

# NERC CIPC Cyber Security Standard Education Team Report to CIPC for 9/15/2004 New Orleans Meeting

## Action

Seeking CIPC approval for this plan.

## Mission

To meet the cyber security compliance training objectives identified in the Blackout Report recommendations and the Compliance Report recommendations presented by Mike DeLaura to the NERC Board.

## Committee

Chair Linda Nappier, the cyber delegates and alternates from all regions, representatives from NERC compliance, along with some additional members from the Outreach Working Group

## Need

A letter and survey were mailed out in July. Results of the survey indicated that there is a desire to have NERC sponsor workshops designed to help members who are struggling with Cyber Security Standard 1200 compliance, and to better prepare for the upcoming permanent Cyber Security Standard 1300. In addition, the survey respondents indicated that they would like a binder of sample documentation and training materials.

## Committee Progress to Date

Two committee meetings and several teleconferences have been held so far. The committee plans to host several workshops, located in various locations, with the intent that the first workshops will be focused on Cyber Security Standard 1200 issues on the top three concerns of the Compliance report. As more information and progress is made on the Cyber Security Standard 1300, the workshop agenda will be expanded to support the proposed implementation plan. In addition, virtual workshops may be added to supplement the program.

The focus for the initial workshops has been defined as:

1. The proposed focus audience will be those in the Electricity Sector entities who are responsible for the implementation of, and compliance with the Cyber Security Standard.
2. It is assumed that the audience will be familiar with the Cyber Security Standard 1200 and the NERC compliance process.
3. The Cyber Security Standard Education Team recommends *both* onsite workshops and virtual workshops. The latter may be segmented and focused to very specific needs (including operations, cyber security, physical security, and compliance). The Team will commence its efforts on the onsite format, with future consideration to the virtual format.

The committee has drafted the agenda to be as follows:

1. Open up with Management video
2. Cyber Security Standard 1200/1300 Status update; Cyber Security Standard 1300 FAQs
3. Cyber Security Standard 1200 (overview what we're going to cover in depth)
4. Handouts (here's what you're going to take away)
5. Major Topics:

- a. Policies
  - b. What the policies mean and the supporting procedures, how to implement them, and how *important* they are
  - c. Monitoring access (physical and electronic)
6. Major Q & A session
  7. Prototype Compliance Audit (what to expect, generally the types of questions that the compliance officers would be looking for)

We intend for the participants to walk away with a binder of samples and examples. The proposed table of contents for that binder is:

1. Cyber Security Policy
2. Critical Asset Inventory
3. Electronic Security Perimeter Document
4. Physical Security Perimeter Document
5. Electronic Access Control Procedures
6. Physical Access Control Procedures
7. Background Check Procedures
8. Access Monitoring Procedures
9. Employee Training Program
10. System Management Standards and Procedures
11. Cyber Incident Response Plan

### **Proposed Schedule**

1. Plan approval is being requested from CIPC at the September 2004 meeting.
2. Present more information for CIPC comment at the November 2004 meeting in Kansas City.
3. Send out the announcement and registration form by October 1, 2004.
4. Hold the first workshop on January 12, 2005, in Phoenix, AZ.
5. Second workshop on January 26, 2005, in Orlando, FL.
6. The committee plans to hold a rehearsal session on December 8, 2004, in St. Louis, MO and have the materials printed after that.
7. In addition, we will be producing copies of the training CDs and CDs of all of the workshop materials so that members and regions can use them as “Train-the-Trainer” opportunities if they wish to hold sessions within their own organizations or regions.

### **Next Steps**

The Committee has divided into multiple sub-groups to address various portions of the workshop content. We need volunteers to help out. The teams currently are:

1. Sub-team to develop course outline for 1 to 1.5 hours of content addressing role-based securities policies, what they mean, how to implement them, importance of training, and emphasis on why they are important. — Tom Flowers (lead), .....
2. Sub-team to develop course outline for 1 to 1.5 hours of content addressing electronic and physical access control. — Linda Nappier (lead), .....

3. Prototype of typical compliance audit – what to expect, etc. — Dave Hilt, Mark Engels, Mike DeLaura
4. Cyber Security Standard 1300 Update — Larry Bugh
5. Binder Materials — Joe Doetzl
6. Training Materials Team — George Miserendino
7. Management Message from Compliance — Wally Johnson, Dave Hilt

Teleconferences will be scheduled by the above team leads once the additional volunteers are added.

We also need samples for our binders. These are being requested by CIPC Cyber Members, alternates, and associates.