AEP’s Guide to Internal Compliance Training & Awareness for NERC Reliability Standards...

SPP RE Compliance Workshop
November 13, 2012

Thad Ness
American Electric Power
Really Big Or Herding Cats
You Can and Should Use A Variety of Methods and Media

Requirement Focus

Each quarter a NERC requirement will lessons learned or other noteworthy a.

CIP 004-3 R4.1
The Responsible Entity shall review the Assets quarterly, and update the list(s) of access to Critical Cyber Assets, or any entry shall ensure access list(s) to the new AEP Access.

Steps for removing

Change of Personnel access

Complete the Puzzle

Compliant?

Good ... Now prove it

Compliance—It's our business

I shall use strong passwords.
I shall use strong passwords.
I shall use strong passwords.

To create strong passwords replace letters with numbers or special characters as in the examples above.
Periodic Newsletters

Requirement Focus

Each quarter a NERC requirement will be highlighted in the newsletter along with lessons learned or other noteworthy assessments. This month we are focusing on CIP-004-3 R4.1.

CIP-004-3 R4.1

The Responsible Entity shall ensure access to Critical Cyber Assets quarterly, and on a continuous basis, by providing access only to the new AEP Access Management Steps for removing access.

Change of Personnel

Management review of user specific access rights

In this issue

The North American Transmission Forum ("The Forum")

Promoting Excellence/Continuous Improvement

A monthly newsletter highlighting compliance with NERC Standards

The North American Transmission Forum

Current topics

AEP Transmission Reliability Compliance
Intranet News Items

News & Events
Timely, accurate information about AEP and our industry.

News from AEP

Creating secure passwords

- Protect online information with secure passwords
- Use different passwords for work and personal accounts
- Review AEP’s standards for user IDs and passwords

Related Topics: Corporate, Desk & Security

I Shall use strong passwords.

I Sh4ll use strong p4sswords.

I Sh4ll use strongp4sswords.

I Sh4ll use strong p4sswords.

To create strong passwords replace letters with numbers or special characters as in the examples above.
Executive Webcast

• Real-Time

• Question & Answer

• Available on Intranet for later viewing

Videos by Topic

Reliability Webcast

The May 13th Reliability Compliance webcast focuses employee awareness on the critical nature of compliance activities and rules that govern and protect the reliability of the nation's bulk power system.

Produced by: Monte Sanborn | Duration: 1 hour 2 minutes

Order Video | Email Video | Download Video
# Compliance Discussion Guide No. 29

**Topic:** RSAW Development: 5 Minute Audit Rule

**(Total Time: 15 minutes)**

<table>
<thead>
<tr>
<th>Activity Source</th>
<th>Script</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction:</strong></td>
<td><strong>Explain:</strong> We’re going to take a few minutes before we begin to increase and reinforce our compliance knowledge.</td>
</tr>
<tr>
<td><strong>Ask:</strong> Why do we need to ensure that we all have a good clear understanding of compliance issues that affect our jobs?</td>
<td></td>
</tr>
<tr>
<td><strong>(Answers to look for )</strong></td>
<td>• Electric system reliability</td>
</tr>
<tr>
<td></td>
<td>• Avoidance of penalties</td>
</tr>
<tr>
<td></td>
<td>• Maintain AEP’s good name and reputation with customers, regulatory bodies, and investors</td>
</tr>
<tr>
<td><strong>Paragraph painting a scenario</strong></td>
<td><strong>Pass out copies of the discussion guide.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Please read the following scenario:</strong></td>
</tr>
</tbody>
</table>
Signs, Signs, Everywhere Signs

Reporting a Problem is Not a Problem

An effective compliance system anticipates and correcting – problems before they become bigger problems. Report issues:
• Taking with your supervisor
• Calling the AEP Concerns Line 24/7 at 1-800-750-5001 (TTY 1-877-577)
• or, reporting your issue online at www.AEPCareers.com

RELIABILITY—IT’S OUR BUSINESS

Compliant?
Good … Now prove it

• Compliance with NERC reliability standards involves more than doing what’s required.
• It also involves having records and documentation that prove we are compliant.
• Evidence is the key … Do it, and prove it.

RELIABILITY—IT’S OUR BUSINESS
You Don’t Have To Be High
Tech
But, Make Sure Your Message is Clear
You Can Easily Use New Technology

All visitors to NERC CIP facilities must be logged in and logged out with date & time.

Thanks for the reminder.
Or 1980’s Technology

All visitors to
Training Management
Training Search and Register
Training – Supervisors of Employees with CIP Access

How can I determine if my direct report(s) has NERC CIP Access?

What do I do when an individual is terminated or resigns?

What do I do when an individual transfers into my department?

How to periodically review my employees’ NERC CIP access?

What to do when NERC CIP access is no longer needed?
**Evidence Guidelines**

- Start with gathering the evidence
  - Cover all items in the “Compliance Assessment Approach” section
  - Have evidence for the bookend period (typically the previous audit to the pre-audit package date)
- Make the information “Auditor Friendly”
  - Don’t overwhelm auditors with too many documents
  - Point the auditor directly to the relevant sections
  - Order the evidence as RFC, SPP, then TRE
- Have Stacking Evidence Ready
Audit Prep – Soft Skill Training

What’s on Tap?

- What we mean by “soft skills”
- Before the audit – what can I do?
- Rule(s) of the road
- During the audit – what should I do?
- Specific skills
- Specific challenges – and how to handle them

What do we mean by “soft skills”?

Remember that how you say it can be just as important as what you say

(Auditors are people, too. Really.)
Knowledge Assessment
Surveys

Let’s schedule a scenario-based roundtable discussion about our enterprise project management.

We’ll use our infrastructure survey tool to architect a risk-based tiering system.

That almost meant something.

I’m tempted to stop acting randomly.
Any Questions?
Internal Compliance Training

Sandra Sanscrainte
Senior Compliance Analyst

November 13, 2012
Agenda

- Company Overview
- Why is it important to Train our SME’s?
- Internal Compliance Training Methods
  - Learning and Development System (LaDS) Online Training
  - Legal Department Training
  - NERC Compliance Department Training
- Self-Certification Review Process
- Training “Don'ts”!
- Training “Do’s”!
Company Overview

- ITC is registered in 3 Regions
  - RFC, MRO and SPP
- ITC is registered for the following functions:
  - ITCT, METC and ITC Midwest – TO, TOP & TP
  - ITC Great Plains – TO & TOP
# Company Overview

<table>
<thead>
<tr>
<th></th>
<th>ITC Transmission</th>
<th>METC</th>
<th>ITC Midwest</th>
<th>ITC Great Plains</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Peak Load</strong></td>
<td>12,745MW</td>
<td>9,469MW</td>
<td>3,640MW</td>
<td>1,100MW</td>
</tr>
<tr>
<td><strong>Service Area</strong></td>
<td>Southeast Michigan</td>
<td>Lower Peninsula of Michigan</td>
<td>Portions of Iowa, Minnesota, Illinois and Missouri</td>
<td>Portions of Kansas and Oklahoma</td>
</tr>
<tr>
<td><strong>Total Transmission Lines</strong></td>
<td>Approximately 2,800</td>
<td>Approximately 5,500</td>
<td>Approximately 6,600</td>
<td>Approximately 100</td>
</tr>
<tr>
<td><strong>RTO Membership</strong></td>
<td>Midwest ISO</td>
<td>Midwest ISO</td>
<td>Midwest ISO</td>
<td>SPP</td>
</tr>
</tbody>
</table>
Why is it important to train our Subject Matter Experts (SME’s)?

- SME’s are our most important resource and the key to our program success.
- Providing training for our SME’s allows us to Thank them for their efforts and to convey how much they are valued.
- SME’s have the opportunity for venting and in turn what results is improved communication.
- Providing training for our SME’s builds stakeholder support/teamwork and ultimately strengthens our Culture of Compliance.
ITC’s Legal Department provided Audit witness training prior to our external Audit:

- A few of the Audit interview tips included the following:
  - Smile – be pleasant and agreeable
  - Pause – take a moment to formulate your answer. You will not be judged on how quickly you respond but on the content of your response.
  - If the question is not clear, ask for clarification.
  - Respond fully to the question, but do not embellish.

- The sequence followed by many successful witnesses when they are being questioned:
  - LISTEN-STOP-BREATHE-THINK-ANSWER
The intent of this training was to get participants to:

- Think about risks and controls

- Look at the requirements from a compliance point of view and determine the documentation needed to demonstrate compliance.

- Think about documentation and evidence to ensure that stacking of evidence is being performed.

- Be familiar with auditor sampling tools like a Random Sample Generator (RAT-STATS)
Thinking in Terms of Risks and Controls

- In all businesses there are risks that exist and that need to be identified and addressed (via controls) in order to prevent or minimize losses. In many cases the NERC Reliability Standards / Requirements are controls to address identified risks to the BES.
Evidence

- Evidence is in essence the physical manifestation of your controls.
- Required evidence is indicated many times in the body of the requirements. However, additional evidence will probably be needed to substantiate this evidence.
- Evidence needs to be related to the requirement for which you are presenting it and it needs to be complete and sufficient to support your position.
- Stacking of evidence: stronger evidence with weaker evidence or broader evidence with more specific evidence.
The intent of this training was to get participants to:

- Be aware of the purpose of the RSAW.
- Reference and identify evidence consistently using the defined nomenclature.
- Ensure that their narratives contain information necessary to answer the question being asked and show compliance.
- Define the roles and responsibilities of the Standard Owners.
An RSAW is used to:

- Present clear and concise narratives that explain how a registered entity is compliant with a standard and/or requirement
- Identify documentation and evidence that demonstrates compliance
- Provide an auditor with their first impression of the registered entity
Examples of how to identify documentation using the defined nomenclature:

- **SCH = Schedules**
  (e.g. SCH_2010 Summer DE Outage Schedule for SE MI)

- **ARG = Agreements**
  (e.g. ARG_MISO FAC-010 PA Agreement)

Affix a numeric value after the nomenclature of each document if there is more than one type of the same documentation in a RSAW

- EMAIL1_FW:Re Scheduled Outages
- EMAIL2_ITC Base Rating Changes
OATI webCompliance provides ITC the following:

- A complete tracking system pre-loaded with all NERC and Regional Reliability Standards.

- The system is a database that contains tracking records arranged by Standard and is set up to enable documentation to be loaded to the requirement level.

- Compliance documentation management — contained in a secure central repository for easy Audit and Spot Check preparation.

- The ability to archive compliance documentation to assist in the efforts of meeting data retention requirements.
The intent of this training was to get participants to:

- Be trained on any new features and or enhancements to the OATI webCompliance system
- Assist in determining if any enhancements are needed to improve the usage of the OATI webCompliance system as it is or if there is a need to expand or add new features
- Be proficient in the use of the OATI webCompliance system to better facilitate the Self-Certification Review Process
A Standard Owner is assigned to each of the applicable NERC Standards.

<table>
<thead>
<tr>
<th>Standards Assignments Sorted By Owner</th>
<th>RFC - ITCT, METC &amp; MECS</th>
<th>MRO - ITC Midwest</th>
<th>SPP - ITC Great Plains, LLC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards</td>
<td>Requirements</td>
<td>Function(s)</td>
<td>Status</td>
</tr>
<tr>
<td>Interconnection Reliability Operations and Coordination</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modeling, Data and Analysis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MOD-008-1</td>
<td>1,2,3,4,5</td>
<td>TOP</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>
RSAWs are completed and collection of the supporting documentation to show compliance with the requirements of the NERC Standards.

The NERC Compliance Department reviews the completed RSAW and supporting documentation and provides an Assessment Report to the Standard Owner.

The Assessment Report would contain comments, suggestions, action items and sometimes additional data is requested.
- Identifying the Standard Owner for NERC Standards assigns a point of contact of whom would then select their team of Subject Matter Experts to field questions from the Auditors and to respond to data requests for audits and spot checks.
- Completion of the RSAW’s and collection of supporting evidence are kept current of which makes preparation for an Audit or Spot Check more efficient.
- Compliance Review meetings with Compliance Group Reviewer and Standard Owners enable the practicing of being interviewed and responding to questions like those posed during an audit.
- Assessment Reports often include additional data requests and this allows Standard Owners and their teams to practice responding to data requests.
Don’t plan a 3 hour training session intended to cover 4 or more topics!

Don’t plan a training session to close to a holiday!

Don’t plan a training session to early or late in the day!

Don’t cover an important topic only once!

Don’t cover topics for a training session that only a portion of the Subject Matter Experts need to know about!

Don’t limit training for offsite SME’s to video conference WebEx!
Do plan your training sessions in 1 to 2 hour blocks. Allow an 1 hour for each topic to present the material and answer questions!

Do plan your training sessions so that a holiday or compliance activities are not a factor!

Do plan your training sessions mid-morning or mid-afternoon!

Do plan having continuous training topics to ensure the intent and implementation of the training is consistent!

Do have a participant sign-in sheet!

Do have snacks and refreshments for 2 hour block training sessions. Make sure to indicate in the training invite that snacks and refreshments will be available!
Internal Compliance Training

Philip Propes
November 13, 2012
REMEMBER THE FUNDAMENTALS:
(OR, KNOW WHAT YOU’RE DOING BEFORE YOU DO IT!)
Three Compliance Training Basics

1. Be thorough but don’t overwhelm!
   – “Is this an awareness training or a graduate course?”

2. Train based on NEED, not simply to check boxes.
   – “I’m only sitting through this mess so we’ll be compliant.”

3. Training should fit the intended audience!
   – “Wait...I have a CCA from an RBAM, in an ESP and PSP, behind an AP, requiring a CVA, maybe requiring a TFE, that might lead to a NAVAPS, due to a SDT acting on a NOPR, to fend off an APT from PRC or DPRK?”
Be Thorough, but Don’t Overwhelm!

• If your training includes a syllabus, you’ve probably gone too far.
• If you send home progress reports for parent signatures, you’ve missed the point.
• If your entire security program is delivered on a single slide, you’re likely missing something.
• If you’ve decided to cut costs by combining motivational posters and compliance awareness training, you’re in trouble.
COMPLIANCE

Follow the rules so we don't have to pay a bunch of money.
Train for NEED, not for Compliance!

CIP Training Checklist:

<table>
<thead>
<tr>
<th>DUE DATE:</th>
<th>PROCEDURES</th>
<th>COMPLETE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate</td>
<td>Provide enough cool training gadgets to trick Kevin.</td>
<td>X</td>
</tr>
<tr>
<td>Regularly</td>
<td>Lie to Shon and say he really is a good looking man to win him over.</td>
<td>X</td>
</tr>
<tr>
<td>Maybe Tuesday?</td>
<td>Copy and paste the standards into PowerPoint.</td>
<td>X</td>
</tr>
<tr>
<td>After above</td>
<td>Assume people will happily read the PowerPoint.</td>
<td>X</td>
</tr>
<tr>
<td>All the time</td>
<td>Simply believe them when they say, &quot;Yep, I did it.&quot;</td>
<td>X</td>
</tr>
<tr>
<td>When able</td>
<td>Keep a few training records handy, and hope that's what they request.</td>
<td>X</td>
</tr>
</tbody>
</table>
Train Based on the Audience!

امتحـال تدريب عرض هذا.

Это соответствие подготовки презентации.

यह एक अनुपालन प्रशिक्षण प्रस्तुति है।

Se trata de una presentación de capacitación de cumplimiento.
Train Based on the Audience!

If a train left Chicago on Thursday going 30 mph, and another left Orlando on Friday going 10 mph, when would they intersect and why would you care?

If you issue a directive on a Saturday afternoon you must first mute the football game.

Firewall rules should be set to deny all, specific to port and protocol, unless you can name the capitals of all 50 states.

All visitors must be threatened with bodily harm before escorting in the PSP.

Reliability systems MUST be monitored at all times, except when lengthy breaks are really, really necessary.
Train Based on the Audience!

The Employee Hears:

“YOU MUST NOT EVER, EVER, EVER TAILGATE!”

The Employee Thinks:
KEYS TO SUCCESS:
(OR, HOW TO SEEK PERFECT TRAINING IN AN IMPERFECT WORLD OF STANDARDS).
Key Compliance Training Strategies

• Focus on what is needed for specific types of employees.
  – For example, excessive cyber security training for accounting staff is unnecessary.
  – Tailor training to the recipient.
  – ONE SIZE DOES NOT FIT ALL!

• Your firewall guys don’t need to be trained on three-way communication, and your operators don’t need to know deny by default!

• Develop, provide, validate, and track your training in a uniform, repeatable way.
  – Don’t reinvent the wheel each year!
Key Compliance Training Strategies

- Put the training in understandable terms.
  - Describe the rationale behind the activity.
  - Make it PRACTICAL!

- Think broadly but train narrowly.
  - Consider all facets of your program.
  - Develop training on each facet.
  - Match impacted and/or responsible personnel with each facet.
  - For example, consider your physical security program in its entirety, develop brief modules on each facet, and assign.
    - Security guards are trained to monitor; staff is trained to comply.
Key Compliance Training Strategies

• Finally, and most importantly, **FORGET THE STANDARDS!***
  – Your corporate security program, for example, should be the focus of your training efforts.
  – A well crafted training program is standards agnostic!
    ▪ Standards may change, but your training may remain the same if appropriately crafted.

• It’s your job to develop solid programs to meet current and future needs, and to train on those programs.

• Review your program and link it to the standards, don’t review the standards and create a program to satisfy them.

*Understanding that some specific requirements have illogical training needs!*
Philip Propes
Director, Compliance
ppropes@spp.org
501-614-3255