Critical Infrastructure Protection Working Group Report

to Reliability and Operations Subcommittee

May, 2010

The CIPWG meets on the Friday afternoon prior to the ROS meeting. The May meeting was held on May 7. The meeting is generally split into two sections. There is a closed meeting at the beginning that is open to Market Participants only that have executed a confidentiality agreement. The discussion is used to share security issues between companies and possible solutions.

The second portion of the meeting is open and is shared via a webex. This portion of the meeting is where possible issues at the NERC meetings, coordination of comments on the NERC standards or other issues are discussed.

Approximately 40 persons attended the CIPWG meeting including ERCOT, member systems, Texas Department of Public Safety, US Department of Homeland Security, Public Utility Commission of Texas, and TRE.

**Closed Session**

**TFEs**

During the closed session the attendees discussed the status of their submission of the Technical Feasibility Exception Part B’s of the CIP Standards to TRE. TRE is in the process of approving the approximately 500 TFEs submitted by ERCOT member systems. TFEs requested by ERCOT are submitted to NERC not TRE.

During the last several meetings the primary topic was the implementation of the Technical Feasibility Exception (TFE) rule by NERC. When the NERC CIP Standards were approved the standards allowed for the Senior Manager to certify that certain requirements were not "technically feasible". FERC did not agree with this portion of the standards and required NERC to adopt a rule that required that any TFE be approved by NERC or the Regional Reliability Organization (TRE in ERCOT) not the individual market participants. NERC developed the rules over the past several months and these were implemented and the first round of filings were due on on January 31, 2010. At this time NERC has not developed the forms and procedures for the second round of filings.

Discussions with TRE included how to handle equipment that was recently discovered to have needed a TFE initially but no TFE was filed, to new equipment just being installed, to equipment that has been upgraded or removed and a TFE is no longer required.

**NERC Alert System**

The NERC Alert System became effective on May 3. Since it has become effective NERC has not initiated any NERC Alerts. Systems discussed how various members handled the NERC Alterts internally upon receiving an Alert from NERC.

**Mobile Media Alert for CCA**

A discussion was held on the use and policies regarding the use of mobile media (i.e. thumb drives, DVDs, CDs, etc) and the potential guidelines or alerts coming from NERC on this subject.

**Smart Meter Security / Idaho National Lab**

A discussion was held on the potential threat vectors, testing and methodologies presented by the Idaho National Lab (INL) at the Cyber Security Workshop held by the PUCT on May 5. Various members discussed their experiences in cooperating with the INL in Red Team / Blue Team Exercises, testing performed by INL and other testing performed. A general discussion on the vulnerabilities of the SCADA platforms and particularly the security concerns presented by the implementation of the Smart Grid Equipment. Some discussions were held based on methods or specifications that needed to be included to reduce the security concerns.

At this time we requested that TRE leave the meeting so that a more open sharing between the member systems could be held.

**Compliance Sharing**

During this portion of the meeting various attendees brought system configurations and compliance methodologies to the group and the other attendees discussed their interpretation of the standards and whether the proposed solution met the NERC Standard. Systems shared how they might improve on the compliance with the Standard.

**Discussion of the Continuation of Providing the WebEx/Conference Call during the Open Session**

Historically the CIPWG were not broadcast until about a year ago. For the past year either a conference call or WebEx has been broadcast of the open portion of the meeting. This was reasonable when the group was primarily discussing general concepts about future compliance but since December 31 when the member systems were required to be compliant the discussions have a significantly more confidential since we are discussing specific methods used to indicate compliance as well as specific techniques used for security. ERCOT has been required to be compliant for at least some of the CIP Standards back to June, 2008.

Due to the sensitive nature of many of these discussions the members present felt that the telephone conference calls should no longer be provided since their was no good way to determine who was listening in on the other end of the conference calls and the potential damage that could be caused if inappropriate security information was disclosed. During the open portion of the meeting the topic was brought up again with the persons attending on the phone. Although the few persons on the phone indicated they would prefer to allow the conference calls to continue they understood the concerns. Only one person on the phone indicated they were not located in Texas.

**Open Session**

**DHS Security Clearances**

Cathy Eade from the Department of Homeland Security called in to discuss the status of the security clearances that had been applied for and the process for the others that had a need to apply for DHS Sponsored “Secret” clearances, the process for getting access to information and the process for getting DoD or other agencies clearances with reciprocity to DHS. A number of the attendees are going through the clearance process at this time. DHS is making a significant push this year to get at least one person in each utility to obtain a “Secret” clearance so DHS would have someone to communicate with if actionable intelligence indicates a need.

**CIP Standards (Version 4)**

A long discussion was held with the group discussing the requirements in the version 4 of the CIP Standards. Version 4 is almost a complete rewrite from scratch of the CIP Standards. Three members of the Standards drafting team were present for the discussion and to describe the process the committee used to develop the Standards, the process going forward and the intent of several of the requirements. The group was reminded to register for the NERC CIP workshop and the SPP CIP workshop both to be held near the DFW airport on May 19 through 21.

**Copper Theft Workshop**

One of the new issues that has been emerging in the past several month is the copper thefts. We are beginning work on developing a Copper Theft workshop for ERCOT market participants in cooperation with a number of law enforcement agencies including the Texas Department of Public Safety. The purpose of the workshop will be for the attendees (1) to share methods they have used to catch those involved and (2) to focus law enforcement attention on the level of the thefts statewide in order to increase awareness and (3) to get law enforcement to utilize some of the new laws to prosecute some of the persons caught with more severe charges than simply theft. Many of the working group members feel that their expertise is more in the cyber security area than in the physical security area. Therefore many of the persons participating in this effort are not the regular attendees at the CIPWG meetings. At this time the Copper Theft Workshop is planned for the last week in July at the ERCOT Met Center.

**Next Meeting**

The next meeting of the CIPWG will be held on June 4 at the ERCOT Met Center.