p><u>Crisis Response Plan</u> Prepare a coordinated sub-sector-wide crisis response plan; identify roles and responsibilities, including government interfaces.</p> <ol style="list-style-type: none"> 1. Focus on communications between Reliability Coordinators, NERC, Regions and government entities. Assume entity plans are in-place. 2. Develop processes to communicate situation assessments and share sensitive information. 3. Include provisions for exercising this plan as part of periodic large-scale emergency preparedness exercises based on HILF scenarios.
		B.	<p><u>Government Interface</u> Develop executive-level (i.e. ESCC) and Sub-Sector interfaces with government on matters related to critical infrastructure.</p> <ol style="list-style-type: none"> 1. Decide appropriate representation on various government partnership working groups. 2. Clarify with government the roles and authorities during normal and emergency conditions to protect the bulk power system, maintain reliability and recover from severe events. 3. Prioritize Sub-Sector involvement in various government partnership initiatives.
		C.	<p><u>Communications Plan</u> 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.</p> <ol style="list-style-type: none"> 1. Develop and maintain audience-specific key messages. 2. Identify prioritized efforts actively underway. 3. Develop an ongoing feedback process to share lessons-learned across the Sub-Sector, with other critical infrastructures, and with government.
		D.	<p><u>Information Sharing</u> Increase the effectiveness of efforts with government to develop timely and reliable sources of information regarding threats and vulnerabilities.</p> <ol style="list-style-type: none"> 1. Increase the extent to which information is shared between government and the sub-sector on a confidential but unclassified basis, to allow the sub-sector to understand and address potential risks. 2. Reconcile apparent differences in the extent to which classified information is shared by government with entities.

Action Plan

Item	Priority/Tactic	Start Time	Proposed Improvement	Abstract	Lead	Deliverables	Milestones
A. Crisis Response Plan	High - Plan	Near	Improved preparedness to support critical infrastructure during unexpected/extreme conditions	<ul style="list-style-type: none"> ○ Focus on communications between Reliability Coordinators, NERC, Regions and government entities. Assume entity plans are in-place. ○ Develop processes to communicate situation assessments and share sensitive information. 	<i>NERC Staff</i>	Develop a NERC Crisis Response Plan applicable to any severe-impact scenario.	<ul style="list-style-type: none"> ○ Prepare a coordinated sub-sector-wide crisis response plan; identify roles and responsibilities, including government interfaces. <i>Q1 2011</i> ○ Include provisions to test this plan as part of periodic large-scale emergency preparedness exercises involving multiple NERC regions based on severe-impact scenarios, identify lessons-learned and recommend corrective actions. ○ <i>Initial Drill Q1 2011</i> ○ <i>Full-scale exercise Q4 2011</i>
B. Government Interface	High - Plan	Near	Improved government-industry interface on matters related to critical infrastructure.	To ensure roles/responsibilities during attacks on or events that cause widespread impacts on the critical infrastructure are understood and contact points identified.	<i>NERC Staff</i>	Develop executive-level (i.e. ESCC) and Sub-Sector interfaces with government on matters related to critical infrastructure.	<p>Begin Q4 2010</p> <ul style="list-style-type: none"> ○ Decide appropriate representation on various government and cross-sector partnership, working groups. ○ Clarify with government the roles and authorities during normal and emergency conditions to protect the bulk power system, maintain reliability and recover from severe events. <i>Q4 2010</i> ○ Prioritize Sub-Sector involvement in various government and cross-sector partnership initiatives. <i>Q4 2010</i>

Action Plan

Item	Priority/Tactic	Start Time	Proposed Improvement	Abstract	Lead	Deliverables	Milestones
C. Communications Plan	High - Plan	Near	Improved communications of industry activities to address critical infrastructure risks	Communicate broadly to the industry, the public and government/regulators regarding how industry manages risks, with emphasis on severe-impact critical infrastructure risks now and in the future.	<i>NERC Staff</i>	Comprehensive communications plan to help ensure NERC and Sub-Sector efforts to address critical infrastructure (including HILF) risks are adequately resourced and appropriately recognized.	<p>Begin Q4 2010</p> <ul style="list-style-type: none"> ○ Develop and maintain audience-specific key messages. ○ Identify prioritized efforts actively underway and determine the appropriate audiences. Begin delivering key messages. ○ Develop an ongoing feedback process to share efforts to address severe-impact risks across the Sub-Sector, with other critical infrastructures, and with government. ○ Complete Plan Q2 2011
D. Information Sharing	High - Plan	Near	Increase the effectiveness of coordination efforts with government	Increased bi-directional information sharing on threats and vulnerabilities between industry and government before, during and after an event can help manage the overall impact, and develop necessary lessons learned.	<i>NERC Staff</i>	Whitepaper on timely and reliable sources of information regarding threats and vulnerabilities.	<p>Begin Q4 2010</p> <ul style="list-style-type: none"> ○ Influence greater information sharing between government and the sub-sector on a confidential but unclassified basis, to allow the sub-sector to understand and address potential threats and vulnerabilities. ○ Reconcile apparent differences in the extent to which classified information is shared by government with entities. Q2 2011

Scenario 1: Physical Attack

Scenario	Tactic	#	Initiative
Scenario 1: Physical Attack	Plan	E.	<p><u>Physical Attack – Current Capability Assessment</u> 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.</p> <ol style="list-style-type: none"> 1. Model the impact of this scenario on the bulk power system. 2. Identify practices needing particular attention, enhancement, or significant change through this scenario. 3. Develop guidance to enhance overall response.
	Prevent	F.	<p><u>Protect Critical Equipment</u> Study options and practices to enhance physical protection of critical equipment requiring long recovery times (e.g. large high-voltage transformers). NOTE: Portions may also apply to Scenario 3 Geomagnetic Disturbance.</p>
	Recover	G.	<p><u>Critical Spares</u> Enhance the availability of critical spare equipment that may not be readily available, starting with high voltage transformers.</p> <ol style="list-style-type: none"> 1. Identify options and develop alternatives to achieve a robust spares capability. 2. Enhance NERC and industry spare equipment programs. 3. Develop plans and procedures to deploy critical equipment during emergency situations. 4. Identify areas where government may be able to assist in procuring or deploying equipment. <p>NOTE: Portions may also apply to Scenario 3 Geomagnetic Disturbance.</p>
		H.	<p><u>Physical Attack – Restore the Bulk Power System.</u> Enhance restoration plans and procedures, and consider:</p> <ol style="list-style-type: none"> 1. Priorities to restore critical power system loads, and priority customer loads 2. Backup voice and data communications systems, including minimum functionality needs 3. Blackstart, island operation, island synchronization, rotational load shedding 4. Staff safety considerations <p>NOTE: Coordinate with other scenarios</p>

Action Plan

Item	Priority/ Tactic	Start Time	Proposed Improvement	Abstract	Lead	Deliverables	Milestones
E. Physical Attack – Current Capability Assessment	High - Plan	Near	System planning that improves design to harden for physical attacks	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.	OC	<p><i>Task 1:</i> Whitepaper for improved planning methods and designs to withstand physical attacks. Develop new industry guidance or identify opportunities to enhance standards.</p>	<p>Start Task Force <i>Q4 2010</i></p> <p><i>Task 1:</i></p> <ul style="list-style-type: none"> ○ Identify practices needing particular attention, enhancement, or significant change through this scenario. ○ Develop guidance to enhance overall response. ○ Substantial progress⁷ <i>Q2 2011</i> ○ Final report <i>Q4 2011</i>
F. Protect Critical Equipment	Important - Prevent	Mid-term	Improved protection from physical attacks on existing and future equipment requiring long recovery times	<p>Study options and practices to enhance physical protection of critical equipment requiring long recovery times (e.g. high-voltage transformers).</p> <p>NOTE: Portions may also apply to Scenario 3 Geomagnetic Disturbance.</p>		<p><i>Task 2:</i> Whitepaper for improved physical protection of critical equipment requiring long recovery times (e.g. high-voltage transformers). Develop new industry guidance or identify opportunities to enhance standards</p>	<p><i>Task 2:</i></p> <ul style="list-style-type: none"> ○ Survey industry practices ○ Identify improved design options ○ Substantial progress <i>Q2 2011</i> ○ Final report <i>Q4 2011</i>

⁷ Throughout this document, the term “substantial progress” means that resources are engaged, an agreed work plan has been established, and alternative solutions to address the initiative have been drafted.

Action Plan

Item	Priority/Tactic	Start Time	Proposed Improvement	Abstract	Lead	Deliverables	Milestones
G. Critical Spares	Important - Recover	Mid-Term	Improved knowledge of existing spare equipment needed to respond to coordinated physical attacks	<p>Enhance the availability of critical spare equipment that may not be readily available, starting with high voltage transformers. Industry-wide plans and options for deployment are needed</p> <p>NOTE: Portions may also apply to Scenario 3 Geomagnetic Disturbances</p>	PC	<ul style="list-style-type: none"> ○ Whitepaper on development of robust spare inventories, plans to deploy the equipment during emergencies, and how government can support. Develop new industry guidance or identify opportunities to enhance standards ○ Review and enhance spare equipment database ○ Document existing mutual aid or collaborative equipment sharing programs. 	<p>Start Spare Equipment Task Force <i>Q3 2010</i></p> <ul style="list-style-type: none"> ○ Identify options and develop alternatives to achieve a robust spares capability. <i>Q1 2011</i> ○ Enhance NERC and industry spare equipment information-sharing programs. ○ Develop plans and procedures to deploy critical equipment during emergencies. ○ Identify areas where government may be able to assist in procuring or deploying equipment. ○ Finish Whitepaper <i>Q4 2011</i>

Action Plan

Item	Priority/Tactic	Start Time	Proposed Improvement	Abstract	Lead	Deliverables	Milestones
H. Physical Attack – Restore the Physical Bulk Power System	High - Recover	Near	Improved restoration after physical attacks	<p>During large-scale physical attacks and cyber attacks which can be coordinated and timed can threaten reliability and /or damage equipment. Geomagnetic Disturbances can also result in widespread equipment damage.</p> <p>An adaptive plan is needed to ensure timely restoration</p> <p>NOTE: All Restoration activities (H, L & P) are to be completed by one Task Force. Appropriate expertise will be obtained to address the specifics of restoration for each of the cyber, physical and Geomagnetic Disturbances</p>	OC	Whitepaper on enhancing restoration plans and procedures. Develop new industry guidance or identify opportunities to enhance standards.	<p>Start Task Force <i>Q4 2010</i></p> <ul style="list-style-type: none"> ○ Priorities to restore critical power system loads and priority customer loads.⁸ ○ Assess interdependencies between dependent sectors such as communications, transportation, etc. ○ Backup voice and data communications systems, including minimum functionality needs ○ Blackstart, island operation, island synchronization, rotational load shedding ○ Staff safety consideration ○ Substantial progress <i>Q3 2011</i> ○ Final report <i>Q4 2011</i>

⁸Examples of priority loads include end-users such as military bases, hospitals, oil refineries, water treatment plants, etc.

Scenario 2: Cyber Attack

Scenario	Tactic	#	Initiative
Scenario 2: Cyber Attack	Plan	I.	<p><u>Cyber Attack – Current Capability Assessment</u> 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. Consider:</p> <ol style="list-style-type: none"> 1. Adequacy of CIP cyber security standards under this scenario. 2. Ability of system operators to detect and respond to cyber attacks. 3. Opportunities to isolate, prevent further propagation, or otherwise protect in the event of advance warning.
	Prevent	J.	<p><u>Isolate Critical Cyber Systems</u> Isolate critical cyber systems from other business systems and the Internet.</p> <ol style="list-style-type: none"> 1. Assess options, benefits and costs of isolating critical cyber systems (i.e. control systems, energy management systems, protection systems, and their networks). 2. Consider complete or virtual (e.g. Virtual Private Network) separation.
	Recover	L.	<p><u>Cyber Attack – Restore the Bulk Power System.</u> Enhance restoration plans and procedures, and consider:</p> <ol style="list-style-type: none"> 1. Priorities to restore critical power system loads, and priority customer loads 2. Backup voice and data communications systems, including minimum functionality needs 3. Blackstart, island operation, island synchronization, rotational load shedding 4. Integrate cyber incident response processes with operational responses <p>NOTE: Coordinate with other scenarios</p>

Item	Priority/ Tactic	Start Time	Proposed Improvement	Abstract	Lead	Deliverables	Milestones
I. Cyber Attack – Current Capability Assessment	High - Plan	Near	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	The objective is to plan and operate the bulk power system to withstand a coordinated cyber attack as outlined in this scenario.	CIPC	<p><i>Task 1:</i> Whitepaper that outlines opportunities to prevent propagation, ability to detect and respond to cyber attacks and develop new industry guidance or identify opportunities to enhance standards</p>	<p>Start Task Force <i>Q4 2010</i></p> <p><i>Task 1:</i></p> <ul style="list-style-type: none"> ○ Opportunities to isolate, prevent further propagation, or otherwise protect in the event of advance warning. ○ Ability of system operators to detect and respond to cyber attacks. ○ Adequacy of CIP cyber security Standards under this scenario. ○ Substantial progress <i>Q1 2011</i> ○ Final Report <i>Q4 2011</i>
J. Isolate Critical Systems	High - Prevent	Near	Improve cyber security by isolating critical systems from business systems	Investigate isolation approaches to secure critical cyber systems from other business systems and the Internet.		<p><i>Task 2:</i> Whitepaper that investigates isolation methods (i.e. VPN). Develop new industry guidance or identify opportunities to enhance standards.</p>	<p><i>Task 2:</i></p> <ul style="list-style-type: none"> ○ Assess options, benefits and costs of isolating critical cyber systems (i.e. control systems, energy management systems, protection systems, and their networks). ○ Consider complete or virtual (e.g. Virtual Private Network) separation. ○ Substantial progress <i>Q1 2011</i> ○ Final report <i>Q4 2011</i>

Action Plan

Item	Priority/ Tactic	Start Time	Proposed Improvement	Abstract	Lead	Deliverables	Milestones
L. Cyber Attack – Restore the Bulk power System	High - Recover	Near	Improved restoration after cyber attacks	<p>During large-scale physical attacks and cyber attacks which can be coordinated and timed can threaten reliability and /or damage equipment. Geomagnetic Disturbances can also result in widespread equipment damage.</p> <p>An adaptive plan is needed to ensure timely restoration</p> <p>NOTE: All Restoration activities (H, L & P) are to be completed by one Task Force. Appropriate expertise will be obtained to address the specifics of restoration for each of the cyber, physical and Geomagnetic Disturbances</p>	OC	See H for description of Deliverables	See H for description of Milestones

Scenario 3: Geomagnetic Disturbances

Scenario	Tactic	#	Initiative
Scenario 3: Geomagnetic Disturbance	Plan	M.	<p><u>Geomagnetic Disturbance – Current Capability Assessment</u> 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.</p> <ol style="list-style-type: none"> 1. Study the potential impact of a severe Geomagnetic Disturbance on electricity facilities, and impact on reliable operations. When available, consider the results of a FERC study in this area. 2. Identify practices needing particular attention, enhancement, or significant change through this scenario. 3. Develop guidance to enhance overall response.
	Prevent	N.	<p><u>Geomagnetic Disturbance Protection</u> Determine protective enhancements needed to prevent or minimize damage to facilities.</p> <ol style="list-style-type: none"> 1. Shield or shunt damaging fields and currents from sensitive bulk power system equipment. 2. Identify system protection enhancements that may be needed for control systems and protective relays. 3. Study options and practices to prevent catastrophic damage to critical equipment requiring long recovery times (e.g. high-voltage transformers). 4. Consider bolt-on retrofit solutions as well as built-in new designs. <p>NOTE: May also apply to Scenario 1 Physical Attack.</p>
	Mitigate	O.	<p><u>Geomagnetic Disturbance Response</u> Determine what advance warning would be needed for system operators to take action to prevent or mitigate the impact of a Geomagnetic Disturbance. Identify operating procedures to reduce equipment loading, or isolate portions of the grid to limit adverse impact and possible cascade. Communicate this to government to influence advances in the predictive science.</p>
	Recover	P.	<p><u>Geomagnetic Disturbance – Restore the Bulk Power System.</u> Enhance restoration plans and procedures, and consider:</p> <ol style="list-style-type: none"> 1. Priorities to restore critical power system loads, and priority customer loads. 2. Backup voice and data communications systems, including minimum functionality needs. 3. Blackstart, island operation, island synchronization, rotational load shedding. 4. Prolonged operation in islanded configurations. <p>NOTE: Coordinate with other scenarios.</p>

Item #	Priority/ Tactic	Start Time	Proposed Improvement	Abstract	Lead	Deliverables	Milestones
M. GMD – Current Capability Assessment	High - Plan	Near	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.	Identify the current ability to respond to Geomagnetic Disturbances	PC	<p><i>Task 1:</i></p> <p>Whitepaper that outlines the current capability and provide guidance on managing Geomagnetic Disturbances. Develop new industry guidance or identify opportunities to enhance standards.</p>	<p>Start GMD Task Force <i>Q3 2010</i></p> <p><i>Task 1:</i></p> <ul style="list-style-type: none"> ○ Study the potential impact of a severe Geomagnetic Disturbances on electricity facilities, and impact on reliable operations. When available, consider the results of a FERC study in this area. <i>Q1 2011</i> ○ Identify practices needing particular attention, enhancement, or significant change through this scenario. <i>Q2 2011</i> ○ Substantial progress <i>Q2 2011</i> ○ Develop guidance to enhance overall response <i>Q3 2011</i> ○ Final report <i>Q4 2011</i>

Action Plan

Item #	Priority/Tactic	Start Time	Proposed Improvement	Abstract	Lead	Deliverables	Milestones
N. GMD - Protection	High - Prevent	Near	Determine protective enhancements needed to prevent or minimize damage to facilities.	Identifying options available can help planners ensure systems are prepared and operators have the tools/systems available to protect the bulk power system for significant damage. NOTE: May also apply to Scenario 1 Physical Attack.	PC	<i>Task 2:</i> Whitepaper that reviews prevention approaches. Develop new industry guidance or identify opportunities to enhance standards.	<i>Task 2:</i> <ul style="list-style-type: none"> ○ Study options and practices to prevent catastrophic damage to critical equipment requiring long recovery times (e.g. high-voltage transformers). <i>Q3 2011</i> ○ Assess options available for industry application ○ Substantial progress <i>Q4 2011</i> ○ Final report <i>Q4 2011</i>
	Important - Mitigate	Mid-Term	Improved warning will enhance response ability	Advance warning would be needed for system operators to take action to prevent or mitigate the impact of a Geomagnetic Disturbances.		<i>Task 3:</i> Whitepaper on the current warning abilities and areas for improvement. Develop new industry guidance or identify opportunities to enhance standards.	<i>Task 3:</i> <ul style="list-style-type: none"> ○ Review current status of warning abilities ○ Identify improvements and needed resources ○ Substantial progress <i>Q2 2011</i> ○ Final report <i>Q4 2011</i>

Action Plan

Item #	Priority/ Tactic	Start Time	Proposed Improvement	Abstract	Lead	Deliverables	Milestones
P. GMD – Restore the Bulk power System	High - Recover	Near	Enhanced restoration plans and procedures.	<p>During large-scale physical attacks and cyber attacks which can be coordinated and timed can threaten reliability and /or damage equipment. Geomagnetic Disturbances can also result in widespread equipment damage.</p> <p>An adaptive plan is needed to ensure timely restoration</p> <p>NOTE: All Restoration activities (H, L & P) are to be completed by one Task Force. Appropriate expertise will be obtained to address the specifics of restoration for each of the cyber, physical and Geomagnetic Disturbances</p>	OC	See H for description of Deliverables	See H for description of Milestones

Scenario 4: Pandemic

Scenario	Tactic	#	Initiative
Scenario 4: Pandemic	Plan	Q.	<u>H1N1 Lessons-Learned</u> Entities should review existing plans and lessons-learned from H1N1, and consider enhancements.
	Mitigate	R.	<u>Pandemic Severity</u> Continue encouraging government (i.e. Centers for Disease Control) to develop a pandemic “severity index”. 1. Coordinate with other critical infrastructure sectors to reinforce to government to more effectively monitor and communicate severity.

Item	Priority/Tactic	Start Time	Proposed Improvement	Abstract	Lead	Deliverables	Milestones
Q. H1N1 Lessons Learned	Monitor - Plan	Near	Improved pandemic preparedness.	Entities should review existing plans and lessons-learned from H1N1, and consider enhancements.	<i>NERC Staff</i>	Identify possible enhancements to current NERC pandemic planning guidance to the industry.	<ul style="list-style-type: none"> ○ Identify lessons learned <i>Q4 2010</i> ○ Identify possible enhancements to existing NERC pandemic planning guideline <i>Q1 2011</i>
R. Pandemic Severity	Monitor-Prevent	Near	<p>Continue encouraging government (i.e. Centers for Disease Control) to develop a pandemic “severity index.”</p> <p>Coordinate with other critical infrastructure sectors to reinforce to government to more effectively monitor and communicate severity.</p>	Enhanced granularity of the warning system and cross-sector coordination will enhance industry’s ability to manage this risk by limiting over-and under-response during an event.	<i>NERC Staff</i>	<ul style="list-style-type: none"> ○ Coordinate cross-sector support for improved severity index, and prepare white paper to government expressing the need. 	<ul style="list-style-type: none"> ○ Collaborate with other critical infrastructure sectors to decide approach and desired results <i>Q4 2010</i> ○ Communicate results to government <i>Q1 2011</i>

Item	Priority/ Tactic	Start Time	Proposed Improvement	Abstract	Lead	Deliverables	Milestones
K. Smart Grid Security	Important - Recover	Mid- Term	Influence the development of smart grid technologies to ensure security needs address potential reliability impacts on the bulk power system.	<p>Ensure that smart grid integration includes required cyber security measures to maintain reliability during this scenario.</p> <p>Identify smart grid security issues at risk of not being addressed appropriately and escalate through industry stakeholder mechanisms (e.g. industry associations, ESCC).</p>	<i>PC</i>	Document ongoing participation in industry and governmental smart grid cyber security activities.	<ul style="list-style-type: none"> ○ Continue to participate on the NERC Smart Grid Task Force and resulting initiatives. ○ Identify smart grid security Standards development activities requiring substantially greater industry participation and coordination. <i>Q1 2011</i> ○ Monitor and contribute to the development of smart grid security standards. ○ Substantial progress <i>Q4 2011</i>

Appendix 1: Letter from NERC's BOT



John Q. Anderson, Chairman
NERC Board of Trustees

May 25, 2010

**To: NERC Operating Committee
NERC Planning Committee
NERC Critical Infrastructure Protection Committee**

This week, the NERC Board of Trustees formally approved the *Summary Report on the November 2009 High-Impact, Low-Frequency Event Risk Workshop*. Thank you for your review and consideration of the document.

As you are aware, the document contains 19 *Proposals for Action* to more fully address these risks on a sector-wide basis. Through our approval of the document, we formally request that the committees work with NERC staff to develop such an action plan and submit that plan to the Board of Trustees for its consideration within a reasonable time frame.

We recognize that this request comes to the committees amid a large volume of work on subjects ranging from the reliable integration of renewables to cyber security to frequency response, in addition to the ongoing development of the seasonal and long-term assessments and other routine standing committee activities. We appreciate your efforts to accommodate this additional activity.

The volunteers making up NERC's standing technical committees are one of the organization's greatest assets. We commend you, as always, for your service and recognize your immeasurable contributions to this organization.

Regards,

A handwritten signature in black ink, appearing to read "John Q. Anderson".

John Q. Anderson
Chairman

cc: Gerry Cauley, President and CEO, NERC
David Cook, Vice President and General Counsel, NERC
Mark Lauby, Director, Reliability Assessments and Performance Analysis, NERC
David Hilt, Vice President and Director of Operations and Engineering, NERC
NERC Secretaries:
NERC Operating Committee
NERC Planning Committee
NERC Critical Infrastructure Protection Committee

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

Appendix 2: Scope Development Process

PART A: Required for Committee Approval

Purpose

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

The purpose of the TF is to *[one or two sentences in high-level terms describing what the TF will accomplish.]*

Background

[Short paragraph or two describing the background and rationale for the need to establish this TF.]

Scope

[Short paragraph or two describing overall scope of the project. Don't repeat details that will be in the remainder of this document.]

Assumptions and Limitations

[Describe the underlying assumptions that are important or unique for this TF. Describe any limitations or areas that are intentionally out of scope.]

Goals and Objectives

[Complete this table to describe the specific objectives that will accomplish each high-level goal. The objectives essentially describe what will be achieved, and how. There may be several objectives needed to address each goal. Note that these are different than milestones and deliverables, which are addressed in Part B.]

Goals	Objectives
Review current situation and capabilities	1.
Perform needs assessment	2.
Develop alternative solutions	3.
Recommend solutions	4.

Task Force Reporting Structure

The TF will:

- Report to *[name of NERC Committee]*.
 - Provide periodic status reports to *[name of NERC Committee]*
 - Coordinate closely with *[name other Committees or Task Forces that need to be particularly connected to the work of this TF]*

Resources Required

The TF requires expertise and representation in the following areas: *[Be as specific as possible. Include expertise that is needed from the electricity industry as well as outside, such as equipment suppliers and manufacturers, government partners, etc. Consider which segments of the industry should be most involved and sufficient regional, U.S. and Canadian representation. As a rule of thumb, membership should be between 12 and 20 members. As the Task Force proceeds with its work, additional subject matter experts may be included in sub-groups as needed.]*

- Experience in ...
- In-depth experience in...
- Familiarity with...

[X]conference calls expected per month, and a total of [Y] face-to-face meetings will be required, in addition to the time required to contribute to this effort. This work will begin in [month/year] and end by [month/year].

References

[Identify references needed to provide TF members with a common understanding of related reports or initiatives.]

Name	Link
DOE/NERC HILF “ <i>High Impact, Low Frequency Risk to the North American Bulk Power System</i> ” report	http://www.nerc.com/files/HILF.pdf
<i>Critical Infrastructure Strategic Roadmap</i>	http://www.nerc.com/docs/escc/ESCC_Strat_Roadmap_V3_31_Aug2010_clean.pdf
NERC Technical Committees’ Report – <i>Critical Infrastructure Strategic Initiatives Coordinated Action Plan</i>	

PART B: Required Following Committee Approval

Deliverables

[Describe the final products or deliverables for each milestone.]

Milestone	Deliverable
1. Determine scope and resources <ul style="list-style-type: none"> • Confirm assumptions and limitations • Identify and recruit industry experts • Develop project plan and timelines 	<ul style="list-style-type: none"> • Accept Scope by Qx-20yy
2. Provide comprehensive assessment <ul style="list-style-type: none"> • Identify options and alternatives with pros and cons • Decide specific solutions • Propose final deliverables and timelines 	<ul style="list-style-type: none"> • First draft report or whitepaper by Qx-20yy
3. Provide final deliverables <ul style="list-style-type: none"> • Prepare final report • Develop new industry guidance, or enhance existing • Propose new or revised NERC reliability standards, where necessary and appropriate • Identify next steps 	<ul style="list-style-type: none"> • Final report or whitepaper by Qx-20yy

Task Force Members

Role	Name	Organization
Chair		
Vice-Chair		
Facilitator		NERC
Member		
Member		
Member		

Prepared by: _____
 NERC Facilitator

Approved by: _____
 Sponsor – Operating, Planning, or Critical Infrastructure Protection Committee

 Date

Technical Committee Leadership Roster

Position	Name / Title	Company City, State/Province	Phone/ E-mail
CIPC Chair	Barry Lawson Manager, Power Delivery	National Rural Electric Cooperative Association 4301 Wilson Blvd Arlington, Virginia 22203	(703) 907-5781 (703) 907-5517 Fx barry.lawson@nreca.coop
CIPC Vice Chair	Robert D. Canada Business Assurance Principal	Southern Company Services, Inc. 30 Ivan Allen Jr. Blvd; NW, Atlanta, Georgia 30308	(404) 506-5145 rdcanada@southernco.com
CIPC Vice Chair	Robert Howard McClanahan Vice President, Information Technology	Arkansas Electric Cooperative Corporation One Cooperative Way P.O. Box 194208 Little Rock, Arkansas 72219-4208	(501) 570-2403 (501) 570-2903 Fx Robert.McClanahan@aecc.com
OC Chair	J.S. Holeman Director, System Operations	526 South Church Street, Charlotte, North Carolina 28202	(704) 382-0011 Sam.Holeman@duke-energy.com
OC Vice Chair	Tom Bowe Executive Director Reliability Integration	PJM Interconnection, L.L.C. 955 Jefferson Avenue Valley Forge Corporate Center Norristown, Pennsylvania 19403-2497	(610) 666-4776 (610) 666-4282 Fx bowet@pjm.com
PC Chair	Thomas C. Burgess Director, FERC Compliance	FirstEnergy Corp. 76 South Main Street Akron, Ohio 44308	(330) 384-5225 burgess@firstenergycorp.com
PC Vice Chair	Jeffrey Mitchell Director - Engineering	ReliabilityFirst Corporation 320 Springside Dr. Suite 300 Akron, Ohio 44333	(330) 247-3043 (330) 456-3648 Fx jeff.mitchell@rfirst.org

NERC Staff Roster

North American Electric Reliability Corporation
 116-390 Village Boulevard
 Princeton, New Jersey 08540-5721

Reliability Assessments and Performance Analysis

Name	Title	E-mail
Mark G. Lauby	Director of Reliability Assessment and Performance Analysis	mark.lauby@nerc.net

NERC Contractor

Name	Title	E-mail
Stuart Brindley	Consultant	stuart.brindley@gmail.com

Critical Infrastructure Protection

Name	Title	E-mail
Mark Weatherford	Vice President and Chief Security Officer of the Critical Infrastructure Protection	mark.weatherford@nerc.net
Tim E Roxey	CIP Program Manager	tim.roxey@nerc.net
Brian Harrell	Manager of CIP Standards	brian.harrell@nerc.net

NERC Staff Coordinators Standing Committees

Name	Title	E-mail
Larry J. Kezele	Manager of Operations	larry.kezele@nerc.net
Scott R. Mix	CIP Technical Manager	scott.mix@nerc.net
John L. Seelke	Manager of Planning	john.seelke@nerc.net