



**NORTH AMERICAN
ELECTRIC
RELIABILITY
COUNCIL**

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5721
www.nerc.com • 609-452-8060 (Voice) • 609-452-9550 (Fax)

Critical Infrastructure Protection Committee Meeting

June 20–21, 2006
Arlington, Virginia

Highlights

Formalities

A quorum was present during the meeting. Proxies were noted. NERC Antitrust Guidelines were read. The agenda for this meeting and the minutes of the March 16–17, 2006 meeting were approved. Presentations made at this meeting will be posted at the NERC CIPC Internet site with availability as specified by the presenters.

CIPC Executive Committee Report and Actions

Stuart Brindley reported (refer to presentation).

Linda Nappier has been named the new chair of the Control Systems Security Working Group. Tom Flowers was thanked by CIPC for his significant leadership of this important position.

The NERC Board of Trustees unanimously adopted the standards CIP-002 through CIP-009, stating that these standards are “major and significant”.

Meetings of the Electricity Sector Coordinating Council (ESCC) have established paths forward to complete the Electricity Sector (ES) part of the Energy Sector specific part of the National Infrastructure Protection Plan (NIPP), to engage with the Government Energy Coordinating Council regarding policy for setting the threat alert levels (physical and cyber) for the ES, and to consider space at the DHS for ES subject matter experts (in time of urgency and possibly as a routine function).

The NIPP ES specific plan has eight significant sections; refer to the presentation.

Stuart described the Critical Infrastructure Protection Advisory Council (CIPAC) concept and the Partnership for Critical Infrastructure Security (PCIS) and the relationships with government agencies, other sectors, and the Information Sharing and Analysis Centers (ISAC) Council.

The ESCC put forth a motion that CIPC passed with no dissenting votes:

- Include the National Mining Association (NMA) as a non-voting member of the ESCC.

Attendees at the DHS cleared briefing conducted the morning of June 20, 2006 are requested to provide quality comments (with no specifics on any classified materials) to Stan Johnson at Stan.Johnson@nerc.net; the intent is to learn from each session to provide input for subsequent briefings.

NERC and the ESISAC

Stan Johnson reported.

NERC continues on a fast track to complete the formation and approval of the Electric Reliability Organization. Functional areas of the organization have been delineated. Situational awareness, one of the areas, is under continued development including delineation of duties and tools.

The ESISAC has been involved in the ERCOT event of April 2006, the Amtrak event of May 2006, the TOPOFF-4 Command Post Exercise, and several hurricane preparedness exercises. Interest remains focussed on the copper and aluminum thefts from electrical facilities.

Regis Binder reported on the Federal Energy Regulatory Commission (FERC) staff review of the NERC Cyber Security Standards (version-1200). Discussion ensued on the replacement standards, CIP-002-009. The existing CIP-001 deals with physical security incident reporting. CIP-008 deals with cyber security incident reporting.

Cyber Security Standard Education Team

Dale Zahn reported.

The team has been meeting to organize the CIP-002-009 training materials and workshops. There will be three modules:

1. Introduction to NERC and standards; to be developed by NERC and presented via four or five Webex two-hour sessions during August 2006.
2. Understanding the standards.
3. Audit compliance.

Modules two and three will be presented at ten workshops beginning in late August and running through early December 2006. The schedule is attached as **Attachment A**.

Control Systems Security Working Group

Linda Nappier reported (refer to presentation).

The CSSWG work plan (included in agenda materials) has been revised to include focus on development of a security guideline on incident response. Additional efforts on security guidelines and reference documents are included in the plan.

CSSWG is engaging with the US Cyber Consequences Unit regarding a draft Cyber Security Checklist.

CSSWG offered the following motion that CIPC approved with no dissenting votes:

- 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 and provide an active role in guiding the implementation of the Roadmap.

Indications, Analysis, and Warnings Working Group

Chuck Noble reported.

The IAW program is under detailed revision. The work plan (included in agenda materials) is aggressive leading to a revised program together with legal documents for CIPC approval by June 2007. A summary will be provided at the December 2006 CIPC meeting.

The possibility of a future related standard was suggested. The working group will also develop associated roles for the ESISAC.

Homeland Security Information Network (HSIN)

Carl Eng reported (refer to presentation).

Nancy Wong, DHS Preparedness/Infrastructure Partnerships Division, presented on the Suspicious Activity Reporting with emphasis on how information is used and protected. Ms Wong discussed information sharing and the facets that go beyond intelligence information to cover hurricane response and natural disasters of all kinds. An analysis of information sharing and submitter controls is expected to be completed by August 2006.

It was noted that the Department of Energy (DOE) is the sector specific agency for the ES and will be involved in the DHS Protected Critical Infrastructure Information (PCII) program. We expect that the DOE will be able to receive Form-417 reports via porting through the HSIN. This will allow for ease of electronic submission of these reports in a timely manner with access only to those authorized.

Julie Silberger, Josh Canary, Carlos Kizzee, and Patrick Ansaldi discussed the current status of the HSIN technologically and legally. It will be possible to seamlessly link between CI sector HSIN portals to which an individual is authorized. Connectivity will include the US-CERT and the DHS LLIS portals for those so registered.

Authorization for an individual within an ES entity to use the HSIN-ES will be controlled by the ESISAC. The authentication and authorization process will be similar to that currently in use for the NERC Critical Infrastructure Protection Information System (CIPIS) and will be considerably more rigorous, including means to control continued access and password updating; documentation will be developed.

Regarding DHS PCII, the HSIN-ES DHS form will contain PCII protection automatically; the "free-form" will provide the opportunity to request PCII protection. In either case PCII applies to the DHS. Submitters may select other recipients of information (e.g., and not limited to: Reliability Coordinators, Balancing Authorities, ES CIP community), but these will not have PCII application.

Discussion ensued regarding the ability to use the HSIN-ES to send information to other entities (e.g., and not limited to state and provincial authorities). This was referred to the Indications, Analysis, and Warnings Working Group to provide guidance on applicability of such sharing for the ES. The Reporting Technologies Working Group will examine technology regarding the submitters' choice of to whom reports posted to HSIN-ES will be transmitted. This will include consideration of the FERC, DOE, Canadian and other US government agencies, and provincial and state agencies.

There are some Canadian ES entities that cannot use the HSIN-ES at this time due to legal constraints. The existing CIPIS will continue in service as a NERC system for some time, at least until 2007. NERC Staff will assure that double reporting will not be required and that all recipients receive information submitted to them. Likewise the porting with the Reliability Coordinators Information System (RCIS) will be developed.

The following motion was passed with no dissenting votes and three abstentions:

- 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.

It is recognized that the dates in the above motion are suggested targets that are subject to subsequent motions.

The following addending motion regarding HSIN-ES was passed by CIPC with no dissenting votes: Allow for the registration of current CIPIS users in HSIN. Complete the user access validation protocols, with CIPC approval. Re-authorize existing CIPIS users; upon completion of this step, exit the test phase.

David Cook, NERC Vice President and General Counsel reported on the status of the HSIN-ES Memorandum of Understanding (MOU) between DHS and NERC. This was discussed and agreed to by CIPC at the March 2006 meeting. The MOU is now in the final stages of signing by both DHS and NERC.

The HSIN-ES End Use Agreement (EUA) is intended to assure due diligence in use of HSIN-ES by DHS and the ES. There are no therein stated reporting requirements. The EUA was previously commented on by some CIPC members; comments were included in the agreement included in the agenda materials for the June 2006 meeting.

The following motion was passed by CIPC: 21 yes, 6 no, 3 abstentions:

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

Presentations

The following excellent presentations were made to CIPC:

1. Gridsurance: A National Program for Rapid Physical Restoration of the Electric Grid. Presented by Dr Keith Lindsey, Lindsey Manufacturing Company.
2. Pressures of Pandemic Influenza: Preparing the Work Force. Presented by Ann Norwood, MD, Department of Homeland Security.
3. Eco-Terrorism. Presented by Suzanne Solomon, Federal Bureau of Investigation.

CSSET Modules Two and Three Workshops

Aug 31–Sept 1	Vancouver, BC
Sept 21–22	Hartford, CT
Sept 28–29	Minneapolis, MN
Oct 5–6	Dallas, TX
Oct 12–13	Toronto, ON
Oct 19–20	Washington DC
Oct 26–27	St. Louis, MO
Nov 2–3	Atlanta, GA
Nov 9–10	San Diego, CA
Nov 16–17	SKIP – no workshop
Nov 30–Dec 1	Tampa, FL