NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Scope

Cyber Attack Task Force (CATF)

PART A: Required for Committee Approval

Purpose

This document defines the scope, objectives, organization, deliverables, and overall approach for the Cyber Attack Task Force (CATF).

The purpose of the CATF is to consider the impact of a coordinated cyber attack on the reliable operation of the bulk power system, and identify opportunities to enhance existing protection, resilience, and recovery capabilities.

Background

The NERC and DOE report *High Impact, Low Frequency Risk to the North American Bulk Power System* 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. Two of these initiatives (i.e. items I and J) identify the need to assess the current capability of the bulk power system to withstand and recover from a coordinated cyber attack scenario.

NERC staff and the leadership of the NERC technical committees (Planning, Operating, and Critical Infrastructure Protection Committees) have developed the *Critical Infrastructure Strategic Initiatives Coordinated Action Plan* (Coordinated Action Plan) to address these severe-impact scenarios. This Scope document provides clear direction to the CATF and builds on the deliverables and milestones described in the Coordinated Action Plan.

Scope

The primary intent of the CATF is to consider the impact of a coordinated cyber attack on the operation of the bulk power system, and to develop flexible options for detecting, operating, and recovering. These flexible options will enhance the bulk power system's resilience because operators should be even better prepared to recognize such an event and be ready to implement mitigation tactics that may include unique solutions tailored to the situation using approaches not typical to daily operations.

The CATF will consider what detection, response, and recovery processes will be particularly challenged through a coordinated cyber attack, and propose options to improve timely response.

These processes will include power system operations practices, plans, and procedures, as well as the tools and systems that operators rely upon to manage the reliable operation of the bulk power system.

The CATF will recommend solutions for broad implementation across the electricity sector. 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 CATF may consider establishing sub-teams to address the various operational and tools/systems issues that may be unique to coordinated cyber attack scenarios.

Assumptions and Limitations

The CATF will focus on early detection of a coordinated cyber attack and the means to continue to reliably operate the bulk power system. Opportunities to enhance restoration of the bulk power system following a major blackout under this scenario will be addressed by the Severe-Impact Resilience Task Force (SIRTF) that will address all three severe-impact scenarios; coordinated physical attack, coordinated cyber attack, and geomagnetic disturbance. The SIRTF will seek support and advice from the CATF.

A separate Smart Grid Security Task Force is being established to address security issues related to smart grid.

The coordinated cyber attack scenario described in the Coordinated Action Plan is intended to describe extreme conditions that would make bulk power system operations much more challenging than would normally be considered by electricity entities through their usual planning and preparedness activities. Therefore, solutions that may offer limited, yet measurable, enhancements are encouraged. For example, the CATF should identify the minimum functionality of operations tools and systems needed to maintain reliability.

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 events.

Goals and Objectives

Goals	Objectives
Review current situation and capabilities	1. Consider the ability of entity system operators and cyber security analysts to detect and respond to a coordinated cyber attack. 2. Consider the extent to which entities may not isolate critical cyber systems from other business or Internet-facing systems, and the extent to which this increases the vulnerability of their systems. 3. Consider opportunities to isolate, prevent further propagation, or otherwise protect cyber systems and bulk power system assets. 4. Consider the capabilities of voice and data communications tools and energy management systems, with a focus on which minimum functional needs system operators must retain and the alternative

	methods to acquire or maintain this capability even in a reduced state. 5. Consider staffing capacity, challenges, and safety. 6. Assess the adequacy of current CIP cyber security practices under a coordinated cyber attack scenario.
Perform needs assessment	7. Identify the functions needed to support reliable power system operations that would be particularly challenged under a coordinated cyber attack scenario.
Develop alternative solutions	8. Assess the options, benefits, and costs associated with isolating critical cyber systems (i.e. control systems, energy management systems, protections systems, and their networks). Consider complete or virtual (e.g. virtual private network) separation. 9. Propose a range of alternative solutions to enhance operating capabilities, 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	10. Assist in outreach efforts to educate regulators, organizations, and other infrastructures in better understanding the electricity sector's preparations to address these threats.
Recommend solutions	11. Recommend potential practices or programs for use by NERC or individual entities. Create scalable drill templates that registered entities could utilize to train personnel and enhance current restoration and operating protocols.

Task Force Reporting Structure and Coordination with other Related Initiatives

The task force will:

- Report to the Critical Infrastructure Protection Committee. Seek Operating Committee endorsement prior to Critical Infrastructure Protection Committee approvals.
- Provide periodic status reports to the Critical Infrastructure Protection Committee and Electricity Sub-Sector Coordinating Council.
- Coordinate closely with the SIRTF on items related to restoration.
- Coordinate with other NERC and industry resources that may be able to contribute, such as the:
    - NERC Cyber Security Standards Drafting Team
    - Energy Sector Control Systems Working Group (ESCSWG)
    - Industrial Control Systems Joint Working Group (ICSJWG)

Resources Required

The task force requires expertise in the following areas:

- Experience with the real time operation of the bulk power system, in particular the communications and energy management systems and tools typically used by reliability coordinators, transmission operators, and generator operators.
- In-depth experience with implementing, maintaining, and operating cyber security policies, practices, tools, and procedures.
- Familiarity with the NERC CIP Cyber Security Standards.

It is anticipated that two conference calls per month, and a total of four 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's Report – *High Impact, Low Frequency Risk to the North American Bulk Power System*	http://www.nerc.com/files/HILF.pdf
ESCC's *Critical Infrastructure Strategic Roadmap*	http://www.nerc.com/docs/escc/ESCC_Strat_Roadmap_V5_20_Oct2010_clean.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_102510.pdf

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PART B: Required Following Committee Approval

Deliverables

Milestone	Deliverable
1. Determine scope and resources • Confirm assumptions and limitations • Identify and recruit industry experts • Develop project plan and timelines	• Accept Scope by Q4-2010
2. Provide comprehensive assessment • Identify options and alternatives with pros and cons • Decide specific solutions • Propose final deliverables and timelines	• Substantial progress by Q1 2011 • Draft report or whitepaper by Q3-2011
3. Provide final deliverables • Prepare final report • Develop new industry guidance, or enhance existing • Identify next steps	• Final report or whitepaper by Q4-2011

Task Force Members

Role	Name	Organization
Chair	Mark Engels	Dominion
Vice-Chair		
Facilitator	Tim Roxey	NERC
Member		
Member		
Member		
Member		

Prepared by: _____
NERC Facilitator

Approved by: _____
Sponsor – Critical Infrastructure Protection Committee

_____
Date