

Frequently Asked Questions  
Critical Infrastructure Protection  
SERC Reliability Corporation  
July 8, 2008

- 1) **Question:** When a single registered entity has a Critical Asset and/or a Critical Cyber Asset (“CA/CCA”) that is shared by two or more of its registered functions, what is the proper method of reporting this on the self-certification forms?

**Answer:** The registered entity assigns one of its responsible functions (e.g. TOP) to be the primary responsible function for this shared CA/CCA and the primary responsible function reports this CA/CCA and the status towards compliance.

The other function (e.g. LSE) who is sharing this CA/CCA should indicate that they have no CA/CCA but add a comment that this CA/CCA is shared with and covered by the primary responsible function. [NOTE: If the other function has a CA or CCA that is not shared, the CA/CCA and the function’s status towards compliance for the CA/CCA must be reported separately.]

- 2) **Question:** When multiple registered entities have a Critical Asset and/or a Critical Cyber Asset (“CA/CCA”) that is shared (jointly owned) by multiple registered entities, what is the proper method of reporting this on the self-certification forms?

**Answer:** Both registered entities must report the CA/CCA and both registered entities must report their own status towards compliance.

- 3) **Question:** A single registered entity has identified a list of critical assets. The critical assets do not relate to some of the registered functions, e.g. IA and LSE. What is the proper method of reporting this on the self-certification forms for the IA and the LSE?

**Answer:** If the IA and the LSE do not own, operate or use the critical assets, then they should not report those critical assets on their self-certification forms.

- 4) **Question:** By answering “No” to question #6 on the self-certification form, the CIP-003 through CIP-009 lines disappear from the Status section. However, all functions must be in compliance with CIP-003 R2 (assign a Senior Manager with overall responsibility), how do we report our status on CIP-003 R2 after the line disappears?

**Answer:** Complete the text box found below question #6, “Please identify the senior manager or delegates who approved the risk-based methodology, list of critical assets, and list of critical cyber assets for this function”. By entering the names of the approving individuals indicates the function status for the requirement set forth in CIP-003 R2.

- 5) **Question:** If a registered entity is on the Table 3 implementation timeline, can the registered entity put a future date in response to question #5 (When did you last perform the assessment to identify critical assets?)?

**Answer:** Yes, you can put a future date in for question #5. A date is required to be entered for question #5. [Note: For Table 3 entities, if the future date is later than December 31, 2009 you must provide an explanation in the field adjacent to CIP-002-1 R2. Penalties and sanctions may be applicable if the assessment has not been performed by December 31, 2009.]

- 6) **Question:** My registered entity needs the forms for the BA-SCC and TOP-SCC but not the BA-Other and the TOP-Other forms. Do I only fill out the forms for the BA-SCC and the TOP-SCC?

**Answer:** No, you need to fill out the BA-Other and the TOP-Other forms even though you have no facilities for these functions. In effect, your risk-based methodology found no facilities. Provide an explanation in the Additional Comments field at the bottom of the form. You should retain documentation of the determination that there are no “other facilities.”

- 7) **Question:** Can you help me understand TOP-Other (Facilities)?

**Answer:** TOPs that were required to self-certify to UA Standard 1200, must use Table 1 as your implementation schedule for the CIP Standards. The TOP/SCC form is used to self-certify your System Control Center (SCC). The TOP-Other form is used for all other facilities (excluding the SCC). For example, the TOP will usually have Cyber Assets (e.g. relaying equipment) located in substations. And usually, the TOP will have remote access to these Cyber Assets via dial-up or WAN. In this case, the TOP-Other form will be used to self-certify compliance on these (Critical) Cyber Assets that are located in substations determined to be Critical Assets by the Risk-based Assessment Methodology.