

**Questions for SERC's 3rd Quarter 2010 Open Forum
August 16, 2010**

1. Two questions concerning jointly-owned BES assets:
 - a. One registered entity has delegated compliance responsibilities to a second registered entity for a jointly-owned transmission asset. A written delegation agreement exists. Does the delegating entity need any other evidence to demonstrate compliance with applicable standards?
 - b. One registered entity has delegated compliance responsibilities to a second registered entity for a jointly-owned generating unit, which the second entity operates. The operating entity has provided letters of attestation to the delegating entity. Does the delegating entity need any other evidence to demonstrate compliance with applicable standards?
2. Is a computer accessing a Critical Cyber Asset (CCA) remotely also a CCA? If it is a CCA, do all of the same Physical Security Perimeter requirements apply? Some guidance suggests that NERC and the regions would answer the first question by saying that it depends on the intended use of the computer. If the computer is intended for use to provide technical support, it is not a CCA, but if it is intended to be used for operations, it is a CCA. Importantly, computers used to provide technical support could require administrative rights such that the technical support computer's rights could include the ability to escalate privileges to allow operational control from that computer, even though that control is not actually used. Also, does the answer change based on whether or not dual factor authentication and VPN encryption are already in place?
3. Regarding VAR-002 Requirement 3, is a change in an AVR set point considered a status or capability change?
4. CIP-006-3, R1.6.1 states that a Responsible Entity must have "Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters." If a person enters and exits the same PSP multiple times in one day (e.g., employee without authorized unescorted physical access who is performing routine maintenance on CCAs), is it necessary to record each entry and exit, or is it sufficient to record the initial entry and final exit from that PSP?

5. Should a perimeter firewall be considered a CCA, an Access Point, an Access Control and Monitoring Device, or all of the above?
6. What types of systems are in scope for Access Control and Monitoring Systems (CIP-005)? Specifically, are the following included:
 - a. Upstream Patch Servers outside of the ESP used to pull patches into the ESP and monitor deployment?
 - b. Upstream Antivirus Distribution Servers outside the ESP used to pull Virus Signature into the ESP and monitor deployment?
 - c. Central Logging Systems outside the ESP where logs are sent from the ESP to be stored centrally?
 - d. Authentication Systems outside the ESP that provide access to or through the perimeter firewalls or access points?
7. Would it be possible to include a presentation of the DATA REPORTING, GENERATOR TESTING, SERC Portal screen for MOD-024/025 (for the October 1 data reports)? It's just not a user-friendly data submittal screen.
8. One entity is registered as a TOP, TO, and several other functions. This entity routinely supplies information required by IRO-004 for itself and for a second entity (which is registered as a TO, DP, and LSE). The second entity was recently audited by SERC. During the second entity's audit, the first entity was asked to provide supporting evidence for Requirement 4 of IRO-004 which states:

"Each Transmission Operator, Balancing Authority, Transmission Owner, Generator Owner, Generator Operator, and Load Serving Entity in the Reliability Coordinator Area shall provide information required for system studies, such as critical facility status, load, generation, operating reserve projections, and known Interchange Transactions. This information shall be available by 1200 Central Standard Time..."

During the audit, the audit team asked the first entity to provide documentation confirming that system changes were logged into the Reliability Coordinator's models for July 15, 2009, September 24, 2009, and March 11, 2010 so that system studies could be performed by the Reliability Coordinator. (The Reliability Coordinator was not a party to this audit.)

Under Section D Compliance, subsection 1.3, the data retention period is stated:

"Documentation shall be available for 3 months to provide verification that system studies were performed as required."

Two of the dates clearly fell outside this 3 month retention period. Can the audit team select any date that falls within the audit period, regardless of the data retention period stated in the standard? Or must the selected date honor the data retention?