10/8/2014

NERC CIP Version 5 webinar series “Version 5 transition”

Housekeeping

- All attendees are automatically in “Mute”.
- If you have any questions, please type them into the questions panel.
- This webinar is being recorded and can be found on http://new.abb.com/us/about/nerc-cip-education after the live event.
- You will get a copy of this presentation in a follow-up email.
- Please take a few moments at the end of the webinar to answer the survey questions.

About the presenter(s)

- **Joseph Baxter**
  NERC CIP Lead – HVDC / FACTS
  joseph.baxter@us.abb.com
  (919) 807-5077
  Before coming to ABB, Joseph Baxter completed several years as a NERC CIP Auditor for the SERC region, with special emphasis on the technical side of cyber security. He has both audited and been audited in the realm of CIP, and brings over fifteen years of Information Security experience gleaned from the Financial Sector to bear on the problems facing Grid Security today.

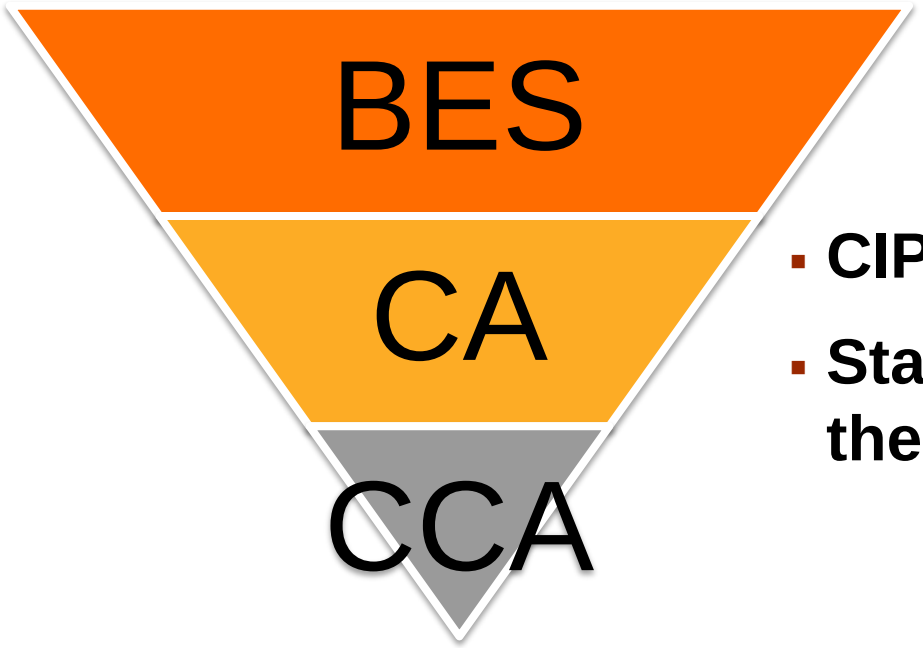
- **Tim Conway**
  EKC Consulting
  Technical Director ICS and SCADA programs at SANS. Formerly, the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO). Former Chair of the RFC CIPC, current Chair of the NERC CIP Interpretation Drafting Team, member of the NESCO advisory board, current Chair of the NERC CIPC GridEx Working Group, and Chair of the NBISE Smart Grid Cyber Security panel.

From the other side of the table
Audit tales

- **2009 Spot Check**
- **CIP-002-1 in scope**
- **One of our auditors knew just a little too much about our system**
- **Just how *did* that substation connect**

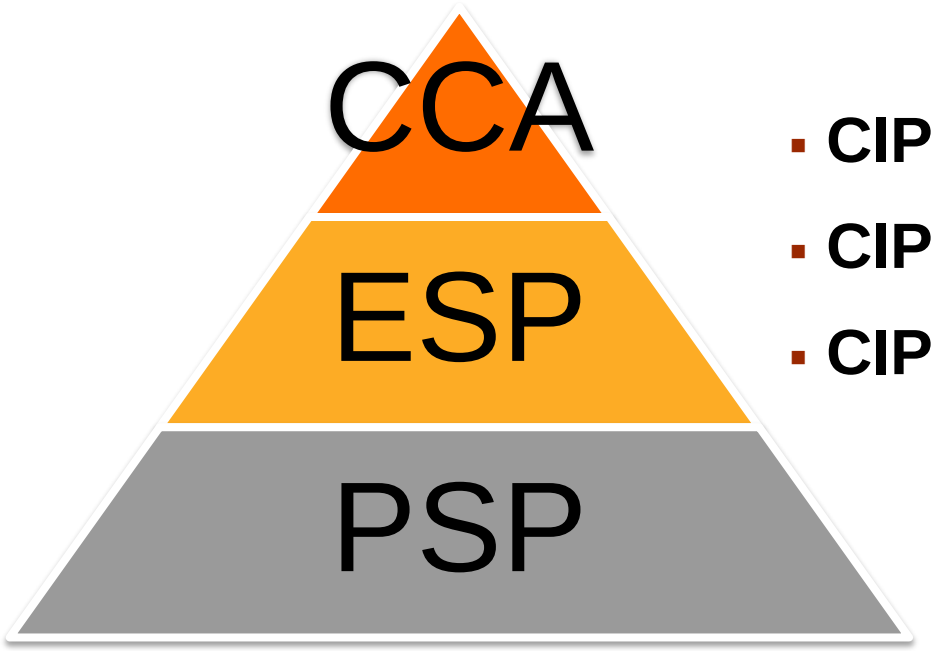
Audience Question #1
CIP Program

In the old days of CIP-002
A deductive process



- **CIP-002 Pilot Program**
- **Starting inventory always the problem**

CIP-005 and CIP-006
The inductive process



- **CIP-002 took things out**
- **CIP-005 declared an ESP**
- **CIP-006 declared a PSP**

Meant to be quantitative
Turned out qualitative

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

CIP Version 4
How the future became bright

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

The Metcalf Substation
A new standard

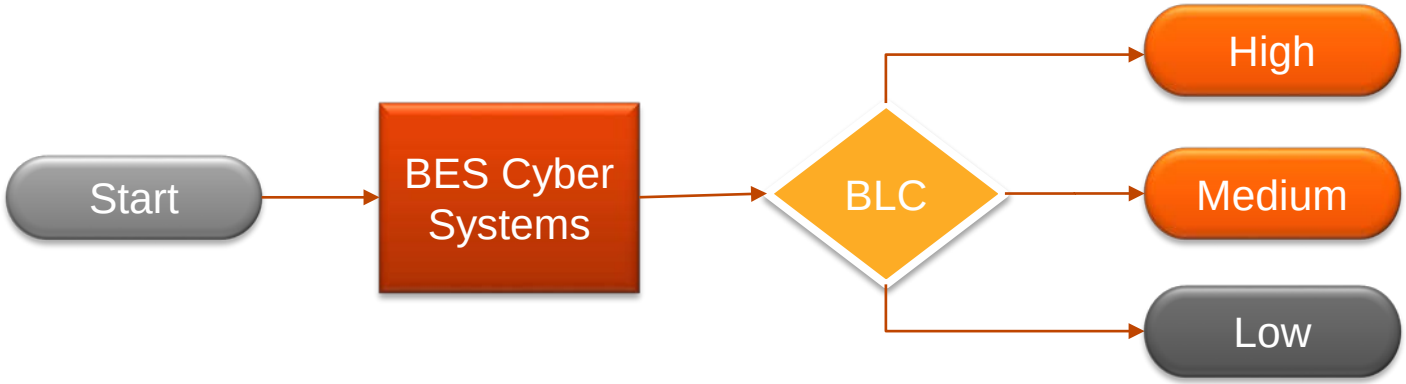
R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or

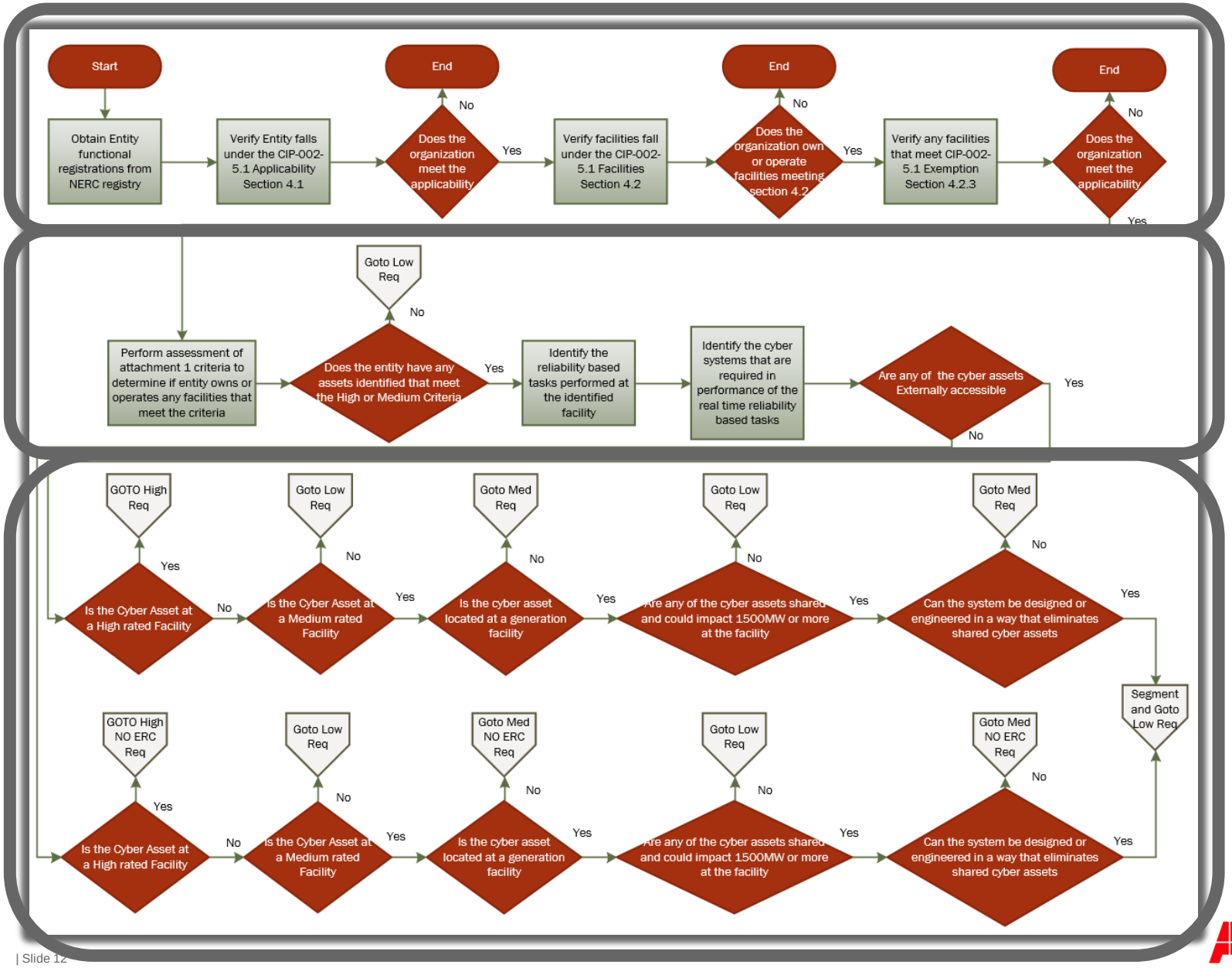
- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

CIP v5 BLC Simplified
The easy way



- **Well, maybe not quite *that* easy…**
- **A lot of moving parts exist inside that small yellow diamond labeled “BLC”**
- **Replaces my deductive pyramid**

The big picture



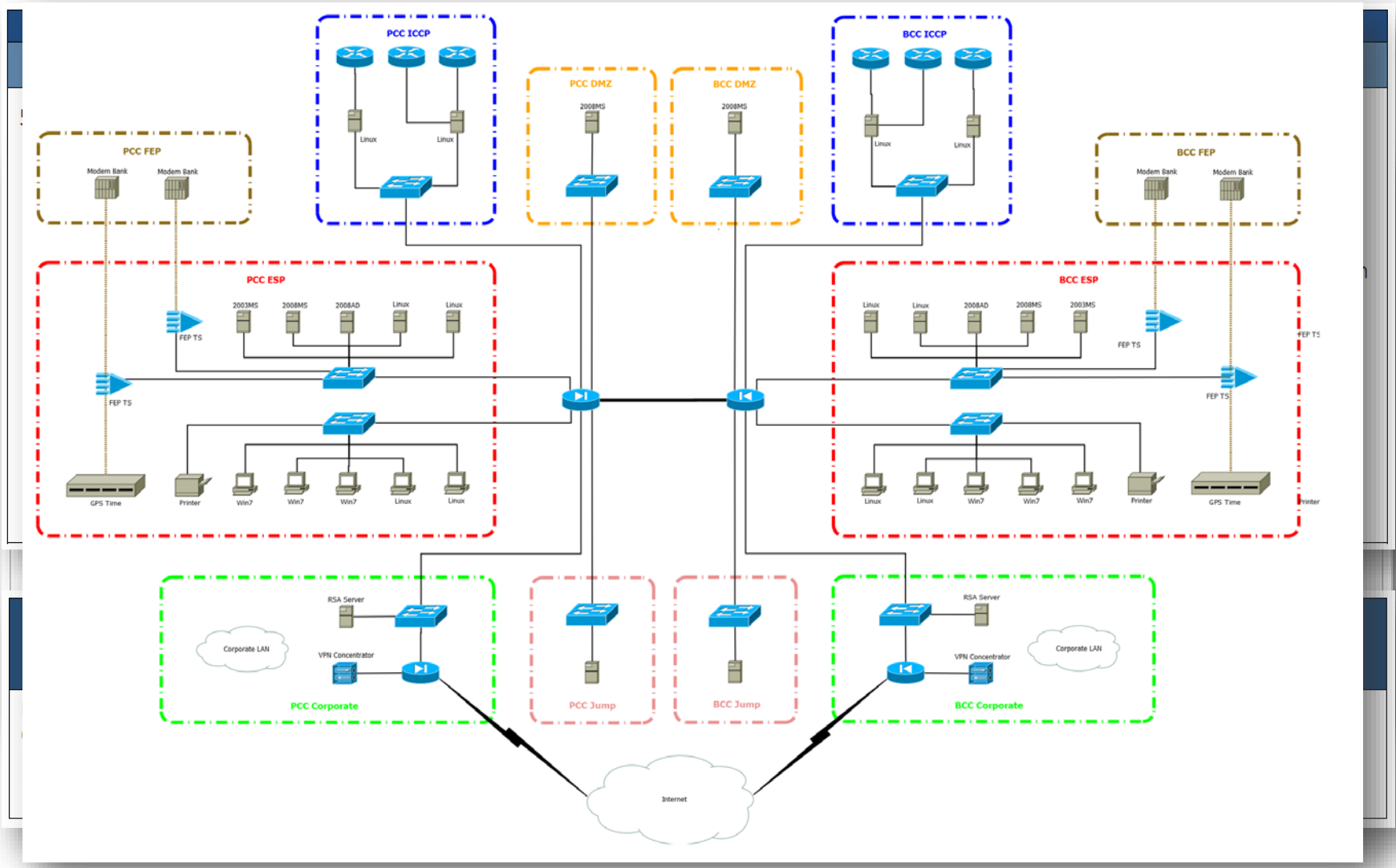
Audience Question #2
Asset Analysis

Impact Ratings
High, Medium, and Low

CIP-007-5 Table R1– Ports and Services			
Part	Applicable Systems	Requirements	Measures
			others.

CIP-010-1 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.5		Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

External routable connectivity
And what it means to you



Quality Evidence
Documentation is king

A	B	C	D	E	F	G
		10/5/2013 15:02				
ID	**1b) Device Hostname or Identifier**	**1c) Device IP Address or Layer 2 MAC address**	**1d) - CA**	**1e) PSP**	**1f) ESP**	**1g) CCA or Cyber Asset within an ESP**
1	*web01_B (example)*	*192.168.1.200*	*Ima Primary Control Center*	*SCC Data Center*	*EMS2 Segment*	*CCA*
2	*support_pc (example)*	*192.168.1.210*	*Anytown 500 kV sub*	*AT500 Control House*	*AT500_DNP*	*Cyber Asset within ESP*
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						

Additional NERC CIP educational webinars (All webinars are Eastern Time)

- **Change management**
  Wednesday, October 15, 2014 at 2:00 p.m.
  Learn about change management and the fact that this will be the largest area of recurring effort. You will gain understanding of why Patch Management is not a solution to meet your NERC CIP updates and why Version 3 no longer applies.
  Register now: https://www1.gotomeeting.com/register/567897657

- **Baseline management**
  Wednesday, October 22, 2014 at 2:00 p.m.
  Learn what a baseline and testing are, why automation is key and what is required to meet Version 5 compliance.
  Register now: https://www1.gotomeeting.com/register/937111497

- **Cyber asset grouping**
  Thursday, October 23, 2014 at 12:00 p.m.
  (Power generation specific) Learn process approaches to CIP-002-5.1 R1 as it pertains to BES cyber asset categorization.
  Register now: https://www1.gotomeeting.com/register/774616816

Additional NERC CIP educational webinars (All webinars are Eastern Time)

- **Access management and malicious software controls**
  Wednesday, October 29, 2014 at 2:00 p.m.
  Learn how to access control fits with CIP-004-5 and why account management is not effortless.
  Register now: https://www1.gotomeeting.com/register/448008129
- **Low assets and future CIP versions**
  Wednesday, November 5, 2014 at 2:00 p.m.
  (Power generation specific) Learn the compliance requirements for entities with low assets and audit worksheets as well as future standard activities.
  Register now: https://www1.gotomeeting.com/register/872327665
- **Identification and review of critical transmission assets**
  Wednesday, November 12, 2014 at 2:00 p.m.
  Learn how to approach the guidelines and criteria highlighted by NERC to fulfill the risk assessment goal.
  Register now: https://www1.gotomeeting.com/register/639963169

Automation & Power World (APW)
Power SmartStream Digital Conference

- **Theme:** **Preparing for the power evolution**
- **Date:** **November 6, 2014 – 11 a.m. – 6 p.m. EST**
- **Why should you attend?**
  25 educational webinars, dozens of scheduled chats and interviews and more than 100 white papers available for download from knowledgeable subject matter experts.
  - **Earn Professional Development Hours (PDH)**
    Download an official attendance certificate for every live webinar session you attend to get credit for your learning time
  - **No travel or registration costs!**
  - **Can't attend the day of?**
    That's fine. All webinars will be recorded and will be available for on-demand viewing after the live event.
- **Register now:** **http://bit.ly/SmartStreamPower**

Automation & Power World (APW) LIVE conference – APW 2015

- **Theme:** **Harnessing the power of change**
- **Date:** **March 2-5, 2015 in Houston, Texas**
- **Location:** **George R. Brown Convention Center**
- **Why should you attend?**
  - **Listen to interesting and topical keynote presentations**
  - **Chose from over 300 industry and solution-focused educational sessions and panel discussions**
  - **Network with ABB experts and your peers**
  - **Earn Professional Development Hours (PDH)**
  - **Completely free!**
- **Check the website for updates:** **http://new.abb.com/apw**

Questions?

This is the point to review and answer any questions in the panel. If you have a question, please type your question in now.

Survey

Please take a few moments to answer the survey questions.

Thank you.

Power and productivity
for a better world™