









***Observation***

Study participants noted that the CIP version 5 Reliability Standards did not sufficiently define the “programmable electronic device” component of the BCA NERC Glossary term, and the considerations provided in this lesson learned helped the study participants to assess and identify their Cyber Assets.

***Referral to Standards Development***

The transition study participants found a lack of clarity in the CIPV5 Reliability Standards because they do not specifically define the “programmable electronic device” component of the BES Cyber Asset NERC Glossary term. Consequently, the CIP V5 Transition Advisory Group referred the identified issues to be evaluated for standards development.

**Relevant NERC Glossary Terms**

**BES Cyber Asset** – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, A Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

**BES Cyber System** – One or more BES Cyber Assets logically grouped by a Responsible Entity to perform one or more reliability tasks for a functional entity.

**Cyber Assets** – Programmable electronic devices, including the hardware, software, and data in those devices.