Critical Infrastructure Protection Working Group

Report to

ERCOT Reliability Operation Subcommittee

December 8, 2011

The CIPWG has held two meetings since the last report on October 13.

**October 7, 2011 Meeting**

In attendance were 34 persons from 15 companies.

At the October 7, 2011 CIPWG meeting discussions were held on:

1. Members of the NERC CIP version 4 Standards drafting team were present. They provided information on the status of the CIP version 4 standards as well as the status of the version 5 standards.
2. The NERC CIPC meeting in St Louis was discussed including the IED Awareness seminar presented by DHS.
3. NOGRR0074 was discussed and the group developed draft language.
4. Several NERC CANs were discussed including:

* Final CAN-0010 - Definition of Annual
* Draft CAN-0012 - Completion of Periodic Activity by Effective Dates
* Draft CAN-0016 - CIP-001-1-R-1 - Applicability to Non-BES
* Draft CAN-0017 - CIP-007 R5 System Access and Password Controls
* Draft CAN-0023 CIP-005, CIP-006, CIP-007 - Logging System Failures
* Draft CAN-0024 CIP-002 - Data Diodes
* Draft CAN-0030 Attestations
* Draft CAN-0031 CIP-005, CIP-006 - Defining Access Points, Physical

Security Perimeter and size of physical access

* Proposed CAN-0035 Periodic Data Submittals
* Proposed CAN-0037 Roll-Up Violations
* Proposed CAN-00xx - CIP-007 - Time Period to Install Patches
* Proposed CAN-00xx - CIP-005, CIP-006, CIP-007 - Self Reporting Log Access

1. A discussion was held on the status of various NERC Task Forces including, SIRTF, Substation Guidelines TF, Business Continuity TF, Cyber Attack TF, and the Information Protection TF.
2. Recent NERC Alerts were discussed.
3. The members discussed the DOD study within ERCOT, NERC Grid Ex National Exercise in November and items discussed on the ES-ISAC conference call.
4. Members discussed issues related to CIP compliance within their organizations and discussed possible solutions.
5. The members held a long roundtable discussion on their interpretation of various CIP requirements and how they were implementing those requirements in their own companies.

**November 4, 2011 Meeting**

In attendance were 42 persons from 20 companies and agencies including NERC, PUCT, Texas DPS, and the DoD.

1. The Department of Defense Mission Assurance Division made a presentation on the proposed DFW area study.
2. NERC Staff then made a presentation on:

Incident Response Assessment  
              Cyber Attack Task Force  
              NERC ES-ISAC Firewall from Compliance Activities  
              Grid Ex  
              Grid Security Conference - New Orleans  
              CSO Transition

1. The presentation prepared by the FBI on Combating Computer Intrusions was then presented to the WG.
2. The Texas Department of Public Safety made a presentation on the organization of the PSAG.
3. Members of the NERC CIP version 4 Standards drafting team were present. They provided information on the status of the CIP version 4 standards as well as the status of the version 5 standards.
4. Discussions on the status of NOGRR0074 and possible draft language were held.
5. Some discussion were held about the status of various NERC CANs.
6. A discussion was held on the status of various NERC Task Forces including, SIRTF, Substation Guidelines TF, Business Continuity TF, Cyber Attack TF, and the Information Protection TF.
7. Recent NERC Alerts were discussed.
8. A fairly long roundtable discussion was held on the various topics including secure communications methods between CIPWG members and other topics.

The next meeting is scheduled for December 2, 2011 at the ERCOT offices in Austin.