Criterion 3 - Adequacy of the Technical Approach for Addressing Interoperability and Cyber Security

Applications will be evaluated on the adequacy of the plans for addressing interoperability and cyber security.

The Project Plan's technical approach for interoperability will be evaluated as to how clearly it provides a description of the automation component interfaces (devices and systems), how integration is supported to achieve interoperability, and how interoperability concerns will be addressed throughout all phases of the engineering lifecycle, including design, acquisition, implementation, integration, test, deployment, operations, maintenance, and upgrade.

The Project Plan's technical approach for cyber security protections will be evaluated as to how clearly and concisely it provides a description of how cyber security concerns will be addressed throughout the project. Of particular concern in the evaluation will be the integration of the new smart grid application into the existing environment, and how any new cyber security vulnerabilities will be mitigated through technology or other measures. Although sensitive cyber security details that would jeopardize system security if they were exposed should not be revealed in the application, sufficient detail should be included to judge the project on its cyber security merits.

DOE may not make an award to an otherwise meritorious application if that application cannot provide reasonable assurance that their approach to cyber security will prevent broad based systemic failures in the electric grid in the event of a cyber security breach.

Opportunities to Earn a High Technical Merit Rating for Criterion 3

With respect to interoperability, project applications have the opportunity to earn a higher technical merit rating when the Project Plans clearly and concisely address the following:

- The information exchange interface points for each type of communicating automation device and system.
- The reasonableness of the openly-available and proprietary aspects of the interface specifications.
- Where a type of communicating device or system is expected in large numbers (e.g., meters, sensors, customer interfaces), the extent of support for multiple suppliers who will integrate their devices or systems that may be based on different technologies at the points of interface.
- If existing (legacy) communicating devices or systems are integrated into the project, the extent to which they integrate and interoperate at the points of interface with new components.
- The reasonableness of the interacting parties' anticipated response to failure scenarios, particularly loss of communications, such that overall system impact is mitigated in the event of such failure.
- The reasonableness of the anticipated process for upgrading devices or systems (hardware and software) so that overall system operation impact is mitigated.
- The extent of the evidence that will be provided (interface specifications, interoperability test plans and results, reviews, and other engineering artifacts) to ensure interoperability at the interfaces of communicating automation devices and systems.

- The reasonableness of the project's ability to support compatibility with NIST's emerging smart grid framework for standards and protocols as information becomes available.

With respect to cyber security, project applications have the opportunity to earn a higher technical merit rating when the Project Plans clearly and concisely address the following:

- The methodology used to identify cyber security risks and the results of this assessment (e.g., the assessment should consider the mission of the new smart grid project and also potential impacts to other critical grid control functions to which they are connected).
- How cyber security risks will be mitigated at each phase of the engineering lifecycle, including policy, procedural, and technical (logical and physical) controls, with special emphasis on strategies for:
  - ensuring the confidentiality, integrity, and availability of device and system data and communications commensurate with the application requirements,
  - securing, logging, monitoring, alarming, and notification, and
  - applications where logical and physical security may not be under the direct jurisdiction of the installing entity.
- The relevant cyber security standards or best practices that will be used.
- The capability of the components or system to be updated to meet future cyber security requirements or technologies.
- How evidence will be provided (e.g., a test plans, engineering artifacts, independent testing and review) to demonstrate and validate the effectiveness of the cyber security controls.