DRAFT - 4

North American Electric Reliability Council

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

CRITICAL INFRASTRUCTURE PROTECTION COMMITTEE (CIPC)
Agenda

Meeting Schedule
The Critical Infrastructure Protection Committee meets:
25-26 March 2004, Thursday (0800-1630 hr) – Friday (0800-1200 hr)
Renaissance Nashville Hotel
611 Commerce Street; Nashville, Tennessee 37203
tel: 615-255-2400, fax: 615-255-8202
Attire is casual.

Please register for the meeting at: http://www.nerc.com (link: Meetings).

Materials
1. Minutes of the NERC CIPAG Meeting 13-14 January 2004, draft-2
2. CIPC Action Items
3. CIPC 2004 Organization and Work Plan
4. NERC Board Recommendations on Blackout and Committee(s) Involvement
5. (Other materials to be forwarded as available.)

Agenda

	Time	Topic	Presenter
1	15 min	Administrative items: • Welcome and introductions • Logistics: NERC anti-trust compliance guidelines, CIPC governance, proxies • Amend and approve this agenda. • Amend and approve minutes of the 13-14 January 2004 CIPAG meeting (reference materials).	Stuart Brindley Lou Leffler Stuart Brindley Lou Leffler
2	15 min	NERC update. Standards and Compliance programs	Lou Leffler Wally Johnson
3	15 min	August 14, 2003 outage: CIPC related actions (reference materials)	Lou Leffler
4	15 min	CIPC action items review (reference materials)	Lou Leffler
5	45 min	CIPC Executive Committee: • Feedback: February 2004 NERC Board meeting • Sector Coordinators, ISACCouncil, governance • Sector Coordinators/ISACCouncil/DHS retreat • National Infrastructure Advisory Group (NIAC) • Operation Clarity and Improvement (OCI) Matrix	Stuart Brindley Lou Leffler
6		**ESISAC Subcommittee updates:**	
6a	15 min	Outreach Working Group	Wally Johnson

	Time	Topic	Presenter
6b	30 min	Reporting Technologies Working Group	Carl Eng
6c	15 min	Analysis Working Group	Chris Uranga
6d	15 min	Indications, Analysis, Warnings Working Group • Overview of the revised National Response Plan • Situational response expected of the ESISAC	Larry Bugh
6e	30 min	NESEC Task Force	Jack Bernhardsen Dejan Sobojic, EPRI
6f	5 min	IDS Pilot Task Force	Stuart Brindley
7		**Security Planning Subcommittee updates:**	
7a	30 min	Standards and Guidelines Working Group • DHS Critical Infrastructure Information order and proposed NERC comments • Urgent action Cyber Security Standard: compliance, renewal • Permanent Cyber Security Standard	John Maguire Barry Lawson, Larry Brown Larry Bugh
7b	30 min	Risk Assessment Working Group	Ted Heller
7c	30 min	Process Control Systems Security Task Force	Scott Mix
7d	15 min	Public Key Infrastructure Task Force	Larry Bugh
7e		HEMP Task Force	Jim Silk
7f	15 min	Critical Spares Task Force	Michael Innocenzo Ken Hall
8	Thursday evening 1700-1900	Cyber Security Summit Task Force reports	ITAA representatives
9		**Agency briefings:**	
9a	15 min	Public Safety and Emergency Preparedness Canada	Kara Yorke
9b	15 min	Department of Energy	Hank Kenchington
9c	15 min	Department of Homeland Security	Paul Carrier
9d		Federal Energy Regulatory Commission	
10	45 min	Follow up and actions from all briefings and working group/task force reports	All
11	45 min	CIPC Work Plan review (reference materials)	All
12	30 min	Roundtable discussion (pens down).	All
13		Other	All
14	10 min	Confirm future meetings (see below).	Lou Leffler

Future meetings:

1. 09 June 2003, Wednesday (0800-1700 hr); Washington, DC.
2. 10 June 2003, Thursday (0800-1200 hr); Washington, DC (cleared briefing by DHS).
3. 16-17 September 2004, Thursday (0800-1700 hr) – Friday (0800-1200 hr); New Orleans, LA (coupled with EEI Security Committee).
4. 11-12 November 2004, Thursday (0800-1700 hr) – Friday (0800-1200 hr); Kansas City, MO (coupled with NERC Standing Committees).
5. Security briefing conference calls will be conducted on first and third Fridays each month and as conditions require.
6. CIPC, Working Group, Task Force conference calls will be conducted as required.

12 Feb 2004, 24 Feb 2004, 29 Feb 2004, 02 Mar 2004
{agd_cipc_25mar2004.doc}

Attachment 3

NERC CRITICAL INFRASTRUCTURE PROTECTION COMMITTEE

2004 ORGANIZATION WORK PLAN

- Organization Chart
- CIPC Work Plan 2004
- Working Group and Task Force Rosters
- Role Descriptions for CIPC Working Groups and Task Forces
- ESISAC (Electricity Sector Information Sharing and Analysis Center) Subcommittee: Working Group and Task Force Plans
  - Outreach Working Group
  - Reporting Technologies Working Group
  - Analysis Working Group
  - IDS (Intrusion Detection System) Pilot Task Force
  - IAW (Indications, Analysis, Warning) Working Group
- Security Planning Subcommittee: Working Group and Task Force Plans
  - Standards and Guidelines Working Group
  - Process Control Systems Security Task Force
  - Risk Assessment Working Group

March 03, 2004

CIP Committee Structure

CIPC

Executive Committee

Manage policy matters and provide support to SCs, WGs

ESISAC SC

Develop & maintain ISAC capability to respond to security threats & incidents

Outreach WG
Reporting Technologies WG
NESEC TF
Analysis WG
IDS Pilot TF
IAW WG

Security Planning SC

Improve ES ability to protect critical infrastructure

Standards & Guidelines WG
PCSS TF
PKI TF
Risk Assessment WG
HEMP TF
Critical Spares TF

CRITICAL INFRASTRUCTURE PROTECTION COMMITTEE (CIPC)
WORK PLAN – 2004

Note: The CIPC will adjust this plan as necessary through time.

Each Subcommittee, Working Group, Task Force will have chair, vice chair, NERC staff, with representation from Physical Security, Cyber Security, Operations, Governments. Staffing will come from CIPC Members, Alternates, Associates, and others with specific contributory capability. Each group will have a CIPC Executive Committee sponsor. (Individual assignments are in a separate document.)

Activity	***Deliverables***	***Assignments***
1. Manage policy matters, provide leadership to Subcommittees and support to Working Groups and Task Forces. Identify new initiatives driven by: • Lessons-learned from real events such as August 14, 2003 blackout, physical and cyber security events • Government policy - HSPD-7 (CIP) and HSPD-8 (Emergency Preparedness) • Industry evolution to mandatory standards • CIP activities of other critical sectors.	Continue development of relationships between the ES and Government decision-makers (Canada and US). Identify CIPC alignment with government CIP activities. Meeting of CIPC Executive Committee with senior contacts at DOE, DHS and PSEPC regarding strategic and tactical measures to enhance security of the ES.	CIPC Executive Committee
2. Improve Electricity Sector Information Sharing and Analysis Center (ESISAC) capabilities to respond to security threats & incidents.	**Define the scope of a mature ESISAC and develop a NERC business case.**	**ESISAC Subcommittee, Working Groups, Task Forces**
3. Establish and maintain coordination with the other ten ISACs via the ISAC Council.	Participate with the ISAC Council. Participate, as feasible, with the National Infrastructure Advisory Council (NIAC). Participate in exercises. Coordinate with other critical sectors. Participate in interdependency studies.	CIPC Executive Committee
4. Develop mechanisms to reach out broadly from CIPC to the electricity industry to raise awareness, and enhance security.	Review existing Library of CIPC products and organize for better access and use. Establish RRO CIP organizations or liaison & build Regional email exploders for CIP. Explore Communications concepts and business plan. Establish Speakers Bureau and workshop planning organization.	Outreach Working Group.
5. Assure effective two-way reporting of security-related threats and incidents between ES and Governments.	Propose coordinated reporting with DHS, DOE, other agencies. Identify and assess reporting technologies for applicability, reliability, security.	Reporting Technologies Working Group.
6. Coordinate with the Operating Committee and DHS in development of the North American Electric Security Monitoring System.	Participate as defined by NESEC project scope.	NESEC Task Force
7. Develop the business case for ISAC analysis. Add to the relevance of information from Government to ES.	Conduct industry threat analysis. Analyze collected events from the ES and local and federal authorities. Notify industry of events that could potentially impact the security of ES critical infrastructure.	Analysis Working Group.

Activity	*Deliverables*	*Assignments*
8. Assess the capability of IDS tools and analytical processes to detect targeted attacks.	Determine data requirements and install sensors (ISOs only due to confidentiality concerns). Gather and analyze data. Issue report identifying methodology lessons-learned applicable to industry as a whole.	Intrusion Detection System Pilot Task Force.
9. Conduct a thorough review of the Indications, Analysis, Warnings Program (IAW) Standard Operating Procedure (SOP).	Review and revise the ES's IAW SOP.	IAW Program Working Group.
10. Improve ES ability to protect critical infrastructure.	**Identify or develop practical methods to be used by the ES to protect their critical infrastructure.**	**Security Planning Subcommittee, Working Groups, Task Forces**
11. Promote and contribute to the development and maintenance of NERC security standards and guidelines.	Coordinate and aggregate CIPC comments on NERC standards, SARs, and guidelines to provide appropriate CIP perspective. Review existing, and coordinate the development of new, CIPC security guidelines. Develop a schedule to review and comment on non-CIPC, security focused, electric and non-electric industry standards and guidelines. Liaise with ESISAC outreach group to inform and educate on existing and proposed standards and guidelines, as necessary.	Standards and Guidelines Working Group.
12. Develop a plan to secure process control systems in collaboration with vendors.	Work with NERC Standing Committees to complete the Time Synchronization Guideline as one of a set of documents to fulfill Blackout Recommendations. Review and propose updates to the DOE 21 Steps to Improve Cybersecurity of SCADA document. Develop one to two new Security Guidelines based on topics contained in the DOE 21 Steps document. Maintain a relationship with the Risk Assessment Task Force to ensure that security is implemented commensurate with the risk to be assumed.	Process Control Systems Security Task Force.
13. Develop a Public Key Infrastructure (PKI) trust model and technical specification for the ES.	Develop a PKI framework as defined by project plan approved by NERC Board.	PKI Task Force
14. Develop criteria to identify critical ES assets, assess security threats, identify risk assessment methodologies, assess effectiveness of physical protection measures.	Interface with government entities performing risk assessments on the ES and help guide, direct, or influence these assessment efforts. Review risk assessment analyses and vulnerability exercises and provide "Lessons Learned" as appropriate. Assess current threat situation and trend. Establish metrics for assessing vulnerability of the ES and establish the ability to track the vulnerability trend in the future. Assess effectiveness of protection measures. Identify risk assessment methodologies. Provide input and material regarding risk assessments for Standards and Guidelines as appropriate.	Risk Assessment Working Group.
15. Review impact of HEMP on the ES and identify mitigation measures.	Review Commission report as impacting the ES. Include consideration of Radio Frequency Warfare. Identify recommendations to the ES.	HEMP Task Force
16. Protect transformers and other long lead-time critical components.	Establish and operate a critical spares database. Coordinate with others (FERC, EPRI, DHS). Liaise with OC, PC to meet planning and operational needs.	Critical Spares Task Force

CIPC Working Group and Task Force Rosters

WG/TF Name	Scope	Chair	EC Sponsor	NERC Staff
CIPC Executive Committee: Manage policy matters, provide leadership to Subcommittees and support to Working Groups and Task Forces Stuart Brindley, Chair; Larry Bugh, Vice Chair; Pat Laird, Vice Chair; Bob Canada, Physical Security; Roger Lampila, Operations; Barry Lawson, Policy; Jamey Sample, Cyber Security; Lou Leffler, Secretary				
ESISAC Subcommittee: Develop and maintain ISAC capability to respond to security threats & incidents.				
Outreach WG	Develop mechanisms to increase the awareness and use of these products across the ES Members: Wally Johnson, Bob Canada, Michael Lynch, Chris Uranga, Paul Carrier, Eric Solberg, Larry Dolci, Allen Klassen, Brian Malfant, Tom Glock, Rob Hoffman	Wally Johnson	Bob Canada	Lou Leffler
Reporting Technologies WG	Assure effective two-way reporting of security-related threats and incidents between ES and Governments. Members: Carl Eng, Jamey Sample, Eric Solberg, Steve Myers, Dave Baumken, Jean-Guy Ouimet, Bob Windus, Ted Heller, Frank Prieto, Joe Weiss, Scott Mix, Allen Klassen, Hank Kenchington, Tom Glock, Paul Carrier	Carl Eng	Jamey Sample	Lyn Costantini
• NESEC TF	Coordinate with the Operating Committee and DHS in development of the North American Electric Security Monitoring System. Members: Jack Bernhardsen, Barry Lawson, Stuart Brindley, Steve Myers, Bonnie Bushnell, Bob Windus, Ted Heller, Roger Lampila, Paul Carrier	Jack Bernhardsen	Barry Lawson	Lyn Costantini
Analysis WG	Develop the business case for ISAC analysis. Add to the relevance of information from Government to ES. Members: Chris Uranga, Bob Canada, Todd Thompson, Glenn Coplon, Tom Kropp, Ted Heller, Joe Weiss, Chuck Noble, Jerry Freese, Mike Peters, Jason Larson, Carl Eng, Scott Moore, Jack Bernhardsen, Michael Cohen	Chris Uranga	Bob Canada	Ron Niebo
• IDS Pilot TF (For ISOs only)	Assess the capability of IDS tools and analytical processes to detect targeted attacks Members: Stuart Brindley, Roger Lampila, Jamey Sample, Chris Uranga, Chuck Noble	Stuart Brindley	Stuart Brindley	Not required

WG/TF Name	Scope	Chair	EC Sponsor	NERC Staff
IAW WG	Conduct a thorough review of the Indications, Analysis, Warnings Program (IAW) Standard Operating Procedure. Members: Larry Bugh, Roger Lampila, Tom Kropp, Allen Klassen, Bob Windus, Bob Beahm, Ted Heller, Kara Yorke, Chuck Noble, Paul Carrier	Larry Bugh	Roger Lampila	Lou Leffler
Security Planning Subcommittee: Improve ES ability to protect critical infrastructure.				
Standards & Guidelines WG	Promote and contribute to the development and maintenance of NERC security standards and guidelines Members: John Maguire, Pat Laird, Bruce Metruck, Joe Doetzl, Tom Kropp, Dave Baumken, Jay Cribb, Franklin Dessuit, Joe Weiss, Deborah Linke, Al Tardiff, Jerry Freese, Seiki Harada, Bill Flynt, Scott Webber, Linda Nappier, Sandy Brewer, Michael Lynch, Randy Mayfield, Bob Sypult, Lyman Shaffer, Larry Bugh, Chuck Noble, Kurt Muehlbauer, John Pavek, Scott McCoy, Elizabeth Rhodenizer	John Maguire	Pat Laird	Lyn Costantini
• PCSS TF	Develop a plan to secure process control systems in collaboration with vendors. Members: Scott Mix, Jamey Sample, Ted Heller, Joe Weiss, Franklin Dessuit, Linda Nappier, Tom Flowers, Bob Richhart, Homer Cotton, Jerry Freese, Sergio Guzman, Judith Harris, Rishi Tripathi, Ron Belval, Martin Morgan, John Maguire, Tim DeLoach, Dave Norton, Jim Miller, Paul Carrier, Scott Boyer, Mike Peters, Al Tardiff, Roman Shaffer, Tom Kropp, Abbie Layne, Jeff Dagle, Mark Bruen, Hank Kenchington, Elizabeth Rhodenizer, Eric Byres	Scott Mix	Jamey Sample	Lou Leffler
• PKI TF	Develop a PKI trust model and technical specification for the ES Members: Larry Bugh, Tom Kropp, Jay Cribb, John Maguire, Scott Mix, Elizabeth Rhodenizer	Larry Bugh	Larry Bugh	Lynn Costantini

WG/TF Name	Scope	Chair	EC Sponsor	NERC Staff
Risk Assessment WG	Develop criteria to identify critical assets, assess security threats, identify risk assessment methodologies, assess effectiveness of physical protection measures Members: Ted Heller, Pat Laird, Len Januzik, Glenn Coplon, Bob Windus, Bob Beahm, Bill Flynt, Dave Baumken, Jim Fetzer, Tom Kropp, Jean-Guy Ouimet, Deborah Linke, Scott McCoy, Tom Flowers, Paul Carrier, John Pavek, Jim McGlone, Brad Hyland, Joe Bucciero, Dave Andrews, Lyman Shafer, Elizabeth Rhodenizer, Chuck Chakravarthi, Ken Hall, Chuck Harper, S. Jackson, John Maguire, G. McGlynn, Scott Mix, G. Stephens, Jeff Dagle, Mike Peters, Michael Cohen	Ted Heller	Pat Laird	Gerry Cauley
• HEMP TF	Review phenomena associated with HEMP and recommend mitigation measures. Members: Jim Silk, Jamey Sample, Len Januzik, Larry Dolci, Bob Windus, Ted Heller, Nick Abi-Samra , John Baranowski, Jack Bernhardsen, Navin Bhatt, Bonnie Bushnell, Glenn Coplon, Wally Johnson, Dick Kafka, Sam Jones, Scott Mix, Scott Moore, John Pavek, Ron Smith, Raymond Vojdani, Francois Lévesque	Jim Silk	Jamey Sample	Lou Leffler
• Critical Spares TF	Protect transformers and other long lead-time critical components. Members: Michael Innocenzo, Ken Hall, Roger Lampila, Len Januzik, Ted Heller, Scott McCoy, Larry Dolci, Bob Windus, Deborah Linke, Bill Bojorquez, Jamey Sample, Don Covaleski, Sandy Brewer, Eric Solberg, Michael Lynch, Paul Johnson, John Riley, Lee Westbrook, Mike Green, Bill Harm, Bruce Renwick, Don Volzka, Larry Brusseau, Karl Tammar, Doug Powell, Perry Stowe, Chuck Chakravarthi, Michael Hagee, Malcolm V. Thaden, Jr., Mike Gevaza, Paul Carrier, Hank Kenchington, John Pavek, Scott Mix, Alison Silverstein	Michael Innocenzo Ken Hall	Roger Lampila	Gerry Cauley

Role Descriptions for CIPC Working Groups and Task Forces

Chair:
1. Provide overall leadership to define scope, deliverables, milestones and resource requirements.
2. Seek the active involvement of CIPC participants.
3. Assign tasks to participants.
4. Schedule and conduct meetings.
5. Provide periodic updates to CIPC and early notice of missed milestones or deliverables.

Vice-Chair:
1. In the absence of the Chair, assume the Chair role.
2. Take on specific Chair tasks, as delegated by the Chair.

Executive Committee (EC) Sponsor:
1. Act as a single point-of-contact to the CIPC Executive Committee.
2. Provide support and guidance to the Chair to ensure that deliverables are consistent with CIPC's policy direction and work plan.
3.

NERC Staff:
1. Arrange meeting facilities such as physical space or conference calls.
2. Provide administrative support.

CIPC Working Group/Task Force

Deliverables and Work Schedule

CIPC Subcommittee:	ESISAC
Working Group/Task Force Name:	Outreach WG

1. Statement of Need

The CIPC, in support of the ESISAC, needs to reach out to the Electricity Sector (ES) to promote the need for Critical Infrastructure Protection (CIP); to promote and support the use of the CIPC's products and services; and to encourage two way communications on CIP topics. The Outreach WG of the ESISAC Subcommittee will be the lead group for this effort.

2. Background

The CIPC is the organization within NERC to: promote the ESISAC and its role with Governments' and other critical infrastructure industries: promulgate CIPC sponsored products and services; provide the communications and training needed to ensure those products and services are used properly; and to interact with ES participants, directly or indirectly, to ensure that said products and services are being adequately deployed, used, and maintained. The CIPC has formed the Outreach WG of the ESISAC Subcommittee to lead this effort through the following Objectives and Deliverables.

3. Objectives

- Publicize training materials and delivery mechanisms through
  - Workshops
  - Speakers bureau
  - Session opportunities at industry meetings
  - Consider sponsorship of a major conference
- Sponsor and work with CIPC-like groups in each NERC Region
- Develop a means to assure that CIP concepts and programs are driven through organizations
- Develop and distribute newsletters and other appropriate information
- Interface between the work of the CIPC and the membership within the ES

4. Members and Structure

	Name / RRO	Tel	Email
Chair	Wally Johnson / MAAC	1-301-469-5252	wajohnson@pepco.com
Vice-Chair	TBD		
EC Sponsor	Bob Canada / SERC	1-404-506-5145	rdcanaca@southernco.com
NERC staff	Lou Leffler	1-609-452-8060	Lou.leffler@nerc.net
Physical	Mike Lynch / ECAR	1-313-235-7733	lynchm@dteenergy.com
	Larry Dolci / SPP	1-816-654-1661	larry.dolci@kcpl.com
Cyber	Brian Hogue / NPCC	1-212-840-1070	bhogue@npcc.org
	Brian Malfant / FRCC	1-813-289-5644	bmalfant@frcc.com
Operations	Chris Uranga / ERCOT	1-512-248-3036	curanga@ercot.com
	Thomas Glock / WECC	1-602-250-1160	thomas.glock@aps.com

		Eric Solberg / MAIN	1-262-506-6746	esolberg@atcllc.com
		Allen Klassen / SPP	1-785575-6073	Allen_Klassen@wr.com
	Policy			
	Government	Paul Carrier	202-282-8696	paul.carrier@hq.dhs.gov

5. Deliverables and Work Schedule

1. Review existing Library of CIPC products and organize for better access and use.
   - Catalog by 7/1/04 & recommend revised library access by 9/1/04
2. Establish RRO CIP organizations or liaison & build Regional email exploders for CIP
   - RRO org. / liaison by 7/1/04 & email exploders available for sign up by 12/1/04
3. Explore Communications concepts
   - Develop concepts by 6/1/04 & develop business plan by 8/1/04 for 2005 budgeting
4. Establish Speakers Bureau and workshop planning organization
   - Set up speakers list by 5/1/04 & workshop planning structure by 10/1/04

6. References and Resources

North American Electric Reliability Council

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Revision 1

CIPC Working Group/Task Force

Deliverables and Work Schedule

CIPC Subcommittee:	**ES-ISAC**
Working Group/Task Force Name:	**Reporting Technologies Working Group** (formerly Real-Time Reporting Working Group)

1. Statement of Need

A common set of technologies is needed to allow various reporting requirements to be integrated and communicated to appropriate entities in a similar manner. The integration would allow the information for a report to be submitted once and automated to support various report requirements.

2. Background

Various methodologies have evolved over the years to facilitate the timely transmittal of information to interested entities. As newer communications technologies have matured to gain widespread use, the reporting methodologies have evolved to employ these technologies to allow more accurate and timely reporting. Today, a combination of mail, facsimile, E-mail, Internet web page entries and other technologies are used to convey information to the intended recipient(s). The diversity in reporting mechanisms has resulted in disjointed and separate processes for reporting the same information to multiple entities.

3. Objectives

- Coordinate efforts with the IAW Working Group to identify specific reporting requirements.
- Inventory the various systems and processes used to file various industry/government reports, specifically including the Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) / Indications, Analysis & Warning (IAW) and Department of Energy's EIA-417 reports.
- Identify common technologies employed to submit information to report recipients. (Filing reports)
- Identify common technologies that would facilitate accurate and timely dissemination of information to key recipients. (Receiving alerts and notifications)
- Assess technologies and determine optimum facilities to employ for submission of reports as well as technologies widely used that can be used to broadcast information to key recipients.

4. Members and Structure

	Name	Tel	Email
Chair	Carl J. Eng (Operations)	(804) 273-3305	Carl_eng@dom.com

Vice-Chair			
EC Sponsor	Jamey Sample (Cyber)	(916) 608-5891	jsample@caiso.com
NERC staff	Lynn Costantini	(609) 452-8060	Lynn.costantini@nerc.net
Physical	Robert Windus	(503) 230-5148	rlwindus@bpa.gov
	Frank Prieto	(305) 442-5804	frank_prieto@fpl.com
Cyber			
Operations	Dave Baumken	(416) 345-4009	David.baumken@hydroone.com
	Thomas Glock	(602) 250-1160	Thomas.glock@aps.com
	Allen Klassen	(785) 575-6073	Allen_klassen@wr.com
	Steve Myers	(512) 248-3077	smyers@ercot.com
	Jean-Guy Ouimet	(450) 565-2210 x2232	ouimet.jean-guy@hydro.qc.ca
	Eric Solberg	(262) 506-6746	esolberg@atcllc.com
Policy			
Government	Hank Kenchington		Henry.Kenchington@hq.doe.gov
	Ted Heller		hellerfp@nswc.navy.mil
	Paul Carrier		pcarrier@mitre.org
Other	Scott Mix	(215) 682-7938	smix@epri.com
	Joe Weiss	(408) 253-7934	jweiss@kemaconsulting.com

5. Deliverables and Work Schedule

-

6. References and Resources

- DOE EIA-417 Report and instructions → http://www.eia.doe.gov/oss/forms.html#eia-417
- IAW Standard Operating Procedure → http://www.esisac.com/publicdocs/IAW_SOP.pdf
- IAW Information Flow Diagram → http://www.esisac.com/publicdocs/IAW-information-flow-diagram.PDF

CIPC Analysis Working Group

Statement of Need: Anticipate and/or React to potential threats

Make recommendations for improvements to reduce the likelihood and severity of terrorist and criminal acts for consideration by federal authorities based on the nature of the threat, process vulnerabilities, possible consequences, and existing security measures and safeguards.

Objective: Comprehensive evaluation of US and Internet threat conditions and detailed analysis tailored for the electricity sector.

- Conduct industry threat analysis
- Analyze collected events from local and federal authorities.
- Notify industry of events that could potentially impact the security of this critical infrastructure.
    - Current and forecast threat information and alert conditions
    - Daily, Vulnerability and Alert notifications
    - Detailed Trending and Attack Metrics
    - Analysis and correlation of security threats by local and federal authorities

Threat analysis is the first step in risk assessment for deliberate and unintentional acts. It is used to identify the sources and types of threats and their likelihood of impact to the electricity sector.

Once specific threats have been identified, process vulnerability analysis is used to identify threat scenarios, i.e. SCADA impact. The results of the analysis are used to assist in making decisions on the levels of safeguards that are needed.

North American Electric Reliability Council

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

CIPC Working Group/Task Force

Deliverables and Work Schedule

CIPC Subcommittee:	ISAC SC, Analysis WG
Working Group/Task Force Name:	IDS Pilot TF

1. Statement of Need

The electricity sector does not currently share intrusion attack information, and cannot assess whether such attacks may be specifically targeted against the electricity sector. The results of this pilot will be used to assess individual ISO capabilities, explore methods to detect whether attacks may be specifically targeted and develop methodologies that may be useful to support ISAC analysis capability.

2. Background

All entities that provide or receive information via the internet should have effective Intrusion Detection Systems in place to monitor and prevent malicious access. This pilot project is intended to determine the extent to which such attacks may be targeted any more or less to the electricity sector.

3. Objectives

- Define common lexicon for attack methods, profiles and metrics
- Detect and classify intrusion attempts from ISO- and Contractor-installed IDS sensors
- Compare attack profiles (eg. ISO versus other ISOs, ISOs versus other sectors)

4. Members and Structure (limited to ISOs only at this time, for data confidentiality reasons)

	Name	Tel	Email
Chair	Stuart Brindley		
Vice-Chair			
EC Sponsor	Stuart Brindley		
NERC staff			
Physical			
Cyber	Jamey Sample, Cal-ISO		
	Chuck Noble, ISO-NE		
	Chris Urunga, ERCOT		

		Roger Lampila, NY-ISO
		John Maguire, PJM
		Jim Orcheson, IMO
	Operations	
	Policy	
	Government	Paul Carrier, DHS

5. Deliverables and Work Schedule

- Finalize participation (Feb-04)
- Determine data requirements and install sensors (Jun-04)
- Gather and analyze data (Sep-04)
- Issue final report (Jan-05)

6. References and Resources

CIPC Working Group/Task Force

Deliverables and Work Schedule

CIPC Subcommittee: ES-ISAC

Working Group/Task Force Name: IAW WG

1. Statement of Need

As the electric industry develops and matures its CIP measures, existing programs need continual review for appropriateness and need. The IAW SOP has been in effect for several years while additional/modified reporting requirements have evolved. Reporting requirements to other agencies should be integrated into a common format, where possible.

2. Background

The Indications and Analysis program has been in effect for several years. During this time, several changes have occurred in reporting requirements and mechanisms.

3. Objectives

- Conduct a thorough review of the Indications, Analysis, & Warnings Program (IAW) Standard Operating Procedure.
  - Review the current IAW program for appropriateness.
  - Review other cyber/physical security reporting requirements applicable to the ES.
  - Develop proposed modifications to the IAW SOP to reflect new reporting requirements and improved reporting mechanisms.
  - Work with the Real-Time Reporting WG to develop necessary communications mechanisms.

4. Members and Structure

	Name	Tel	Email
Chair	Larry Bugh		larryb@ecar.org
Vice-Chair			
EC Sponsor	Roger Lampilla		rlampila@nyiso.com
NERC staff	Lynn Costantini		lynn.costantini@nerc.net
Physical	Bob Beahm, Bob Windus		robert.h.beahm@bge.com, rlwindus@bpa.gov
Cyber			
Operations	Allen Klassen		allen_klassen@wr.com
Policy			
Government	Kara Yorke, Ted Heller, Paul Carrier		kara.yorke@ocipep-bpiepc.gc.ca
Other/Vendor	Tom Kropp		

5. Deliverables and Work Schedule

- Prepare an updated IAW SOP

- Coordinate with the Real-Time Reporting WG on

6. References and Resources

Current IAW SOP

North American Electric Reliability Council

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

CIPC Working Group/Task Force

Deliverables and Work Schedule

CIPC Subcommittee:	Security Planning
Working Group/Task Force Name:	Standards & Guidelines Working Group

1. Statement of Need

As part of the Official CIPC Scope, specifically activity items seven and eight, the Standards & Guidelines Working Group exists to coordinate the drafting, review, editing, publishing, and promotion of standards, guidelines, and electric industry opinions as it related to critical infrastructure protection (CIP).

2. Background

The Standards & Guidelines Working Group is tasked to review existing CIPC guidelines, and other electric and non-electric industry standards and guidelines, for currency and relevance; to coordinate the drafting, review, editing, publishing, and promotion of new standards and guidelines; to coordinate the review of non-CIPC NERC standards in draft for security concerns and provide coordinated responses; and to communicate the value of CIPC publications to the CIPC community through the ESISAC's outreach program.

3. Objectives

- Coordinate CIPC comments on NERC standards, SARs, and guidelines to provide appropriate CIP perspective.
- Review existing CIPC security standards and guidelines and risk objectives produced by the Risk Assessment Working Group; develop a prioritized list of standards revisions and new standards and guidelines necessary to meet risk objectives.
- Develop and implement a schedule to review and comment on other security focused electric and non-electric industry standards & guidelines.
- Liaise with outreach programs to inform and educate on standards and guidelines.

4. Members and Structure

	Name	Tel	Email
Chair	John Maguire	610-666-4420	maguij@pjm.com
EC Sponsor	Pat Laird	312-394-8553	patrick.laird@exeloncorp.com
NERC staff	Lou Leffler	609-452-8060	lou.leffler@nerc.net
	Lynn Constantini	609-452-8060	lynn.costantini@nerc.

net

Physical	Michael Lynch
	Scott Webber
	Scott McCoy
	Bruce Metruck
	Robert L. Sypult
	Lyman H. Shaffer
	John Pavek
Cyber	Larry Bugh
	Frank Dessuit
	Jerry Freese
	Linda Nappier
	Kurt Muehlbauer
	Chuck Noble
	Jay Cribb
	Joe Doetzl
	Tim Deloach
	Seiki Harada
Operations	Roger Lampila
Other	Joe Weiss
	Sandy Brewer
	Tom Kropp
	Ken Hall
Government	Elizabeth Rhodenizer

5. Deliverables and Work Schedule

- Coordinate and aggregate CIPC comments on NERC standards, SARs, and guidelines to provide appropriate CIP perspective.
    - Determine whether NERC document requires a CIPC review within ten business days of NERC document's release for comment.
    - Coordinate response within two weeks of the end of any comment period.
    - Start with the proposed permanent Cyber Security Standard, immediately.
- Review existing, and coordinate the development of new, CIPC security guidelines
    - Determine a list of the top five guidelines that should be created in 2004, by March 2004.
    - Coordinate development of one guideline every other month, starting March 2004.
    - Determine a list of the top ten guidelines that need to be reviewed and revised in 2004, by February 2004.
    - Review one guideline each month, starting February 2004.
    - Revise SGWG "top ten" list per the highest priorities produced by the Risk Assessment Working Group, when publicly available.
- Develop a schedule to review and comment on non-CIPC, security focused, electric and non-electric industry standards & guidelines.
    - Prepare a monthly list of the top five security focused electric and non-electric

industry standards, guidelines, rules, orders, etc. to be considered for review.
    - Start with EEI guideline(s) on patch management, immediately.
- Liaise with ESISAC outreach group to inform and educate on existing and proposed standards and guidelines, as necessary.

6. References and Resources

http://www.esisac.com/library-guidelines.htm

http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

North American Electric Reliability Council

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

CIPC Working Group/Task Force

Deliverables and Work Schedule

CIPC Subcommittee:	**Security Planning**
Working Group/Task Force Name:	**Process Control System Security Task Force**

1. Statement of Need

Develop a plan to secure process control systems in collaboration with vendors and relevant industry and government organizations.

2. Background

Process Control Systems are the "brains" of the control and monitoring of the bulk electric system and other critical infrastructures, but they were designed for functionality and performance, not security. Most Process Control Systems assume an environment of complete and implicit trust. The PCSS TF is charged with working with other appropriate organizations to develop economical procedures to apply security into existing systems; as well as to look forward to have security built into newly designed or delivered systems. In addition, the PCSS TF looks at Control System specific issues, such as patch installation and management, which cannot be blindly adopted from traditional IT methodologies.

3. Objectives

- Work with NERC groups, other industry groups, vendors and government to enhance their understanding of security issues within Process Control Systems
- Work with utilities, vendors, consultants, and government organizations including those with process control system test beds to identify and implement appropriate security technology and guidelines, both for existing and future implementations

4. Members and Structure

	Name	Tel	Email
Chair	Scott R. Mix	(215) 682-7938	smix@epri.com
Vice-Chair			
EC Sponsor	Jamey Sample (Cyber)	(916) 608-5891	jsample@caiso.com
NERC staff	Lou Leffler	(609) 452-8060	Lou.Leffler@nerc.net
Physical	Ron Belval Jim Miller		

Cyber	Franklin Dessuit Linda Nappier Tom Flowers Bob Richhart Homer Cotton Jerry Freese Sergio Guzman Martin Morgan John Maguire Tim DeLoach Dave Norton Scott Boyer Rishi Tripathi
Operations	
Policy	
Government	Ted Heller Paul Carrier Jeff Dagle Hank Kenchington Abbie Layne Mike Peters Roman Shaffer
Other	Joe Weiss Tom Kropp Mark Bruen Judith Harris Al Tardiff

5. Deliverables and Work Schedule

- Work with Planning Committee (?) to complete the Time Synchronization guideline document as one of a set of documents to fulfill Blackout Recommendation #12b.
- Review and propose updates to the DOE 21 Step document. Develop one to two new Security Guidelines based on topics contained in the DOE 21 Steps document. These documents will aid in the implementation of specific items called out in the 21 steps document.
- Establish top “ten” PCS vulnerabilities (based on bulk electric system impact) and remediations, based on PCSSTF judgement. (Hank Kenchington)
- Establish top generic PCS architectures, based on PCSSTF judgement.
- Maintain a relationship with the Risk Assessment Working Group to ensure that security is implemented commensurate with the risk to be avoided.
- Develop a Security Guideline to provide physical protection for unstaffed facilities. (Tom Flowers team)
- Promote establishment of CERT type information sharing for control systems. (ESISAC)

6. References and Resources

North American Electric Reliability Council

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

DRAFT Rev .01

CIPC Working Group/Task Force

Deliverables and Work Schedule

CIPC Subcommittee:	**Security Planning Sub-Committee**
Working Group/Task Force Name:	**Risk Assessment WG**

1. Statement of Need

CIPC needs to encourage the development of risk assessment capability within the ES industry and, support and guide risk assessments performed by government or academic entities.

2. Background

Risk assessment is a primary component of CIP and the CIPC needs to ensure that credible risk assessments are conducted properly and cover all aspects of the ES. Although many different and diverse industry and government entities are performing risk assessment analyses on various aspects of the electricity sector, there is little or no coordination between these entities, resulting in duplication of efforts and possible leaving gaps in the analyses.

3. Objectives

- Interface with government entities performing risk assessments on the ES and help guide, direct, or influence these assessment efforts.
- Review risk assessment analyses and vulnerability exercises and provide "Lessons Learned" as appropriate.
- Assess current threat situation and trend.
- Establish metrics for assessing vulnerability of the ES and establish the ability to track the vulnerability trend in the future.
- Assess effectiveness of physical protection measures.
- Identify risk assessment methodologies.
- Provide input and material regarding risk assessments for Standards and Guidelines as appropriate.

4. Members and Structure

	Name	Tel	Email
Chair	Ted Heller	540-653-2929	hellerfp@nswc.navy.mil
Vice-Chair	Scott McCoy	612-330-7666	richard.d.mccoy@xcelenergy.com
EC Sponsor	Pat Laird	312-394-8553	patrick.laird@exeloncorp.com

NERC staff	Gerry Cauley	727-360-2399	gcauley@nerc.com
Physical	Bob Windus	503-230-5148	rlwindus@bpa.gov
	Bob Beahm	410-597-7777	robert.h.beahm@bge.com
	Lyman Shaffer	415-973-6920	LHS1@pge.com
	Bob Sypult	626-302-7910	Robert.Sypult@sce.com
Cyber	Tom Flowers	713-207-2122	tom.flowers@centerpointenergy.com
Operations	Len Januzik	630-261-2611	lrj@maininc.org
Policy	Jean-Guy Ouimet	450-565-2210 x2232	ouimet.jean-guy@hydro.qc.ca
	Ken Hall	202-508-5172	khall@eei.org
Government/Others	Hank Kenchington	202-586-1878	henry.kenchington@hq.doe.gov
	Jim McGlone	202-586-1287	james.mcglone@hq.doe.gov
	Paul Carrier	202-282-8696	paul.carrier@hq.dhs.gov
	Michael Cohen	202-282-8695	Michael.Cohen@hq.dhs.gov
	Bill Flynt	816-474-1500	bill.flynt@trcsolutions.com

5. Deliverables and Work Schedule

TBE

6. References and Resources

To be completed

August 14, 2003 Blackout: NERC Actions to Prevent and Mitigate the Impacts of Future Cascading Blackouts
February 10, 2004

Preamble

The Board of Trustees recognizes the paramount importance of a reliable bulk electric system in North America. In consideration of the findings of the investigation into the August 14, 2003 blackout, NERC must take firm and immediate actions to increase public confidence that the reliability of the North American bulk electric system is being protected.

A key finding of the blackout investigators is that violations of existing NERC reliability standards contributed directly to the blackout. Pending enactment of federal reliability legislation creating a framework for enforcement of mandatory reliability standards, and with the encouragement of the Stakeholders Committee, the board is determined to obtain full compliance with all existing and future reliability standards and intends to use all legitimate means available to achieve that end. The board therefore resolves to:

- *Receive specific information on all violations of NERC standards, including the identities of the parties involved;*
- *Take firm actions to improve compliance with NERC reliability standards;*
- *Provide greater transparency to violations of standards, while respecting the confidential nature of some information and the need for a fair and deliberate due process; and*
- *Inform and work closely with the Federal Energy Regulatory Commission and other applicable federal, state, and provincial regulatory authorities in the United States, Canada, and Mexico as needed to ensure public interests are met with respect to compliance with reliability standards.*

The board expresses its appreciation to the blackout investigators and the Steering Group for their objective and thorough work in preparing a report of recommended NERC actions. With a few clarifications, the board approves the report and directs implementation of the recommended actions. The board holds the assigned committees and organizations accountable to report to the board the progress in completing the recommended actions, and intends itself to publicly report those results. The board recognizes the possibility that this action plan may have to be adapted as additional analysis is completed, but stresses the need to move forward immediately with the actions as stated.

Furthermore, the board directs management to immediately advise the board of any significant violations of NERC reliability standards, including details regarding the nature and potential reliability impacts of the alleged violations and the identity of parties involved. Management shall supply to the board in advance of board meetings a detailed report of all violations of reliability standards.

Finally, the board resolves to form a task force to develop guidelines for the board to consider with regard to the confidentiality of compliance information and disclosure of such information to regulatory authorities and the public.

Overview of Investigation Conclusions

The North American Electric Reliability Council (NERC) has conducted a comprehensive investigation of the August 14, 2003 blackout. The results of NERC's investigation contributed significantly to the U.S./Canada Power System Outage Task Force's November 19, 2003 Interim Report identifying the root causes of the outage and the sequence of events leading to and during the cascading failure. NERC fully concurs with the conclusions of the Interim Report and continues to provide its support to the Task Force through ongoing technical analysis of the outage. Although an understanding of what happened and why has been resolved for most aspects of the outage, detailed analysis continues in several areas, notably dynamic simulations of the transient phases of the cascade and a final verification of the full scope of all violations of NERC and regional reliability standards that occurred leading to the outage.

From its investigation of the August 14 blackout, NERC concludes that:

- Several entities violated NERC operating policies and planning standards, and those violations contributed directly to the start of the cascading blackout.
- The existing process for monitoring and assuring compliance with NERC and regional reliability standards was shown to be inadequate to identify and resolve specific compliance violations before those violations led to a cascading blackout.
- Reliability coordinators and control areas have adopted differing interpretations of the functions, responsibilities, authorities, and capabilities needed to operate a reliable power system.
- Problems identified in studies of prior large-scale blackouts were repeated, including deficiencies in vegetation management, operator training, and tools to help operators better visualize system conditions.
- In some regions, data used to model loads and generators were inaccurate due to a lack of verification through benchmarking with actual system data and field testing.
- Planning studies, design assumptions, and facilities ratings were not consistently shared and were not subject to adequate peer review among operating entities and regions.
- Available system protection technologies were not consistently applied to optimize the ability to slow or stop an uncontrolled cascading failure of the power system.

Overview of Recommendations

The Board of Trustees approves the NERC Steering Group recommendations to address these shortcomings. The recommendations fall into three categories.

Actions to Remedy Specific Deficiencies: Specific actions directed to First Energy (FE), the Midwest Independent System Operator (MISO), and the PJM Interconnection, LLC (PJM) to correct the deficiencies that led to the blackout.

1. Correct the Direct Causes of the August 14, 2003 Blackout.

Strategic Initiatives: Strategic initiatives by NERC and the regional reliability councils to strengthen compliance with existing standards and to formally track completion of recommended actions from August 14, and other significant power system events.

2. Strengthen the NERC Compliance Enforcement Program.
3. Initiate Control Area and Reliability Coordinator Reliability Readiness Audits.
4. Evaluate Vegetation Management Procedures and Results.
5. Establish a Program to Track Implementation of Recommendations.

Technical Initiatives: Technical initiatives to prevent or mitigate the impacts of future cascading blackouts.

6. Improve Operator and Reliability Coordinator Training
7. Evaluate Reactive Power and Voltage Control Practices.
8. Improve System Protection to Slow or Limit the Spread of Future Cascading Outages.
9. Clarify Reliability Coordinator and Control Area Functions, Responsibilities, Capabilities and Authorities.
10. Establish Guidelines for Real-Time Operating Tools.
11. Evaluate Lessons Learned During System Restoration.
12. Install Additional Time-Synchronized Recording Devices as Needed.
13. Reevaluate System Design, Planning and Operating Criteria.
14. Improve System Modeling Data and Data Exchange Practices.

Market Impacts

Many of the recommendations in this report have implications for electricity markets and market participants, particularly those requiring reevaluation or clarification of NERC and regional standards, policies and criteria. Implicit in these recommendations is that the NERC board charges the Market Committee with assisting in the implementation of the recommendations and interfacing with the North American Energy Standards Board with respect to any necessary business practices.

Recommendation to Remedy Specific Deficiencies

Recommendation 1. Correct the Direct Causes of the August 14, 2003 Blackout.

NERC's technical analysis of the August 14 blackout leads it to fully concur with the Task Force Interim Report regarding the direct causes of the blackout. The report stated that the principal causes of the blackout were that FE did not maintain situational awareness of conditions on its power system and did not adequately manage tree growth in its transmission rights-of-way. Contributing factors included ineffective diagnostic support provided by MISO as the reliability coordinator for FE and ineffective communications between MISO and PJM.

NERC will take immediate and firm actions to ensure that the same deficiencies that were directly causal to the August 14 blackout are corrected. These steps are necessary to assure electricity customers, regulators and others with an interest in the reliable delivery of electricity that the power system is being operated in a manner that is safe and reliable, and that the specific causes of the August 14 blackout have been identified and fixed.

Recommendation 1a: FE, MISO, and PJM shall each complete the remedial actions designated in Attachment A for their respective organizations and certify to the NERC board no later than June 30, 2004, that these specified actions have been completed. Furthermore, each organization shall present its detailed plan for completing these actions to the NERC committees for technical review on March 23-24, 2004, and to the NERC board for approval no later than April 2, 2004.

Recommendation 1b: The NERC Technical Steering Committee shall immediately assign a team of experts to assist FE, MISO, and PJM in developing plans that adequately address the issues listed in Attachment A, and other remedial actions for which each entity may seek technical assistance.

Strategic Initiatives to
Assure Compliance with Reliability Standards and to Track Recommendations

Recommendation 2. Strengthen the NERC Compliance Enforcement Program.

NERC's analysis of the actions and events leading to the August 14 blackout leads it to conclude that several violations of NERC operating policies contributed directly to an uncontrolled, cascading outage on the Eastern Interconnection. NERC continues to investigate additional violations of NERC and regional reliability standards and expects to issue a final report of those violations in March 2004.

In the absence of enabling legislation in the United States and complementary actions in Canada and Mexico to authorize the creation of an electric reliability organization, NERC lacks legally sanctioned authority to enforce compliance with its reliability rules. However, the August 14 blackout is a clear signal that voluntary compliance with reliability rules is no longer adequate. NERC and the regional reliability councils must assume firm authority to measure compliance, to more transparently report significant violations that could risk the integrity of the interconnected power system, and to take immediate and effective actions to ensure that such violations are corrected.

Violations of NERC standards identified in the November 19, 2003 Interim Report:

1. Following the outage of the Chamberlin-Harding 345 kV line, FE did not take the necessary actions to return the system to a safe operating state within 30 minutes (violation of NERC Operating Policy 2).
2. FE did not notify other systems of an impending system emergency (violation of NERC Operating Policy 5).
3. FE's analysis tools were not used to effectively assess system conditions (violation of NERC Operating Policy 5).
4. FE operator training was inadequate for maintaining reliable conditions (violation of NERC Operating Policy 8).
5. MISO did not notify other reliability coordinators of potential problems (violation of NERC Operating Policy 9).

Recommendation 2a: Each regional reliability council shall report to the NERC Compliance Enforcement Program within one month of occurrence all significant[1] violations of NERC operating policies and planning standards and regional standards, whether verified or still under investigation. Such reports shall confidentially note details regarding the nature and potential reliability impacts of the alleged violations and the identity of parties involved. Additionally, each regional reliability council shall report quarterly to NERC, in a format prescribed by NERC, all violations of NERC and regional reliability council standards.

Recommendation 2b: Being presented with the results of the investigation of any significant violation, and with due consideration of the surrounding facts and circumstances, the NERC board shall require an offending organization to correct the violation within a specified time. If the board determines that an offending organization is non-responsive and continues to cause a risk to the reliability of the interconnected power systems, the board will seek to remedy the violation by requesting assistance of the appropriate regulatory authorities in the United States, Canada, and Mexico.

[1] Although all violations are important, a significant violation is one that could directly reduce the integrity of the interconnected power systems or otherwise cause unfavorable risk to the interconnected power systems. By contrast, a violation of a reporting or administrative requirement would not by itself generally be considered a significant violation.

Recommendation 2c: The Planning and Operating Committees, working in conjunction with the Compliance Enforcement Program, shall review and update existing approved and draft compliance templates applicable to current NERC operating policies and planning standards; and submit any revisions or new templates to the board for approval no later than March 31, 2004. To expedite this task, the NERC President shall immediately form a Compliance Template Task Force comprised of representatives of each committee. The Compliance Enforcement Program shall issue the board-approved compliance templates to the regional reliability councils for adoption into their compliance monitoring programs.

This effort will make maximum use of existing approved and draft compliance templates in order to meet the aggressive schedule. The templates are intended to include all existing NERC operating policies and planning standards but can be adapted going forward to incorporate new reliability standards as they are adopted by the NERC board for implementation in the future.

When the investigation team's final report on the August 14 violations of NERC and regional standards is available in March, it will be important to assess and understand the lapses that allowed violations to go unreported until a large-scale blackout occurred.

Recommendation 2d: The NERC Compliance Enforcement Program and ECAR shall, within three months of the issuance of the final report from the Compliance and Standards investigation team, evaluate the identified violations of NERC and regional standards, as compared to previous compliance reviews and audits for the applicable entities, and develop recommendations to improve the compliance process.

Recommendation 3. Initiate Control Area and Reliability Coordinator Reliability Readiness Audits.

In conducting its investigation, NERC found that deficiencies in control area and reliability coordinator capabilities to perform assigned reliability functions contributed to the August 14 blackout. In addition to specific violations of NERC and regional standards, some reliability coordinators and control areas were deficient in the performance of their reliability functions and did not achieve a level of performance that would be considered acceptable practice in areas such as operating tools, communications, and training. In a number of cases there was a lack of clarity in the NERC policies with regard to what is expected of a reliability coordinator or control area. Although the deficiencies in the NERC policies must be addressed (see Recommendation 9), it is equally important to recognize that standards cannot prescribe all aspects of reliable operation and that minimum standards present a threshold, not a target for performance. Reliability coordinators and control areas must perform well, particularly under emergency conditions, and at all times strive for excellence in their assigned reliability functions and responsibilities.

Recommendation 3a: The NERC Compliance Enforcement Program and the regional reliability councils shall jointly establish a program to audit the reliability readiness of all reliability coordinators and control areas, with immediate attention given to addressing the deficiencies identified in the August 14 blackout investigation. Audits of all control areas and reliability coordinators shall be completed within three years and continue in a three-year cycle. The 20 highest priority audits, as determined by the Compliance Enforcement Program, will be completed by June 30, 2004.

Recommendation 3b: NERC will establish a set of baseline audit criteria to which regional criteria may be added. The control area requirements will be based on the existing NERC Control Area Certification Procedure. Reliability coordinator audits will include evaluation of reliability plans, procedures, processes, tools, personnel qualifications, and training. In addition to reviewing written documents, the audits will carefully examine the actual practices and preparedness of control areas and reliability coordinators.

Recommendation 3c: The reliability regions, with the oversight and direct participation of NERC, will audit each control area's and reliability coordinator's readiness to meet these audit criteria. FERC and other relevant regulatory agencies will be invited to participate in the audits, subject to the same confidentiality conditions as the other members of the audit teams.

Recommendation 4. Evaluate Vegetation Management Procedures and Results.

Ineffective vegetation management was a major cause of the August 14 blackout and also contributed to other historical large-scale blackouts, such on July 2-3, 1996 in the west. Maintaining transmission line rights-of-way (ROW), including maintaining safe clearances of energized lines from vegetation, under-build, and other obstructions[2] incurs a substantial ongoing cost in many areas of North America. However, it is an important investment for assuring a reliable electric system.

NERC does not presently have standards for ROW maintenance. Standards on vegetation management are particularly challenging given the great diversity of vegetation and growth patterns across North America. However, NERC's standards do require that line ratings are calculated so as to maintain safe clearances from all obstructions. Furthermore, in the United States, the National Electrical Safety Code (NESC) Rules 232, 233, and 234 detail the minimum vertical and horizontal safety clearances of overhead conductors from grounded objects and various types of obstructions. NESC Rule 218 addresses tree clearances by simply stating, "Trees that may interfere with ungrounded supply conductors should be trimmed or removed." Several states have adopted their own electrical safety codes and similar codes apply in Canada.

Recognizing that ROW maintenance requirements vary substantially depending on local conditions, NERC will focus attention initially on measuring performance as indicated by the number of high voltage line trips caused by vegetation rather than immediately move toward developing standards for

[2] Vegetation, such as the trees that caused the initial line trips in FE that led to the August 14, 2003 outage is not the only type of obstruction that can breach the safe clearance distances from energized lines. Other examples include under-build of telephone and cable TV lines, train crossings, and even nests of certain large bird species.

ROW maintenance. This approach has worked well in the Western Electricity Coordinating Council (WECC) since being instituted after the 1996 outages.

Recommendation 4a: NERC and the regional reliability councils shall jointly initiate a program to report all bulk electric system[3] transmission line trips resulting from vegetation contact[4]. The program will use the successful WECC vegetation monitoring program as a model.

Recommendation 4b: Beginning with an effective date of January 1, 2004, each transmission operator will submit an annual report of all vegetation-related high voltage line trips to its respective reliability region. Each region shall assemble a detailed annual report of vegetation-related line trips in the region to NERC no later than March 31 for the preceding year, with the first reporting to be completed by March 2005 for calendar year 2004.

Vegetation management practices, including inspection and trimming requirements, can vary significantly with geography. Additionally, some entities use advanced techniques such as planting beneficial species or applying growth retardants. Nonetheless, the events of August 14 and prior outages point to the need for independent verification that viable programs exist for ROW maintenance and that the programs are being followed.

Recommendation 4c: Each bulk electric transmission owner shall make its vegetation management procedure, and documentation of work completed, available for review and verification upon request by the applicable regional reliability council, NERC, or applicable federal, state or provincial regulatory agency.

Should this approach of monitoring vegetation-related line outages and procedures prove ineffective in reducing the number of vegetation-related line outages, NERC will consider the development of minimum line clearance standards to assure reliability.

Recommendation 5. Establish a Program to Track Implementation of Recommendations.

The August 14 blackout shared a number of contributing factors with prior large-scale blackouts, including:

- Conductors contacting trees
- Ineffective visualization of power system conditions and lack of situational awareness
- Ineffective communications
- Lack of training in recognizing and responding to emergencies
- Insufficient static and dynamic reactive power supply
- Need to improve relay protection schemes and coordination

[3] All transmission lines operating at 230 kV and higher voltage, and any other lower voltage lines designated by the regional reliability council to be critical to the reliability of the bulk electric system, shall be included in the program.
[4] A line trip includes a momentary opening and reclosing of the line, a lock out, or a combination. For reporting purposes, all vegetation-related openings of a line occurring within one 24-hour period should be considered one event. Trips known to be caused by severe weather or other natural disaster such as earthquake are excluded. Contact with vegetation includes both physical contact and arcing due to insufficient clearance.

It is important that recommendations resulting from system outages be adopted consistently by all regions and operating entities, not just those directly affected by a particular outage. Several lessons learned prior to August 14, if heeded, could have prevented the outage. WECC and NPCC, for example, have programs that could be used as models for tracking completion of recommendations. NERC and some regions have not adequately tracked completion of recommendations from prior events to ensure they were consistently implemented.

Recommendation 5a: NERC and each regional reliability council shall establish a program for documenting completion of recommendations resulting from the August 14 blackout and other historical outages, as well as NERC and regional reports on violations of reliability standards, results of compliance audits, and lessons learned from system disturbances. Regions shall report quarterly to NERC on the status of follow-up actions to address recommendations, lessons learned, and areas noted for improvement. NERC staff shall report both NERC activities and a summary of regional activities to the board.

Assuring compliance with reliability standards, evaluating the reliability readiness of reliability coordinators and control areas, and assuring recommended actions are achieved will be effective steps in reducing the chances of future large-scale outages. However, it is important for NERC to also adopt a process for continuous learning and improvement by seeking continuous feedback on reliability performance trends, not rely mainly on learning from and reacting to catastrophic failures.

Recommendation 5b: NERC shall by January 1, 2005 establish a reliability performance monitoring function to evaluate and report bulk electric system reliability performance.

Such a function would assess large-scale outages and near misses to determine root causes and lessons learned, similar to the August 14 blackout investigation. This function would incorporate the current Disturbance Analysis Working Group and expand that work to provide more proactive feedback to the NERC board regarding reliability performance. This program would also gather and analyze reliability performance statistics to inform the board of reliability trends. This function could develop procedures and capabilities to initiate investigations in the event of future large-scale outages or disturbances. Such procedures and capabilities would be shared between NERC and the regional reliability councils for use as needed, with NERC and regional investigation roles clearly defined in advance.

Technical Initiatives to Minimize the Likelihood and Impacts of Possible Future Cascading Outages

Recommendation 6. Improve Operator and Reliability Coordinator Training.

NERC found during its investigation that some reliability coordinators and control area operators had not received adequate training in recognizing and responding to system emergencies. Most notable was the lack of realistic simulations and drills for training and verifying the capabilities of operating personnel. This training deficiency contributed to the lack of situational awareness and failure to declare an emergency when operator intervention was still possible prior to the high speed portion of the sequence of events.

Recommendation 6: All reliability coordinators, control areas, and transmission operators shall provide at least five days per year of training and drills in system emergencies, using realistic simulations[5], for each staff person with responsibility for the real-time operation or reliability monitoring of the bulk electric system. This system emergency training is in addition to other training requirements. Five days of system emergency training and drills are to be completed prior to June 30, 2004, with credit given for documented training already completed since July 1, 2003. Training documents, including curriculum, training methods, and individual training records, are to be available for verification during reliability readiness audits.

NERC has published Continuing Education Criteria specifying appropriate qualifications for continuing education providers and training activities.

In the longer term, the NERC Personnel Certification Governance Committee (PCGC), which is independent of the NERC board, should explore expanding the certification requirements of system operating personnel to include additional measures of competency in recognizing and responding to system emergencies. The current NERC certification examination is a written test of the NERC Operating Manual and other references relating to operator job duties, and is not by itself intended to be a complete demonstration of competency to handle system emergencies.

Recommendation 7. Evaluate Reactive Power and Voltage Control Practices.

The August 14 blackout investigation identified inconsistent practices in northeastern Ohio with regard to the setting and coordination of voltage limits and insufficient reactive power supply. Although the deficiency of reactive power supply in northeastern Ohio did not directly cause the blackout, it was a contributing factor and was a significant violation of existing reliability standards.

In particular, there appear to have been violations of NERC Planning Standard I.D.S1 requiring static and dynamic reactive power resources to meet the performance criteria specified in Table I of

[5] The term "realistic simulations" includes a variety of tools and methods that present operating personnel with situations to improve and test diagnostic and decision-making skills in an environment that resembles expected conditions during a particular type of system emergency. Although a full replica training simulator is one approach, lower cost alternatives such as PC-based simulators, tabletop drills, and simulated communications can be effective training aids if used properly.

Planning Standard I.A on Transmission Systems. Planning Standard II.B.S1 requires each regional reliability council to establish procedures for generating equipment data verification and testing, including reactive power capability. Planning Standard III.C.S1 requires that all synchronous generators connected to the interconnected transmission systems shall be operated with their excitation system in the automatic voltage control mode unless approved otherwise by the transmission system operator. S2 of this standard also requires that generators shall maintain a network voltage or reactive power output as required by the transmission system operator within the reactive capability of the units.

On one hand, the unsafe conditions on August 14 with respect to voltage in northeastern Ohio can be said to have resulted from violations of NERC planning criteria for reactive power and voltage control, and those violations should have been identified through the NERC and ECAR compliance monitoring programs (addressed by Recommendation 2). On the other hand, investigators believe these deficiencies are also symptomatic of a systematic breakdown of the reliability studies and practices in FE and the ECAR region that allowed unsafe voltage criteria to be set and used in study models and operations. There were also issues identified with reactive characteristics of loads, as addressed in Recommendation 14.

Recommendation 7a: The Planning Committee shall reevaluate within one year the effectiveness of the existing reactive power and voltage control standards and how they are being implemented in practice in the ten NERC regions. Based on this evaluation, the Planning Committee shall recommend revisions to standards or process improvements to ensure voltage control and stability issues are adequately addressed.

Recommendation 7b: ECAR shall no later than June 30, 2004 review its reactive power and voltage criteria and procedures, verify that its criteria and procedures are being fully implemented in regional and member studies and operations, and report the results to the NERC board.

Recommendation 8. Improve System Protection to Slow or Limit the Spread of Future Cascading Outages.

The importance of automatic control and protection systems in preventing, slowing, or mitigating the impact of a large-scale outage cannot be stressed enough. To underscore this point, following the trip of the Sammis-Star line at 4:06, the cascading failure into parts of eight states and two provinces, including the trip of over 531 generating units and over 400 transmission lines, was completed in the next eight minutes. Most of the event sequence, in fact, occurred in the final 12 seconds of the cascade. Likewise, the July 2, 1996 failure took less than 30 seconds and the August 10, 1996 failure took only 5 minutes. It is not practical to expect operators will always be able to analyze a massive, complex system failure and to take the appropriate corrective actions in a matter of a few minutes. The NERC investigators believe that two measures would have been crucial in slowing or stopping the uncontrolled cascade on August 14:

- Better application of zone 3 impedance relays on high voltage transmission lines
- Selective use of under-voltage load shedding.

First, beginning with the Sammis-Star line trip, most of the remaining line trips during the cascade phase were the result of the operation of a zone 3 relay for a perceived overload (a combination of high amperes and low voltage) on the protected line. If used, zone 3 relays typically act as an overreaching backup to the zone 1 and 2 relays, and are not intentionally set to operate on a line overload. However, under extreme conditions of low voltages and large power swings as seen on August 14, zone 3 relays can operate for overload conditions and propagate the outage to a wider area by essentially causing the system to "break up". Many of the zone 3 relays that operated during the August 14 cascading outage were not set with adequate margins above their emergency thermal ratings. For the short times involved, thermal heating is not a problem and the lines should not be tripped for overloads. Instead, power system protection devices should be set to address the specific condition of concern, such as a fault, out-of-step condition, etc., and should not compromise a power system's inherent physical capability to slow down or stop a cascading event.

Recommendation 8a: All transmission owners shall, no later than September 30, 2004, evaluate the zone 3 relay settings on all transmission lines operating at 230 kV and above for the purpose of verifying that each zone 3 relay is not set to trip on load under extreme emergency conditions[6]. In each case that a zone 3 relay is set so as to trip on load under extreme conditions, the transmission operator shall reset, upgrade, replace, or otherwise mitigate the overreach of those relays as soon as possible and on a priority basis, but no later than December 31, 2005. Upon completing analysis of its application of zone 3 relays, each transmission owner may no later than December 31, 2004 submit justification to NERC for applying zone 3 relays outside of these recommended parameters. The Planning Committee shall review such exceptions to ensure they do not increase the risk of widening a cascading failure of the power system.

A second key finding with regard to system protection was that if an automatic under-voltage load shedding scheme had been in place in the Cleveland-Akron area on August 14, there is a high probability the outage could have been limited to that area.

Recommendation 8b: Each regional reliability council shall complete an evaluation of the feasibility and benefits of installing under-voltage load shedding capability in load centers within the region that could become unstable as a result of being deficient in reactive power following credible multiple-contingency events. The regions are to complete the initial studies and report the results to NERC within one year. The regions are requested to promote the installation of under-voltage load shedding capabilities within critical areas, as determined by the studies to be effective in preventing an uncontrolled cascade of the power system.

The NERC investigation of the August 14 blackout has identified additional transmission and generation control and protection issues requiring further analysis. One concern is that generating unit control and protection schemes need to consider the full range of possible extreme system conditions, such as the low voltages and low and high frequencies experienced on August 14. The team also noted that improvements may be needed in under-frequency load shedding and its coordination with generator under-and over-frequency protection and controls.

[6] The NERC investigation team recommends that the zone 3 relay, if used, should not operate at or below 150% of the emergency ampere rating of a line, assuming a .85 per unit voltage and a line phase angle of 30 degrees.

Recommendation 8c: The Planning Committee shall evaluate Planning Standard III – System Protection and Control and propose within one year specific revisions to the criteria to adequately address the issue of slowing or limiting the propagation of a cascading failure. The board directs the Planning Committee to evaluate the lessons from August 14 regarding relay protection design and application and offer additional recommendations for improvement.

Recommendation 9. Clarify Reliability Coordinator and Control Area Functions, Responsibilities, Capabilities and Authorities.

Ambiguities in the NERC operating policies may have allowed entities involved in the August 14 blackout to make different interpretations regarding the functions, responsibilities, capabilities, and authorities of reliability coordinators and control areas. Characteristics and capabilities necessary to enable prompt recognition and effective response to system emergencies must be specified.

The lack of timely and accurate outage information resulted in degraded performance of state estimator and reliability assessment functions on August 14. There is a need to review options for sharing of outage information in the operating time horizon (e.g. 15 minutes or less), so as to ensure the accurate and timely sharing of outage data necessary to support real-time operating tools such as state estimators, real-time contingency analysis, and other system monitoring tools.

On August 14, reliability coordinator and control area communications regarding conditions in northeastern Ohio were ineffective, and in some cases confusing. Ineffective communications contributed to a lack of situational awareness and precluded effective actions to prevent the cascade. Consistent application of effective communications protocols, particularly during emergencies, is essential to reliability. Alternatives should be considered to one-on-one phone calls during an emergency to ensure all parties are getting timely and accurate information with a minimum number of calls.

NERC operating policies do not adequately specify critical facilities, leaving ambiguity regarding which facilities must be monitored by reliability coordinators. Nor do the policies adequately define criteria for declaring transmission system emergencies. Operating policies should also clearly specify that curtailing interchange transactions through the NERC Transmission Loading Relief (TLR) Procedure is not intended as a method for restoring the system from an actual Operating Security Limit violation to a secure operating state.

Recommendation 9: The Operating Committee shall complete the following by June 30, 2004:

- **Evaluate and revise the operating policies and procedures, or provide interpretations, to ensure reliability coordinator and control area functions, responsibilities, and authorities are completely and unambiguously defined.**
- **Evaluate and improve the tools and procedures for operator and reliability coordinator communications during emergencies.**
- **Evaluate and improve the tools and procedures for the timely exchange of outage information among control areas and reliability coordinators.**

Recommendation 10. Establish Guidelines for Real-Time Operating Tools.

The August 14 blackout was caused by a lack of situational awareness that was in turn the result of inadequate reliability tools and backup capabilities. Additionally, the failure of FE's control computers and alarm system contributed directly to the lack of situational awareness. Likewise, MISO's incomplete tool set and the failure of its state estimator to work effectively on August 14 contributed to the lack of situational awareness.

Recommendation 10: The Operating Committee shall within one year evaluate the real-time operating tools necessary for reliable operation and reliability coordination, including backup capabilities. The Operating Committee is directed to report both minimum acceptable capabilities for critical reliability functions and a guide of best practices.

This evaluation should include consideration of the following:

- Modeling requirements, such as model size and fidelity, real and reactive load modeling, sensitivity analyses, accuracy analyses, validation, measurement, observability, update procedures, and procedures for the timely exchange of modeling data.
- State estimation requirements, such as periodicity of execution, monitoring external facilities, solution quality, topology error and measurement error detection, failure rates including times between failures, presentation of solution results including alarms, and troubleshooting procedures.
- Real-time contingency analysis requirements, such as contingency definition, periodicity of execution, monitoring external facilities, solution quality, post-contingency automatic actions, failure rates including mean/maximum times between failures, reporting of results, presentation of solution results including alarms, and troubleshooting procedures including procedures for investigating unsolvable contingencies.

Recommendation 11. Evaluate Lessons Learned During System Restoration.

The efforts to restore the power system and customer service following the outage were effective, considering the massive amount of load lost and the large number of generators and transmission lines that tripped. Fortunately, the restoration was aided by the ability to energize transmission from neighboring systems, thereby speeding the recovery. Despite the apparent success of the restoration effort, it is important to evaluate the results in more detail to determine opportunities for improvement. Blackstart and restoration plans are often developed through study of simulated conditions. Robust testing of live systems is difficult because of the risk of disturbing the system or interrupting customers. The August 14 blackout provides a valuable opportunity to apply actual events and experiences to learn to better prepare for system blackstart and restoration in the future. That opportunity should not be lost, despite the relative success of the restoration phase of the outage.

Recommendation 11a: The Planning Committee, working in conjunction with the Operating Committee, NPCC, ECAR, and PJM, shall evaluate the black start and system restoration performance following the outage of August 14, and within one year report to the NERC board the results of that evaluation with recommendations for improvement.

Recommendation 11b: All regional reliability councils shall, within six months of the Planning Committee report to the NERC board, reevaluate their procedures and plans to assure an effective blackstart and restoration capability within their region.

Recommendation 12. Install Additional Time-Synchronized Recording Devices as Needed.

A valuable lesson from the August 14 blackout is the importance of having time-synchronized system data recorders. NERC investigators labored over thousands of data items to synchronize the sequence of events, much like putting together small pieces of a very large puzzle. That process would have been significantly improved and sped up if there had been a sufficient number of synchronized data recording devices.

NERC Planning Standard I.F – Disturbance Monitoring does require location of recording devices for disturbance analysis. Often time, recorders are available, but they are not synchronized to a time standard. All digital fault recorders, digital event recorders, and power system disturbance recorders should be time stamped at the point of observation with a precise Global Positioning Satellite (GPS) synchronizing signal. Recording and time-synchronization equipment should be monitored and calibrated to assure accuracy and reliability.

Time-synchronized devices, such as phasor measurement units, can also be beneficial for monitoring a wide-area view of power system conditions in real-time, such as demonstrated in WECC with their Wide-Area Monitoring System (WAMS).

Recommendation 12a: The reliability regions, coordinated through the NERC Planning Committee, shall within one year define regional criteria for the application of synchronized recording devices in power plants and substations. Regions are requested to facilitate the installation of an appropriate number, type and location of devices within the region as soon as practical to allow accurate recording of future system disturbances and to facilitate benchmarking of simulation studies by comparison to actual disturbances.

Recommendation 12b: Facilities owners shall, in accordance with regional criteria, upgrade existing dynamic recorders to include GPS time synchronization and, as necessary, install additional dynamic recorders.

Recommendation 13. Reevaluate System Design, Planning and Operating Criteria.

The investigation report noted that FE entered the day on August 14 with insufficient resources to stay within operating limits following a credible set of contingencies, such as the loss of the East Lake 5 unit and the Chamberlin-Harding line. NERC will conduct an evaluation of operations planning practices and criteria to ensure expected practices are sufficient and well understood. The review will reexamine fundamental operating criteria, such as n-1 and the 30-minute limit in preparing the system for a next contingency, and Table I Category C.3 of the NERC planning standards. Operations planning and operating criteria will be identified that are sufficient to ensure the system is in a known and reliable condition at all times, and that positive controls, whether

manual or automatic, are available and appropriately located at all times to return the Interconnection to a secure condition. Daily operations planning, and subsequent real time operations planning will identify available system reserves to meet operating criteria.

Recommendation 13a: The Operating Committee shall evaluate operations planning and operating criteria and recommend revisions in a report to the board within one year.

Prior studies in the ECAR region did not adequately define the system conditions that were observed on August 14. Severe contingency criteria were not adequate to address the events of August 14 that led to the uncontrolled cascade. Also, northeastern Ohio was found to have insufficient reactive support to serve its loads and meet import criteria. Instances were also noted in the FE system and ECAR area of different ratings being used for the same facility by planners and operators and among entities, making the models used for system planning and operation suspect. NERC and the regional reliability councils must take steps to assure facility ratings are being determined using consistent criteria and being effectively shared and reviewed among entities and among planners and operators.

Recommendation 13b: ECAR shall no later than June 30, 2004 reevaluate its planning and study procedures and practices to ensure they are in compliance with NERC standards, ECAR Document No. 1, and other relevant criteria; and that ECAR and its members' studies are being implemented as required.

Recommendation 13c: The Planning Committee, working in conjunction with the regional reliability councils, shall within two years reevaluate the criteria, methods and practices used for system design, planning and analysis; and shall report the results and recommendations to the NERC board. This review shall include an evaluation of transmission facility ratings methods and practices, and the sharing of consistent ratings information.

Regional reliability councils may consider assembling a regional database that includes the ratings of all bulk electric system (100 kV and higher voltage) transmission lines, transformers, phase angle regulators, and phase shifters. This database should be shared with neighboring regions as needed for system planning and analysis.

NERC and the regional reliability councils should review the scope, frequency, and coordination of interregional studies, to include the possible need for simultaneous transfer studies. Study criteria will be reviewed, particularly the maximum credible contingency criteria used for system analysis. Each control area will be required to identify, for both the planning and operating time horizons, the planned emergency import capabilities for each major load area.

Recommendation 14. Improve System Modeling Data and Data Exchange Practices.

The after-the-fact models developed to simulate August 14 conditions and events indicate that dynamic modeling assumptions, including generator and load power factors, used in planning and operating models were inaccurate. Of particular note, the assumptions of load power factor were overly optimistic (loads were absorbing much more reactive power than pre-August 14 models indicated). Another suspected problem is modeling of shunt capacitors under depressed voltage

conditions. Regional reliability councils should establish regional power system models that enable the sharing of consistent, validated data among entities in the region. Power flow and transient stability simulations should be periodically compared (benchmarked) with actual system events to validate model data. Viable load (including load power factor) and generator testing programs are necessary to improve agreement between power flows and dynamic simulations and the actual system performance.

Recommendation 14: The regional reliability councils shall within one year establish and begin implementing criteria and procedures for validating data used in power flow models and dynamic simulations by benchmarking model data with actual system performance. Validated modeling data shall be exchanged on an inter-regional basis as needed for reliable system planning and operation.

During the data collection phase of the blackout investigation, when control areas were asked for information pertaining to merchant generation within their area, data was frequently not supplied. The reason often given was that the control area did not know the status or output of the generator at a given point in time. Another reason was the commercial sensitivity or confidentiality of such data.

Attachment 4a

Board Recommendations on Blackout

(Revised February 27, 2004)

Rec. #	Staff	TSC	PC	MC	OC	CIPC[1]	CEP	CCC	CCMC	PCGC	SAC	CTTF	RRC	FE	MISO	PJM	ECAR
1.a			x	x	x		x						x	P	P	P	
1.b	P	P											P				
2.a									x				x				
2.b							x		x								
2.c			x	x	x		x					P					
2.d							x	x					x				
3.a							x		x				x				
3.b					x		x		x				x				
3.c							x		x				x				
4.a							x						x				
4.b				x			x						x				
4.c				x			x						x				
5.a	P	P	x		x		x	x	x			x	P				
5.b		x		x													
6					x		x		x				x	x	x	x	
7.a			P	x	x						x		x				
7.b			x		x								x				P
8.a			x	x									P				
8.b			x	x	x								P				
8.c			P	x	x						x		x				
9				x	P						x						
10					P	x											
11.a			x	x	P								x				x
11.b			x	x	x								P				
12.a			P								x		x				
12.b						x	x						x				
13.a				x	x						x		x				
13.b			x				x				x		x				P
13.c			P										x				
14			x	x									P				

P = primary or lead responsibility.
x = secondary or coordinating responsibility.

---

1. The CIPC will provide a security and confidentiality review of all initiatives coming out of the recommendations to ensure that security vulnerabilities are not introduced or increased.