• Covered administrative details and confirmed quorum
• The SDT conducted a webinar on current and planned postings
• The SDT submitted to the Standards Committee modifications to CIP-002 as a proposal to address the issue identified by the V5TAG around Transmission Owner Control Centers (TOCC) performing the functional obligations of a Transmission Operator
  o Pending approval by the Standards Committee, CIP-002 will post in mid-September for a 45 day formal comment and ballot
• The SDT reviewed the status of issue areas identified by the V5TAG
• The SDT continued work reviewing and addressing issues on virtualization
  ▪ The SDT is actively moving towards an informal comment on virtualization
• The SDT heard an update on NERC’s approach to various forms of guidance that may be developed by the SDT including Technical Rationale and Justification documents and Compliance Implementation Guidance
The SDT reviewed the status of issue areas “CIPv5 Issues for Standard Drafting Team Consideration” (Commonly known as the “V5TAG Transfer Document”) document prepared by the V5TAG.

Some issues received treatment through “Lessons Learned” documents which were written by the V5TAG.

- The SDT noted that several of these “Lessons Learned” documents have been formally endorsed by the ERO as Compliance Implementation Guidance. Some relevant “Lessons Learned” documents are noted below:
  - CIP-002-5: BES Cyber Assets
  - CIP-002-5.1: Communications and Networking Cyber Assets
  - Communications to BES Cyber Systems and BES Cyber Assets

The SDT is continuing to evaluate how best to address the areas outlined in the V5TAG Transfer Document.
The SDT reviewed a draft informal comment form for virtualization.

The SDT discussed its work in the virtualization area:

- Potential introduction of new requirements to address risks associated with shared infrastructure for virtual technologies
- Treatment of centralized management consoles associated with virtualization and review of the EACMS definition to determine if changes to the current EACMS concept may be necessary to handle virtual technologies and the expanding availability of cloud-based advanced security services
- Given the expanding availability of cloud-based advanced security services, the SDT discussed considerations for treatment of BES Cyber System Information when stored in cloud environments
- Development of virtualization implementation guidance for currently enforceable CIP Standards
- Development of virtualization implementation guidance for any potential new virtualization requirements
ESZ definition

- The logical separation that enhances cyber security and reliability of one or more Cyber Asset(s);
- The logical separation of one or more Cyber Asset(s);
- The area defined by the logical separation of one or more Cyber Asset(s);

References

- The logical container providing separation or isolation from threats or attack vectors to grouped Cyber Assets, said Cyber Assets being characterized by similar operational criticality, or sensitivity to compromised data confidentiality and integrity, as well as needing similar access controls, audit logging and/or monitoring requirements.
- The logical entity to which one or more interfaces is bound. Security zones provide a means of distinguishing groups of hosts (user systems and other hosts, such as servers) and their resources from one another in order to apply different security measures to them.
  - Ref. Juniper Networks
• Applicable systems
  ▪ High Impact BES Cyber Systems residing in a Multi-instance environment and its associated CMS
  ▪ Medium Impact BES Cyber Systems residing in a Multi-instance environment and its associated CMS

• Part 1.6
  ▪ All Applicable Systems shall reside within one or more defined ESZs to mitigate the risk of unauthorized access, escalation of privilege, unnecessary span of control, and data leakage. At a minimum, per system capability, ensure separation of instances in distinct ESZs
    ▪ Between management plane and the data plane of the applicable BES Cyber Systems;
    ▪ Between the CMS of the applicable BES Cyber System and its data plane;
• Applicable systems
  - High Impact BES Cyber Systems residing in a Multi-instance environment and its associated CMS
  - Medium Impact BES Cyber Systems residing in a Multi-instance environment and its associated CMS
• Part 1.7
  - Identify and implement separation controls for each applicable ESZ
• Applicable systems
  - High Impact BES Cyber Systems residing in a Multi-instance environment and its associated CMS;
  - Medium Impact BES Cyber Systems residing in a Multi-instance environment and its associated CMS.

• Part 1.8
  - When an Infrastructure is shared between BES Cyber Systems and other Cyber Assets not part of any BES Cyber System:
    - The BES Cyber Systems, the management plane of the shared infrastructure, and any hosted Cyber Assets not part of the BES Cyber Systems shall reside in distinct ESZs;
    - Communications between the BES Cyber System and any hosted Cyber Assets not part of a BES Cyber System shall be controlled by an EAP
In the context of virtualization and the EACMS definition, the SDT reviewed the following redline to the current BES Cyber System Information definition:

**BES Cyber System Information**

Data about the BES Cyber System that is processed, organized, structured, or presented in a context that would make it useful could be used about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System.

BES Cyber System Information does not include individual pieces of information, data in its raw, unorganized form. This that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, includes, but is not limited to, device names, individual IP addresses without context, ESP names, or policy statements.

Examples of BES Cyber System Information may include, but are not limited to

- Security procedures, security logs, security configuration information, or security event information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that are not publicly available and could be used to allow unauthorized access or unauthorized distribution;
- collections of network addresses; and
- network topology of the BES Cyber System.
• FERC Order 822 directed NERC to develop standards that require the protection of communication links and sensitive BES data communicated between BES Control Centers

• The SDT explored many avenues for the directive, including
  ▪ Explicit scoping of data vs. entity scoping of data
  ▪ Objective vs prescriptive requirements
  ▪ Models based on the risk of data and the impact level of an entity’s Control Center

• Informal comment held in early spring 2017 seeking industry feedback on various concepts

• Current CIP-012-1 proposal is objective based with data scoped to align with currently approved O&P standards.
**Requirement R1.** The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers. This excludes oral communications. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

1.1. Risk mitigation shall be accomplished by one or more of the following actions:

- Physically protecting the communication links transmitting the data;
- Logically protecting the data during transmission; or
- Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data.

Note: If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity.

**Requirement R2.** The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.
Control Center:
One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and host hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to who perform the Real-time reliability related tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

For Reliability Coordinators, Balancing Authorities and Transmission Operators, the operating personnel above are System Operators.

For Transmission Owners performing the Real-time reliability related tasks of a Transmission Operator, the operating personnel above consist of personnel, excluding field switching personnel, who can act independently to operate or direct the operation of the Transmission Owner’s Bulk Electric System transmission Facilities in Real-time.

For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator’s Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and have the capability to develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.
• The Project 2016-02 SDT’s Standard Authorization Request states that the SDT shall address:
  ▪ The applicability of requirements on a TO Control Center (TOCC) that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES
  ▪ The definition of Control Center
  ▪ The language scope of “perform the functional obligations of” throughout the Attachment 1 criteria
• The TOCC issue relates to the language developed by the Project 2008-06 Cyber Security Order 706 Standards Drafting Team (706 SDT)
• The Project 2016-02 SDT must consider the issue based on the language of FERC Order No. 706 and the intent of the 706 SDT as well as FERC’s reiterated position in FERC Order No. 761
CIP-002, Attachment 1, Criterion 2.12

Control Centers or backup Control Centers, not included in High Impact Rating (H) above, that monitor and control BES Transmission Lines with an "aggregate weighted value" exceeding 6000 according to the table below. The "aggregate weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center.

**continued in table on next slide**
<table>
<thead>
<tr>
<th>Voltage Value of a Line</th>
<th>Weight Value per Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>less than 100 kV (not applicable)</td>
<td>(not applicable)</td>
</tr>
<tr>
<td>100 kV to 199 kV</td>
<td>250</td>
</tr>
<tr>
<td>200 kV to 299 kV</td>
<td>700</td>
</tr>
<tr>
<td>300 kV to 499 kV</td>
<td>1300</td>
</tr>
<tr>
<td>500 kV and above</td>
<td>0</td>
</tr>
</tbody>
</table>
Next Steps

- Post formal ballot and comment for TOCC
  - Posting tentatively scheduled for mid September
- Post informal comment for Virtualization
  - Posting tentatively scheduled for early October
- Prepare formal ballot and comment for CEC
- Address comments received from formal ballot on CIP-012 (CommNet)
- Address comments received from informal posting of Control Center Definition and CIP-012 Technical Rationale
Conference Call Schedule

Conference Dial-in
- See NERC calendar for WebEx info

Reserved Call Times
- Fridays - 11 a.m. – 1 p.m. (ET)
  - Full team update

Discussion topics will vary based on the issue area work progress.

Check the NERC Standards calendar of events for the most updated information.

Issue Area Working Calls--Scheduled if needed on the NERC Standards Calendar
- Tuesdays - Noon – 2 p.m. (ET)
  - Issue area working session
- Thursdays - Noon – 2 p.m. (ET)
  - Issue area working session

Issue area working calls will be scheduled as needed to allow the sub-teams to process input and develop proposals.
2017 Planned Dates:

- September 19-21– Kansas City, MO – KCP&L

- **ALL REMAINING MEETINGS WILL BE SCHEDULED BASED ON POSTING TIMELINES**
  - October
  - November
• Information relative to the CIP Modifications project and SDT may be found on the Project 2016-02 Project Page under Related Files:

  Project 2016-02 Modifications to CIP Standards
Questions and Answers