Critical Infrastructure Protection Working Group

Report to

ERCOT Reliability Operation Subcommittee

July 14, 2011

The CIPWG has held two meetings since the last report. The first meeting was on May 9, 2011 and the second meeting was held on June 3.

At the May 9 meeting the following issues were discussed:

TFE Issues were discussion with TRE including TFE Procedures, In-Person TFE Inspections by TRE Staff, procedures for amendments to TFEs and when needed and the status of the TRE portal.

Rashida Caraway, Director of Enforcement at TRE and Brent Torgrimson of TRE Enforcement made a presentation on the NERC Enforcement Process and what to expect during the enforcement investigation and settlement negotiations.

There was a long discussion that all of the ERCOT Confidential TOP Certification Reports and similar Confidential reports from other regions had been posted to the NERC website. This was discovered soon after the March CIPWG meeting. NERC was contacted and agreed to remove all of the confidential reports from its website. Although ERCOT removed the documents we pointed out to them from their website they were available in cached pages across the internet for weeks after NERC removed them from its site. During the April meeting we were told that all report had been removed. During the April meeting members did further searches and found several other confidential reports still on the NERC website including ERCOT entities. TRE agreed to pursue the issue further with NERC. A few other reports are still being found.

Members of the CIP Standards drafting team discussed the status of the NERC CIP version 5 standards, generally known as CIP-010 and CIP-011. The status of the proposed CIP-005-X currently under development was also discussed.

The status of various NERC CANs was discussed including:

Revised Draft CAN-0010 Definition of Annual

Draft CAN-0012 - Completion of Periodic Activity by Effective Dates

Draft CAN-0016 CIP-001-1 R1 - 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-0031 CIP-005, CIP-006 - Defining Access Points, Physical

Security Perimeter and size of physical access

Proposed CAN-00xx CIP-007 Time Period to Install Patches

The group discussed the NERC Events Analysis program.

The group discussed the status of recent NERC Alerts including:

• Night Dragon

• RSA - Two Factor Identification Compromise

• Increased Activity and Reporting of Suspicious Activity

The group discussed issues being brought up by various federal agencies that may have implications for the electric industry.

The formation of the NERC Severe Impact Resilience Task Force was discussed.

Future CIPC Meetings are planned for:

* June 8–9, 2011 Toronto
* September 14–15, 2011 St Louis
* December 14–15, 2011 Atlanta

The CIPWG met again on June 3.

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.
3. A discussion of the proposed CIPC agenda for the following week in Toronto was discussed. Also discussed was the formation of the Severe Impact Resilience Task Force and the current status of its proposed report.
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. 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-00xx - CIP-007 - Time Period to Install Patches
* Proposed CAN-00xx - CIP-005, CIP-006, CIP-007 - Self Reporting Log Access

1. The WAMPAC (Synchrophasor) Security Profile was discussed.
2. Recent NERC Alerts including Night Dragon, the Alert on RSA second factor authentication and the Increased Activity and Reporting of Suspicious Activity Alerts were discussed.
3. The members discussed the scope of the NERC Severe Impact resilience task Force and noted that two members from ERCOT are working with the task force.
4. Members discussed issues related to CIP compliance within their organizations and discussed possible solutions.
5. 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.

The May CIPWG meeting will be held on July 8 at the ERCOT offices. Note that this is one week later than usual.