Critical Infrastructure Protection Working Group

Report to

ERCOT Reliability Operation Subcommittee

August 11, 2011

The CIPWG has held one meeting since the last report on July 8.

The attendance was down somewhat due to the July 4 holiday.

In attendance were 21 persons from 11 companies.

At the June 3, 2011 CIPWG meeting discussions were held on:

1. The WG discussed TFE Issues with Bill Beaver of TRE. The discussion also covered how to submit TFEs since the portal is still not fully functional.
2. The conversion of the TRE portal to OATI was discussed in length. Including that the site will he hosted by OATI not TRE and the potential security of the data since it will not be held by a NERC registered entity. A discussion of the status of the digital certificates was discussed.
3. Bill Beaver introduced King Farias of the TRE Staff.
4. 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 CIP-010 and CIP-011 standards and CIP-005-X.
5. A long discussion of the CIPC Toronto meeting was lead by persons attending the Toronto Meeting. Also discussed was the status of the Severe Impact Resilience Task Force, the Cyber Attack Task Force and the Substation Protection Guidelines Task Force.
6. 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. Recent NERC Alerts including Night Dragon, the Alert on RSA two factor authentication and the Increased Activity and Reporting of Suspicious Activity Alerts were discussed.
2. The members discussed the NERC Grid Ex National Exercise in November.
3. Members discussed issues related to CIP compliance within their organizations and discussed possible solutions.
4. It was noted that the Texas Regional Infrastructure Security Conference (TRISC) will meet on July 24-26, 2011 in Austin TX, at the Bergstrom Airport Hilton.
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.

The August CIPWG meeting will be held on August 5 at the ERCOT offices.

The September CIPWG meeting will be held on September 2 at the ERCOT offices.