Solar generation sites with a gross plant/facility aggregate nameplate rating greater than 75 MVA meet the North American Electric Reliability Corporation (NERC) registry criteria and are considered part of the Bulk Electric System (BES). Owners and operators of sites of facilities greater than 75 MVA connected at 100 kV or higher generally must comply with the applicable NERC Reliability Standards—both for Operations & Planning (O&P) and Critical Infrastructure Protection (CIP). Pursuant to the CIP Reliability Standards, solar facilities are considered low impact and must comply with CIP-003-6.

Low impact refers to BES Cyber Systems and facilities not already identified as high impact or medium impact per the CIP-002-5.1 impact categorization process.

Per the CIP-003-6 requirements, applicable entities are required to have the following documentation to support the protection of low impact BES Cyber Systems and facilities:

- Cyber Security Plans and Policies that address:
  - Cyber Security Awareness
  - Physical Security Controls
  - Electronic Access Controls
  - Cyber Security Incident Response

NERC Terms to Know

- BES Cyber System
- Low Impact BES Cyber System Electronic Access Point (LEAP)
- Low Impact External Routable Connectivity (LERC)

*For definitions, refer to the published NERC Glossary of Terms.*
Building a Compliant Program

To achieve compliance with the low impact requirements, an entity must pursue a holistic approach to cyber and physical security. Facilities and assets must be evaluated thoroughly to ensure protection that is both appropriate and sufficient. Additionally, processes and procedures must be designed logically for the unique operating environment, taking into account all impacted parties, technology, and equipment.

An entity will need to demonstrate that the potential risks to the organization and the Bulk Electric System as a whole have been properly mitigated via physical and electronic controls, personnel awareness, and a dedication to an overall culture of compliance.

With the implementation timeline determined by NERC, the program development and implementation activities can be backed up to the enforcement dates. However, there is no penalty for implementing a program earlier than the established dates. An organization can benefit from the opportunity to test and refine controls and documentation prior to formal enforcement.

**JULY 1, 2016**
- CIP V6 Enforcement (High/Medium Impact)

**APRIL 1, 2017**

**SEPTEMBER 1, 2018**
- Process Implementation of Physical & Electronic Security Plans that address LERCs & LEAPs