CAPER

Center for Advanced Power Engineering Research

2017 Summer Research Planning Workshop

Top Ten Elements of Enterprise CIP Program Management

Presented By:
Chad Cowan
Director – Duke Energy CIP Program Management

Top Ten Elements of Enterprise CIP Program Management

1. The threat is real – and it's growing
2. Just tell me what I have to do
3. What my boss finds interesting, I find fascinating
4. You won't get it right the first time
5. When will it be done, done, done?
6. You're speaking, but your words are not making any sense to me…
7. Burn down the Ivory Tower
8. Nothing bad happened, so no worries, right?
9. I can't make any sense out of all of these spreadsheets
10. How do I work myself out of a job?

CAPER

The threat is real – and it's growing

External

- *Ukraine targeted by nation-state cyber attack. Petya malware designed to destroy country's infrastructure while operating under the guide of Malware.*

- Asian, non-Chinese cyber espionage on the rise, particularly Vietnam.

-South Korean web hosting company pays $1 million dollars

Threat

- NSA Leaked "Vault 7" exploits continue to be weaponized by both amateur and professional hackers. Patching remains the most reliable defense.

- *Targeted email attacks continue to grow in sophistication. Attackers use social media to build convinces emails using the names of pets, children and colleagues.*

- Petya and WannaCry ransomeware infects 100's of companies around the world

- *Fired meter company employee shuts down meters in 5 US cities.*

Legislative

-President Trump signs executive order "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"

- ***Congress is becoming more interested in the security of gas pipelines given the dependency of the electric industry***

- ***Senate seeks military ban on Russian based Kaspersky Labs (anti-virus products) amid FBI probe.***

Utilities

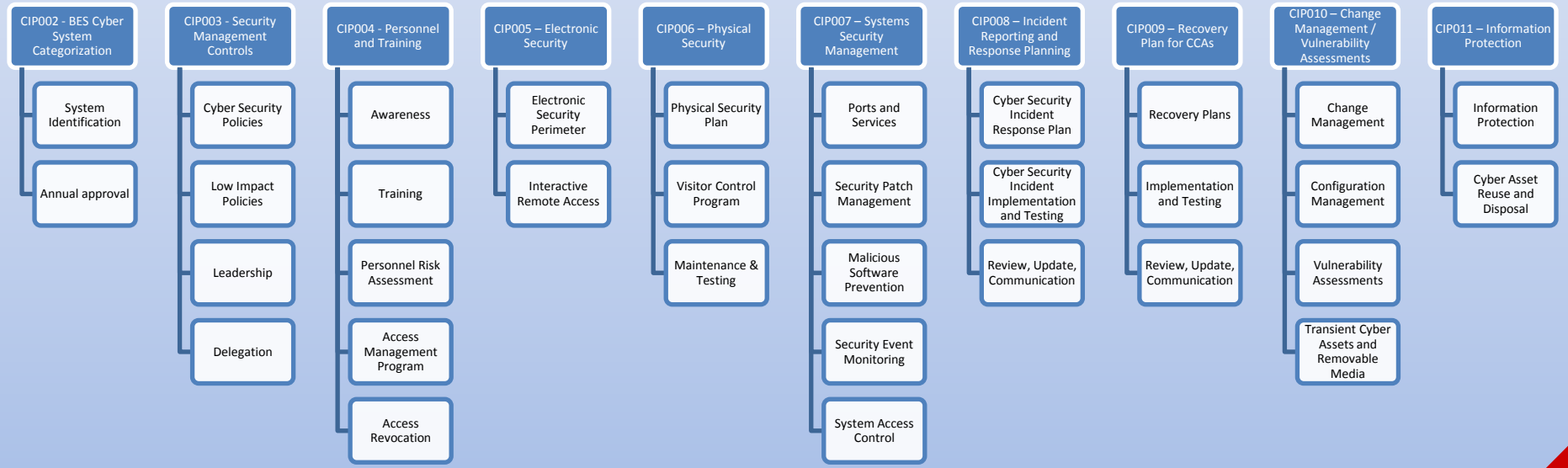
-Wolf Creek Nuclear Station in Kansas targeted (among other facilities)

-CrashOverride is "not unique to any particular vendor or configuration and instead leverages knowledge of grid operations and network communications to cause impact," Dragos' report finds, making it a flexible threat.

-Galina Antova, co-founder of Claroty, which focuses on industrial control system security, told Bloomberg that "we're moving to a point where a major attack like this is very, very possible."

CAPER

What is NERC CIP?



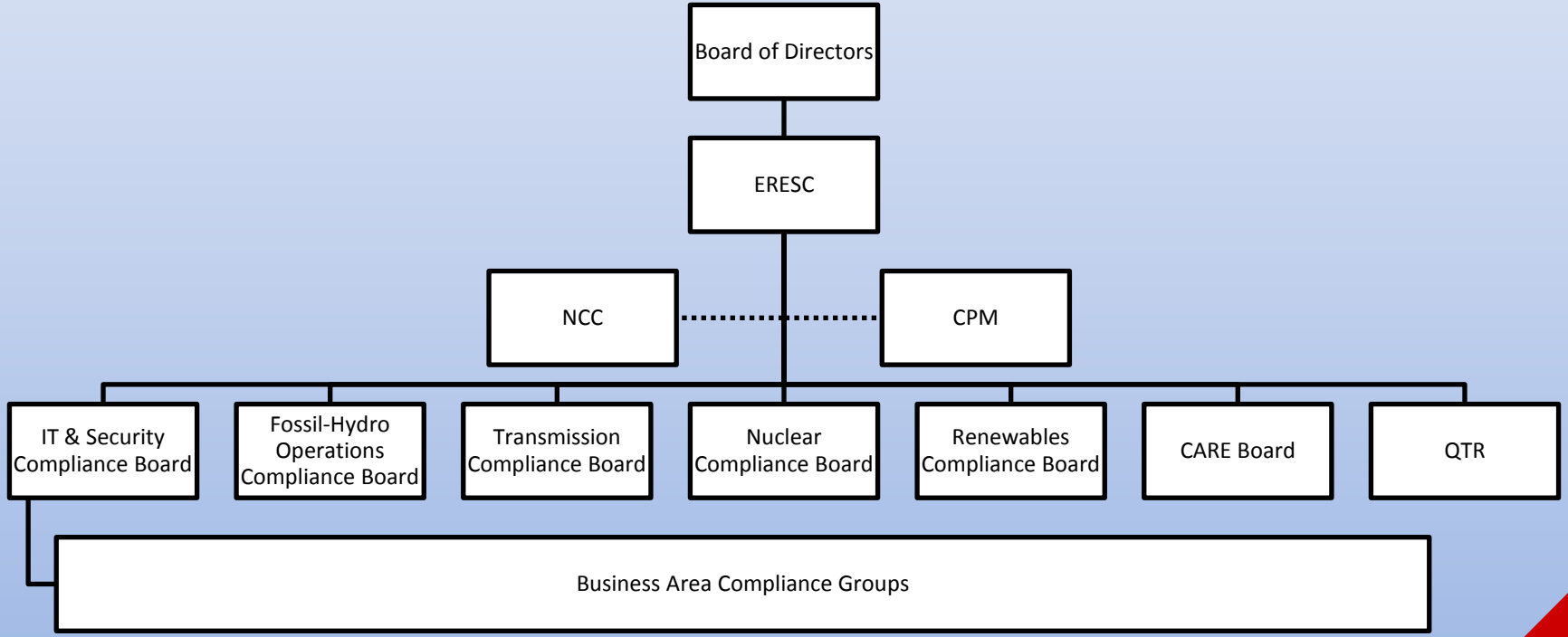
CAPER

Just tell me what I have to do

- What do you want your Enterprise program to be?
  - What degree of consistency is desired?
  - What vs. How?
  - Clearly establish:
    - What activities must be performed and when?
    - What evidence is required to demonstrate what was performed and what outcome resulted?
    - Operations (not just compliance) must be involved
  - NIST vs CIP
  - Implementation is where the rubber meets the road
- Being compliant isn’t enough
  - Move faster than the regulations
  - Understand the topology
  - Awareness and practice

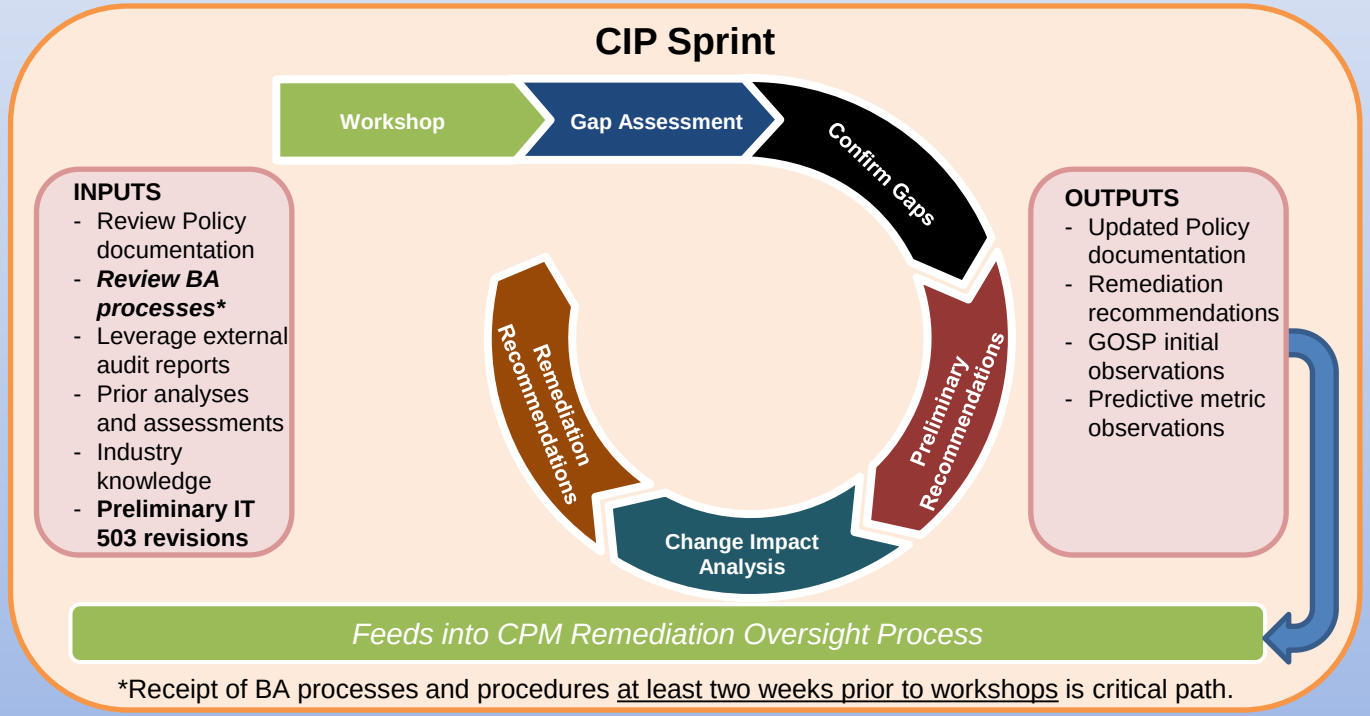
CAPER

What my boss finds interesting, I find fascinating



CAPER

You won’t get it right the first time



When will it be done, done, done?

- Established metrics for:
  - Implementation activities
    - Target Date / Actual Date
  - QA reviews
    - Target Date / Actual date
    - % passed
    - Date complete for remediation of outstanding issues
  - Issue Management
    - Time to enter possible violations into enterprise tool
    - Time to file Self Report (if required)
    - Time to complete Cause Analysis
    - Time to file Mitigation Plan
- Developing metrics around:
  - Mitigation Plan quality
    - % issues with recurring causes
    - % Mitigation Plans remanded
  - Operational compliance activities
    - % patch assessments completed
    - % annual CVAs completed
    - % annual access reviews completed

Indicator	Meaning
	On Target
	At Risk
	Late
	Complete

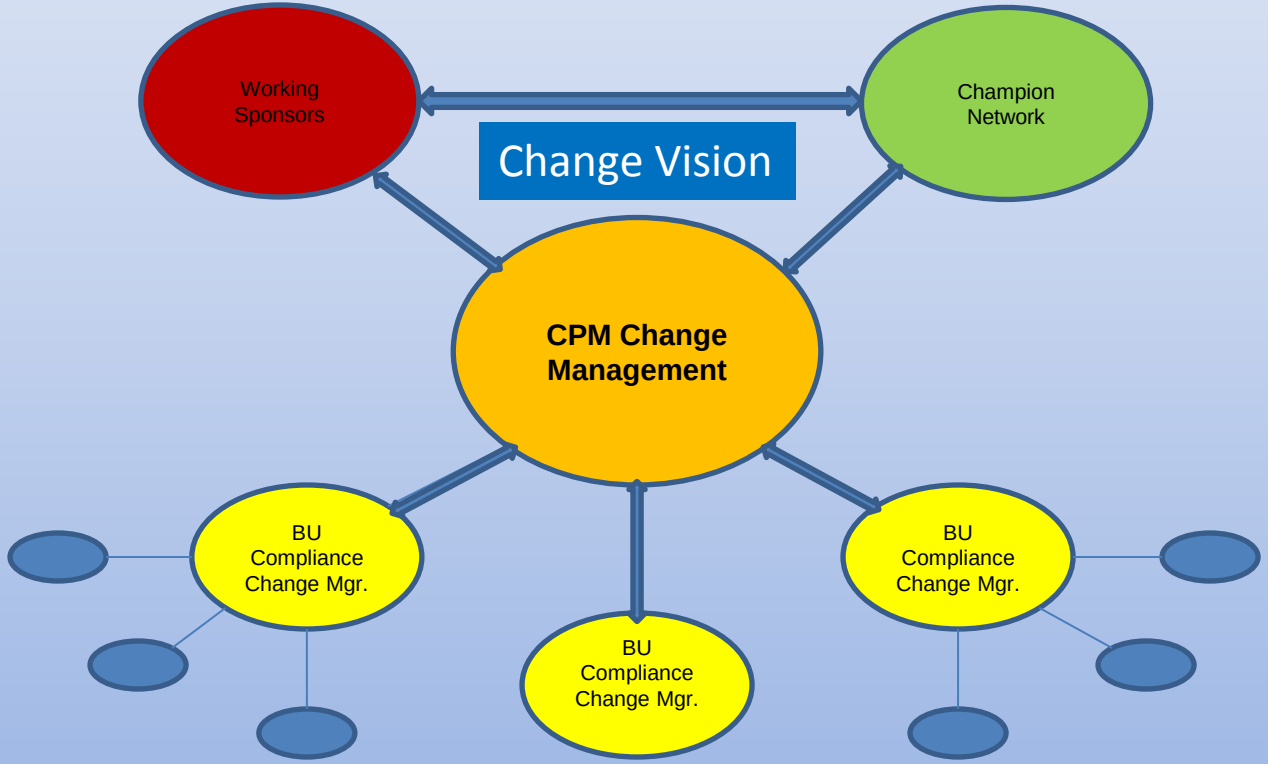
All updated dates require strikethrough:
~~7/31/2017~~ 8/28/2017

CAPER

You’re speaking, but your words are not making any sense to me…

- Communication easily gets lost in nuance, jargon and acronyms – especially in CIP
- Operational areas have to be aware of communications and provide input into them
- A sense of urgency needs to be established (when action is required)
- Leadership needs key points and clear actions (1-pager)
- Compliance needs to be explained in the context of operational activities
- Change and information needs to come from direct supervisors – not a central authority

Burn down the Ivory Tower



CAPER

Nothing bad happened, so no worries, right?

Purpose:

To assess the collective potential and actual risk to the bulk electric system (BES) as well as to identify lower level performance trends based on a collective review of events (e.g. - potential violations, audit findings, near misses, etc.). This meeting will also provide risk insights to allow prioritization of actions.

Agenda:

- Safety
- Review of events that occurred during the previous quarter (e.g. - potential violations, audit findings, near misses, etc.)
- Cognitive discussion to identify any performance trends warranting additional action (including lower risk trends in human performance etc.)
- Review of potential and actual risks associated with the examples and events discussed
- Develop trends / risk insight summary for the ERESC

Key Objectives:

- Provide a forum for collaborative risk identification and management for Duke Energy's NERC CIP program
- Increase the awareness of leaders and other personnel regarding risks of events, potential violations, near misses etc..
- Identify lower level performance trends that warrant additional evaluation and action.
- Prioritize Duke Energy mitigation activities based on assessed risk to BES.

Operating Model:

The QTR's mission is to manage risk and ensure sustainment of effective enterprise security and compliance programs.

- The team will be chaired by the CSO / CIP Senior Manager. Membership will be determined by the CSO. Membership should be representative of business areas throughout the enterprise to ensure appropriate collaboration and risk management.
- The team will meet as determined by the CSO, generally expected to be quarterly and as needed.
- The QTR may invite other subject matter experts and support staff as needed.
- Delegates are allowed. CSO will ensure meeting continuity is maintained.
- The QTR may commission subcommittees to investigate risk, make recommendations and support change.
- Results of QTR will be summarized and provided to the ERESC.

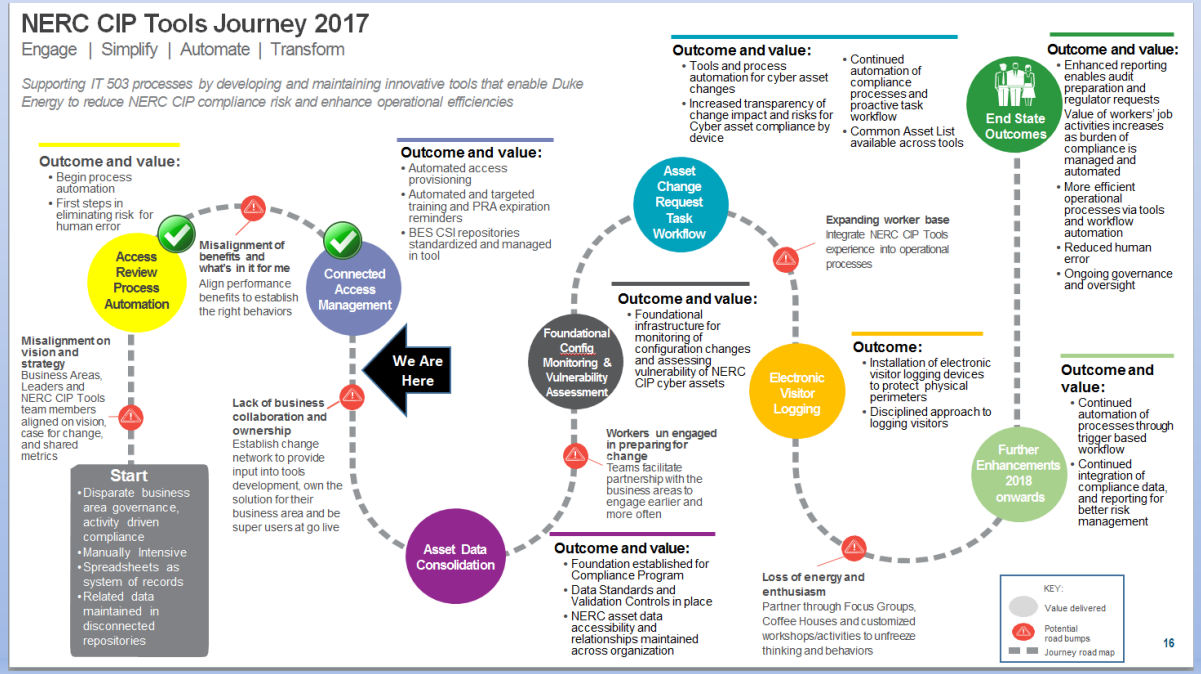
The Quarterly Trend & Risk Assessment established a forum to review issues (both self reports and "near misses") for potential impact to the Bulk Electric System

CAPER

I can’t make any sense out of all of these spreadsheets

NERC CIP Tools Program Vision:

“We are implementing tools for NERC CIP processes to protect and prove the reliability and security of the Bulk Electric System, increase operational and compliance process efficiencies, and reduce compliance risk for Duke Energy.



CAPER

How do I work myself out of a job?

- Compliance requirements and evidence are built into the fabric of operational activities (key components in the procedures, the tools, and the management oversight of each operational organization)
- Good cyber security practices are tied to operational reliability (security should be everyone's responsibility rather than something that is "done" to operations)
- Consistent expectations are set and enforced through continuous validation
- Senior leadership is engaged and has actionable data

CAPER

Thanks !

CAPER