



Critical Infrastructure Protection Committee

Note: DHS Secured Briefing will precede meeting on June 20 (9 a.m. to 11:30 a.m.)
Tuesday, June 20, 2006 — 1 p.m. to 5 p.m.
Wednesday, June 21, 2006 — 8 a.m. to 12 p.m.

Holiday Inn Arlington
4610 North Fairfax Drive
Arlington, Virginia

(PLEASE BE PREPARED TO STAY FOR THE ENTIRE MEETING.)

Meeting Agenda

- | | |
|---|--------|
| 1. Administrative Matters | 20 min |
| a) Arrangements — Stan Johnson | |
| b) Announcement of quorum — Stan Johnson | |
| c) Procedures — Stan Johnson | |
| *d) NERC Antitrust Compliance Guidelines — Stan Johnson | |
| e) Parliamentary procedures — Stan Johnson | |
| f) Introduction of members, alternates, and associates — Stan Johnson | |
| g) Approval of agenda — Stuart Brindley | |
| *h) Approval of March 16–17, 2006 CIPC meeting minutes — Stuart Brindley | |
|
 | |
| 2. Information Items | |
| a) CIPC Executive Committee report — Stuart Brindley | 15 min |
| 1. Board of Trustees highlights — Stuart Brindley | |
| 2. Electricity Sector Coordinating Council update | |
| a. Approve National Mining Association membership | |
| b) NERC report — Stan Johnson | 15 min |
| 1. FERC Staff Report on NERC 1200 Standards — Regis Binder | |
| c) ESISAC report — Stan Johnson | 20 min |
| d) Electric Reliability Organization update — Stan Johnson | 20 min |
| e) Working groups and task force 2006–2007 plans — chairs | 30 min |
| 1. CIPC organization review | |
| 2. Brief update of current activities (5 min each) | |

3. Security Planning

- *a) Cyber Security Standards Education Team — Larry Bugh 45 min
 - Update
 - Schedule for Workshops (see **Agenda Item 3a**)
- *b) Control System Security Working Group — Linda Nappier 30 min
 - 1. **Endorse** the “Roadmap to Secure Control Systems in the Energy Sector” document (See **Agenda Item 3b2** for motion)

4. Security Operating

- a) Indications, Analysis, Warnings program review — Larry Bugh 10 min
- b) Reporting Technology Working Group — Carl Eng 60 min
 - *1. Homeland Security Information Network (HSIN)
 - a. **Approve** recommendation (See **Agenda Item 4b1a** for motions)
- c) Pandemic update — Stan Johnson 30 min
 - 1. Impact on operations — Dr. Ann Norwood (DHS)
Speaker will address the implications for an operating utility experiencing high absentee rates, serious illness and some mortality.
- d) Incident reporting 30 min
 - 1. FBI perspective — Eddie Alford
Speaker will address what and how to report, what to expect from the Bureau.
 - 2. NICC Perspective-Information required and how it is used.
 - 3. Use of Patriot Reports — National Infrastructure Coordination Center Representative, speaker will explain what a patriot report is and how they are used by law enforcement.
- e) Rapid transmission restoration — Lindsey/Hubbel 30 min

5. Agency Reports

- a) Department of Homeland Security
 - b) Department of Energy
 - c) Public Safety Emergency Preparedness Canada
 - d) Federal Energy Regulatory Commission
- 45 min

6. Closing

- a) Follow-up items and future actions — Stuart Brindley 10 min
- b) Future meetings — Stan Johnson 5 min

2006

- September 13–15, Cambridge, Massachusetts (with NERC and AGA/EEI)
- December 6–8, Tampa, Florida, or Houston, Texas (with NERC)
Majority of NERC wants Houston, majority of CIPC wants Tampa.

NOTE: After the CIPC meeting concludes, the International Electricity Infrastructure Assurance Forum (IEIA) will be held in the same conference room. CIPC attendees are welcome to sit in on the IEIA meeting.



NERC ANTITRUST COMPLIANCE GUIDELINES

I. GENERAL

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. PROHIBITED ACTIVITIES

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. ACTIVITIES THAT ARE PERMITTED

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.



Critical Infrastructure Protection Committee Meeting

March 16–17, 2006
Mesa, Arizona

Draft Minutes

A regular meeting of the Critical Infrastructure Protection Committee (CIPC) was held on March 16–17, 2006 in Mesa, Arizona. The meeting notice, agenda, and attendance list are affixed as **Exhibits A, B, and C**, respectively. Meeting presentations that are publicly available may be found at: <http://www.nerc.com/~filez/cipmin.html>.

Vice chairman Barry Lawson presided.

Secretary Stanley Johnson announced that a quorum was present and confirmed the following proxies:

- 1) Nathan Mitchell for Mike Hyland
- 2) Michael Brytowski for Dave Kulissek
- 3) Ivan McClelland for Stuart Brindley
- 4) Todd Thompson for Tom Bowe
- 5) Lyman Shaffer for James Sample

Antitrust Guidelines

The secretary reviewed the NERC Antitrust Compliance Guidelines.

Introductions

The committee members and guests introduced themselves.

Logistics

The secretary reviewed the meeting arrangements, site requirements, and agenda adjustments.

Parliamentary Procedures

The secretary reminded the attendees of the use of proper parliamentary procedures.

Agenda

The CIPC members approved the meeting agenda moved by Carl Eng, seconded and passed with no dissenting votes.

Minutes

The CIPC members approved the minutes of the December 8–9, 2005 meeting, moved by Bob Windus, seconded and passed with no dissenting votes.

CIPC Executive Committee Report and Actions

Barry Lawson reported on the January 2006 Partnership for Critical Infrastructure Security (PCIS) meeting attended by Stuart Brindley. The National Infrastructure Protection Plan (NIPP), National Assets Database, and risk assessment methodologies were discussed. The base NIPP is expected to be released in May 2006 with the specific plan for the energy sectors to be issued six months later.

A spring 2006 meeting of the Electricity Sector Coordinating Council with the Government Energy Coordinating Council is being planned. Topics will include the appropriate procedure for changing the Electricity Sector (ES) Physical and Cyber Threat Alert Levels, the sector specific NIPP, the feasibility study for the development of a transmission monitoring system, and other subjects. Senior DHS personnel will also be in attendance. Note: The meeting was held on May 4, 2006 and will be discussed at the June 20–21, 2006 CIPC meeting.

NERC Update

The current status of the Electric Reliability Organization (ERO) application and the new NERC program based organization was discussed.

Electricity Sector Information Sharing and Analysis Center (ESISAC)

Lou Leffler provided an update on ESISAC activities. The DHS Cyber Storm 2006 communications focused exercise was conducted February 6–9, 2006. The exercise was heavily focused on communication and information sharing. The ES participated and observed as reliability coordinators, balancing authorities, load serving entities, and the ESISAC. Several significant lessons learned regarding emergency communications were discussed. While still under development, The Homeland Security Information Network (HSIN) was used extensively and successfully during the exercise, also with lessons learned to improve HSIN functionality.

The Critical Infrastructure Warning Information Network (CWIN) has been deployed to 11 reliability coordinators and the ESISAC. Additional locations are expected; training and testing will proceed.

The joint Department of Energy (DOE) / Federal Energy Regulatory Commission (FERC) report to Congress for the Energy Policy Act 2005 Section 1839, Transmission Monitoring System was briefly discussed. NERC is working with the DOE and FERC to scope a path forward. CIPC and the Operating Committee will be involved as this initiative proceeds.

The National Security Telecommunications Advisory Committee's Telecommunications Electric Power Interdependencies Task Force (TEPITF) presented its near-term report; this includes recommendations for communications between the Electricity and Communications sectors and designation of utility personnel as "emergency responders" during emergencies. The TEPITF is now working on the issue of long term outages that will focus on dependencies and interdependencies of the electricity and community sectors.

Stan Johnson reported on the Blue Cascades III exercise conducted in the Pacific Northwest, on March 1–2, dealing with infrastructure response to a devastating earthquake. Improvement areas identified included restoration, priorities, dependencies, individual role clarity, and the need to establish and maintain relationships between critical infrastructure sectors, law enforcement, and other federal, state, and local agencies.

Security Guidelines

The Security Guidelines Working Group (SGWG) recommended review of seven security guidelines during 2006 and seven others during 2007. The CIPC approach will use existing working groups and task forces or specifically charged task forces to conduct the reviews and recommend revisions.

The SGWG recommended a modification to the security guideline preamble; this was moved by Chuck Noble, seconded and passed unanimously as:

“This document addresses potential risks that can apply to some electricity sector organizations and provides practices that can help mitigate the risks. Each organization decides *for itself* the risks it can accept and the practices it deems appropriate to manage its risks.”

Seiki Harada was thanked for his contributions; Scott McCoy will assume the chair of the SGWG.

Cyber Security Standards

Larry Bugh reported on the Cyber Security Standards CIP-002-1 through CIP-009-1 ballot status. The standards passed the first ballot and the second ballot will be completed March 24, 2006. The applicability of the standards beyond control centers was noted. The posted implementation plan will not be changed. Note: The cyber security standards passed the second ballot and were approved by the NERC board on May 2, 2006.

Outreach

Wally Johnson and Larry Bugh reported on the Cyber Security Standard Education Team proposed standard education effort for the ES. The path forward will be to develop a three module course. Module One will be a basic overall NERC/ERO review. This is being developed for other workshops and will be available at those venues and through cyber security standard webexes to be scheduled in June and July. Module Two will be developed for workshop presentation to deal specifically with the CIP-002-1, the risk assessment approaches, and identification of critical cyber assets associated with critical bulk electric system assets. Module Three will deal with CIP-003-1 through CIP-009-1, and compliance issues. Modules two and three will include what to expect in an audit.

A request for proposal (RFP) will be written for development and delivery of education modules and associated materials that will be used in workshops and ES entities for their own training. Note: The selected vendor is Dyonyx.

The workshop (modules two and three) will be held in ten cities in the August to December period.

Control Systems Security

Tom Flowers reviewed the Control Systems Security Working Group activities toward development of documents dealing with zero day event detection, incident response, and information security.

The paper, “Top 10 Vulnerabilities of Control Systems and Their Associated Mitigations – 2006” was reviewed, modified, moved by Tom Flowers, and passed by a vote of 31–1, for public availability after NERC format review by technical writers.

Hank Kenchington presented the “Roadmap to Secure Control Systems in the Energy Sector”. This document is available at: <http://www.controlsystemsroadmap.net>

CIPC members were requested to thoroughly review this document for consideration to **vote to endorse**, at the June 2006 meeting, the roadmap as the path forward for the ES, together with the other energy sectors to secure control systems now and in the future.

Bob Hill, Idaho National Labs, reported on the SCADA Summit.

Indications, Analysis, and Warning (IAW) Program

Nominal changes were made to the IAW program in 2005 and the current program has been signed by DHS and NERC. The program is currently under substantive review. A progress report is planned for the June 2006 meeting, with approval by CIPC anticipated at the September 2006 meeting.

Homeland Security Information Network (HSIN)

Carl Eng, Julie Silberger, and Greg Holland reported on the status of the HSIN project including mechanics and development of the registration process. Carlos Kizzee discussed the Memorandum of Understanding (MOU) and the End User Agreement (EUA) that are included in the agenda materials. He also discussed the status of originator control (ORCON) as provided for in the developing application of PCII to HSIN.

Motion 1—moved by Carl Eng, seconded and passed with a vote of 23 yes, 2 no, and 7 abstentions. CIPC recommends NERC execute with DHS the Memorandum of Understanding for use of HSIN by the ES.

After extensive discussion, the question of proceeding with the End User Agreement was called with a vote of 25 yes, 6 no, and 1 abstain.

Motion 2—moved by Carl Eng, seconded and passed with a vote 24 yes, 7 no, and 1 abstention. CIPC recommends proceeding with the End User Agreement as part of the HSIN registration process.

The EUA is an agreement (made during registration) between DHS and individual HSIN users regarding HSIN mechanical use, not inclusive of any posting requirements. The CIPC Executive Committee recommended to CIPC that the EUA be sent to the CIPC, Operating Committee, American Public Power Association, Canadian Electricity Association, Edison Electric Institute, National Rural Electric Cooperative Association, and signatories to the NERC data confidentiality agreement for information and comment. Comments should be sent to NERC.

The HSIN registration and training (likely by webex) will be discussed at the June 2006 CIPC meeting. The current secure messaging system (Critical Infrastructure Protection Information System) will remain in use and parallel operation for some subsequent time period.

Hurricane Experiences

Presentations of the 2005 hurricane season were made by Ron Landry on Lafayette Utilities System experiences and lessons learned (presentation available on request to NERC) and by Stan Johnson on the DOE After Action Report from The Energy Leadership Forum held in January.

Dual Site Energy Control Center

Tom Glock presented on his utility's experience regarding primary center shutdown and restart testing.

Pandemic Document

Stan Johnson reported on the CIPC approval by email ballot of the Influenza Pandemic Summary and Influenza Pandemic Reference Guide, available at: <http://www.nerc.com/~filez/cipfiles.html>

One concern expressed was how to deal with critical infrastructure emergency responders' capability to serve during a pandemic emergency.

Agency Reports

U.S. Department of Homeland Security (DHS) — Paul Carrier discussed improvements to the secured briefing scheduled for June 20, increase in copper thefts from utility facilities, Cyber Storm exercise, and threat level changes.

U.S. Department of Energy (DOE) — Matt Rosenbaum made a brief report for DOE.

Public Safety Emergency Preparedness Canada (PSEPC) — Joan Egan discussed the change in government in Canada, Cyber Storm exercise, cross border interdependencies, consensus building for Canadian CIP strategy, and the initiation of a Canadian Cyber Security Task Force.

Federal Energy Regulatory Commission (FERC) — Regis Binder discussed the ERO filing, two new commissioners being appointed by the president.

Incident Report

Tom Eells reported on the activities in the midwest by the so-called "Dr. Chaos" and his current incarceration.

Appreciation

Ken Hall was thanked for his contributions over many years to CIPC and the security of the ES.

Closing

Vice chairman Barry Lawson closed the meeting at 4:00 pm on March 17, 2006

Future Meetings

September 13–15, 2006: Cambridge, MA (with AGA/EEI)

December 6–8, 2006: Houston, Texas or Tampa, FL (with NERC).

Respectfully submitted,

Stanley L. Johnson
NERC Staff

Suggestions to NERC: Responses to FERC Staff Comments on NERC Reliability Standard Urgent Action 1200

Cyber Security Standards Drafting Team
June 8, 2006

Overarching FERC Staff Comments related to UA 1200:

Staff contends that the requirements in UA 1200 are imprecise, making it difficult to ascertain whether or not an entity was in compliance with the various provisions contained within each section. Additionally, Staff raises concerns about the use of self-certification rather than a formal audit to demonstrate compliance.

New cyber security standards were approved by the industry in March 2006 and adopted by NERC's Board of Trustees in May 2006. These standards, CIP-002 – CIP-009, replace UA 1200. The new standards are more specific and concise, contain compliance measures, and define levels of non-compliance. Furthermore, the language indicating that audits will not be performed has been removed. The implementation plan for CIP-002 – CIP-009 states that full and formal compliance auditing will begin no later than 2010 for already registered entities. NERC's current Compliance Program calls for a formal audit at least once every three years. Annual self-certification is specified between audits.

1. Consensus-based standards development

Staff expressed concern that UA 1200 is ambiguous, especially regarding compliance requirements. CIP-002 – CIP-009, which replace UA 1200, were developed with the expectation that the requirements would become mandatory and enforceable and that financial penalties would be assessed for non-compliance. Each requirement in the new suite of CIP standards has a corresponding measure and each standard defines levels of non-compliance. Care was taken to ensure that the measures associated with each requirement are, in fact, measurable.

The standard development process required decision making by a team of relevant subject matter experts that reflects industry consensus. It often required the team to seek common ground between opposing industry opinions. This process permits the industry to achieve consensus while improving reliability, and is akin to the consensus-based rulemaking process used by the Commission and other federal agencies.

2. Specificity

Staff commented that the requirements of UA 1200 lack sufficient detail to ensure risks are reduced. This deficiency is addressed in CIP-002 – CIP-009. The requirements in these standards contain the specificity needed to ensure reasonable consistency across this diverse industry.

For example, Staff pointed to section 1201, noting that the requirement calls for an entity to have a cyber security policy but does not define what that policy should address. CIP-003, Cyber Security — Security Management Controls, Requirement 1.1 states that, “at minimum, the cyber

security policy [must address] the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.” A similar example exists in the requirements pertaining to the electronic security perimeter.

Staff also commented that UA 1200, section 1203 provides little clarity on how an electronic security perimeter is identified. The definitions promulgated with the CIP standards defines the electronic security perimeter as “The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.” Further, CIP-005, Cyber Security — Electronic Security Perimeter(s), Requirement R.1.1 identifies access points as including “any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).”

The drafters of the CIP standards took great care, however, to avoid being overly prescriptive. The changing nature of cyber security threats and vulnerabilities coupled with the rapid pace of technology advancements and the variety of industry participants demand flexibility to choose context-appropriate solutions using reasonable business judgment. Explanatory details and examples, where appropriate, are included in a supporting document titled “Frequently Asked Questions (FAQ).” Although not part of the formal CIP standards, this document was posted for public review and comment along with the CIP standards. The FAQ is intended to be read along with the CIP standards to provide additional supporting interpretation and materials.

It should be noted that, while Staff commented approvingly of the detail provided by the reference to the Indications, Analysis, and Warning (IAW) program in UA 1200 section 1214, this reference has been removed from the new CIP standards. The IAW Standard Operating Procedure is a document developed outside of the ANSI-accredited standards development process, necessitating its removal from the formal standard itself. However, CIP-008, Cyber Security — Incident Reporting and Response Planning, does contain requirements for developing and maintaining a Cyber Security Incident response plan and details the elements that constitute an adequate plan. The reference to the IAW Standard Operating Procedure has been moved to the “Frequently Asked Questions.”

3. Sufficiency

Staff expressed concern about the lack of definition within UA 1200 relating to the adequacy of required policies, plans, and procedures. As described above, the new standards CIP-002 – CIP-009 address this concern to a degree by adding as much specificity as possible for standards applicable across a wide variety of enterprises, activities, and structures. The purpose of a standard is to specify requirements. Judging the quality of policies, plans, and procedures is the function of a readiness audit.

4. CIP-001-0

Staff also criticized the lack of detail in CIP-001-0, Sabotage Reporting. This standard is considered “Version 0,” which means it was not developed using NERC’s ANSI-accredited standards development process. (It was part of an existing Operating Policy.) NERC intends to update this standard to add missing compliance elements before November 2006. During the development process for Standards CIP-002 – CIP-009, the drafting team generally considered

that standard CIP-001 dealt with physical sabotage reporting, and, therefore, added the separate cyber incident reporting requirements in CIP-008.

CSSET

Schedule of Workshops

Cyber security standards education workshops are presently planned for the following cities:

City	Region	Dates – to be determined
Atlanta	SERC	
Boston	NPCC	
Calgary	WECC	
Dallas	ERCOT	
Denver (tentative)	WECC	
Minneapolis	MRO	
San Diego	WECC	
St. Louis	RFC, SPP, SERC	
Tampa (tentative)	FRCC	
Toronto	NPCC	
Washington, D.C.	RFC	

Motion for NERC to Endorse and Guide Implementation of the Roadmap to Secure Control Systems in the Energy Sector

Motion

The Critical Infrastructure Protection Committee recommends that the North American Electric Reliability Council (NERC):

- Endorse the Roadmap to Secure Control Systems in the Energy Sector
- Provide an active role in guiding the implementation of the Roadmap

Background

- The Roadmap to Secure Control Systems in the Energy Sector (Roadmap), published in January 2006, represents a comprehensive effort to identify, integrate, and prioritize the needs of the energy sector to secure their cyber-based control systems.
- The Roadmap was developed through a public-private partnership that was led by asset owners and operators in the electricity and oil and natural gas sectors. The U.S. Department of Energy (DOE), the U.S. Department of Homeland Security, and Natural Resources Canada were government partners who helped facilitate this process. NERC and electricity sector organizations guided roadmap development through their active participation on the Roadmap Steering Committee and through their strong representation at the roadmap workshop in July 2005.
- The Roadmap presents a strategic framework for improving control systems that is being used by government and the private sector to guide investments in programs and projects that will improve the ability of end-users, system integrators, and vendors to better secure control systems.
- The Sector Coordinating Councils for Electricity and Oil and Natural Gas were identified in the roadmap as logical industry bodies to oversee the implementation of the Roadmap.
- DOE is currently working with organizations to “map” existing industry and government control systems projects onto Roadmap priorities as a first step toward identifying key gaps and opportunities for collaboration.

What does “endorsement” mean?

- “Endorsement” means that NERC concurs with the overall vision and goals contained in the Roadmap but it does not commit NERC to achieving specific milestones or investing in specific projects
- “Endorsement” also communicates to industry and government partners that the Roadmap represents a positive step toward improving control systems security through collaborative efforts and provides a useful framework for industry and government investment.

What does “guide the implementation of the Roadmap” mean?

- NERC will play an active role in overseeing Roadmap implementation, including help in:
 - Mapping industry and government control systems security activities
 - Identifying gaps and overlaps
 - Refining the Roadmap milestones and priorities
 - Measuring progress toward Roadmap goals and milestones
 - Attracting industry and government resources to Roadmap priorities
 - Recommending and endorsing specific actions that will help industry and/or government to achieve the Roadmap vision and goals.

Motion 1

CIPC approves the HSIN-ES End User Agreement for use in granting access to the HSIN-ES. (EUA attached)

Motion 2

CIPC approves the following HSIN-ES implementation plan:

- A. Allow registration and training of users, commencing in July 2006.
- B. Approved users will be allowed access to the HSIN-ES on a non-production (test) basis.
- C. The CIPC will be requested to approve commercial operation of HSIN-ES at the September 2006 CIPC meeting, assuming satisfactory resolution of PCII coverage, protection, and originator control of data submitted via HSIN-ES.
- D. Commercial operation OF HSIN-ES would then commence on October 01, 2006 in parallel with the existing CIPIS.
- E. Success of the HSIN-ES will be judged at the December 2006 CIPC meeting with a subsequent motion for approval to discontinue the existing CIPIS operation effective January 01, 2007.

REGISTRATION EUA
(HSIN-Electricity Sector/Mission Sites)

Registration Notice:

You are entering a United States Government maintained system, which may be used only for authorized information coordination conducted within HSIN-Electricity Sector (HSIN-ES) to include (but not be limited to) functions such as information gathering, processing, dissemination, sharing, archiving, and the general business records management practices associated with Federal, state, municipal, tribal, and private sector information management and exchange. The HSIN platform may not be used for lobbying, advertising, or product endorsement. Unauthorized attempts to gain access, upload, and/or change information on HSIN web sites may be a violation of Federal and/or state criminal law

Monitoring and Auditing:

Use of the HSIN system is subject to monitoring/auditing the usage of this system to ensure the security of the network and to prevent use for any purpose constituting a violation of law.

Access to Information:

The information within HSIN-ES is limited to particular member communities whose users are vetted through detailed registration, identity verification, and access validation protocols. Information reported or posted by a particular entity may be coordinated within/among the relevant or applicable community to which it was reported or posted by the source entity but remains subject to any limitations on use/dissemination imposed by the reporting/posting source entity and remains within the custody and exclusive control of the source entity for information privacy and information production/disclosure requirements imposed by law or regulatory policy. No information posted for HSIN-ES membership may be released or distributed beyond this sector community membership absent the express approval of the source entity.

Use of Information:

HSIN-ES information is presumptively owned or licensed by individuals, companies, or organizations and protected by U.S. and foreign copyright laws. No information sourced from or displayed within HSIN-ES shall be used in a manner that may subject individuals, companies, or organizations to commercial harm, competitive injury, or regulatory action.

Registration Disclaimer: This site is merely maintained by the U.S. Government. Neither the U.S. Government, nor the Department of Homeland Security, nor any other Federal agency controls or manages HSIN-ES content or access to HSIN-ES information. The information communicated on this system may be pre-analytical and unconfirmed information from numerous sources. Neither the U.S. Government, nor any of its agencies, nor the North American Electric Reliability Council, nor any component entity associated with the Electricity Sector involved in HSIN-ES use warrants or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any

information, apparatus, product, or processes disclosed through this system. Neither the U.S. Government, nor any of its agencies, nor the North American Electric Reliability Council, nor any component entity associated with the Electricity Sector involved in HSIN-ES use endorses or recommends any product, process, or service of non-federal or commercial entities. The views and opinions expressed within products on HSIN-ES do not state nor do they reflect the policies, views, or opinions of the U.S. Government, any of its agencies, the North American Electric Reliability Council, or any component entity associated with the Electricity Sector involved in HSIN-ES use. HSIN-ES web pages may provide links to external internet sites for the convenience of its users but the U.S. Government is not responsible for the availability or content of those external sites and does not endorse, warrant, or guarantee the products, services, or information described or offered at those other internet sites. The compliance policies and rules concerning information coordination required for access to HSIN-ES are not intended to create or confer any right, privilege, or benefit to any private person including any person in litigation with the United States, with the North American Electric Reliability Council or with any component entity associated with the Electricity Sector involved in HSIN-ES use.