SPP FALL COMPLIANCE FORUM – CIP V5 TRANSITION – LESSONS LEARNED
CIP-002

- Lessons learned with categorizing your assets?
  - Delineating Networks
    - Identifying applicable Cyber Assets/PEDs?
    - Group by System or Asset?
    - Tie Line Meters?
    - Group by System or Asset?
    - Accounting for Low Impact Cyber Assets at Medium Impact locations?
  - How did you validate items identified by RC or PC (2.3 and 2.6)?
• **What are your plans for securing Low Impact BES Cyber Systems?**
  o **Cyber Security Awareness**
  o **Physical Access Controls**
    o Substations?
    o Generation?
    o Wind Farms?
  o **Electronic Access Controls**
  o **Cyber Security Incident Response**
CIP-004

- How are you training on your Cyber security policies (2.1.1.)? What is the content of the lesson?

- What do you consider “authorization records” (4.2)?
  - What about personnel who were authorized prior to the effective date of the CIP Standards?
• How are you “detecting known or suspected malicious communications for both inbound and outbound communications” (1.5)?
  o Are you doing this between ESPs?

• Lessons learned with methods for Interactive Remote Access?
  o Are you using a digital certificate for multi-factor authentication at the intermediate system (2.3)?
  o Where are you storing the certificate?
CIP-006

• What is your visitor management process for identifying and documenting the “point of contact” (2.2)?
  o Do you allow it to be someone other than the escort?
CIP-007

• Have you had any challenges with identifying a complete vendor source list and ensuring each source is checked every 35 days?

• How do you ensure a patch tracking ticket wasn’t backdated and includes appropriate documentation as to whether patches were available?

• How are you verifying ports are closed before/after putting a device into production?
• Do you have any lessons learned with baselining all Cyber Assets (1.1.)?
  o Operating Systems?
  o Software?
  o Custom Software?
  o Logical ports?
  o Security Patches applied?

• How detailed is your documentation?

• Manual process?

• Automated process?

• Do you have any lessons learned with updating baseline documentation after a change (1.3)?

• Do you have any lessons learned with documenting the status of CIP-005 and CIP-007 controls after a change (1.4)?
• How are you managing information protection?
  o Classification?
  o In storage?
  o In transit?
  o In use?
  o Release to third parties?
Questions?