SUPPLEMENT TO CUSTOMER'S
SMART GRID TEST BED INITIAL APPLICATION FORM

Customer must submit this Supplement after approval of the Smart Grid Test Bed Initial Application Form and provide all detailed information requested by Ameren regarding the Customer's proposal. Please attach any information that you believe would assist with reviewing your application.
Á
Email this form to: TAC@ameren.com

Supplemental Information

AN ENGINEERING ASSESSMENT FEE OF $400 MUST BE SUBMITTED ONLINE using the PAY NOW button
WITH THIS SUPPLEMENT BEFORE ANALYSIS OF CUSTOMER'S PRODUCT CAN CONTINUE.

Customer Contact Information

Company Name: _____

Name: _____

Mailing Address: _____

City: _____ State: _____ Zip Code: _____

Telephone (Daytime) _____ Cellular: _____

Facsimile Number: _____E-Mail Address: _____

Alternate Customer Contact Information

Company Name: _____

Name: _____

Mailing Address: _____

City: _____ State: _____ Zip Code: _____

Telephone (Daytime) _____ Cellular: _____

Facsimile Number: _____E-Mail Address: _____

Provide a Detailed Description of Services to be Performed by Ameren:

_____

_____

_____

_____

_____

_____

_____

Provide the Testing and Analysis Objectives:

_____
_____
_____
_____

Explain all use cases that Ameren will cover under the Services:

_____
_____
_____
_____
_____

Explain and identify all equipment, actors and participants planned for the Product test environment:
(These should represent the devices, systems, software, and users etc. of the technology to be tested. Identify which is to be Customer provided and those that are to be provided by Ameren.)

_____
_____
_____
_____
_____

Provide a diagram showing the desired connectivity requirements for the equipment, each actor and participant in the use case(s) to be tested.

Identify all communication needs. (Include the required layers of the OSI model for each interface needed in the Test Lab environments, i.e. twisted pair Ethernet 100Mbps, TCP/IP, UDP, DNP3 for device number 1, interface number 1, etc.)

_____
_____
_____
_____
_____
_____
_____

Confirm the below security requirements are included in your solution by providing a statement explaining why you believe the criteria is met and providing any information necessary to verify your answer.

(If you do not include these requirements, please explain.)

- Proof that the firmware in use is and always has been the same approved version.

  _____
  _____

- Centralized authentication and authorization of field devices and users using third party methods (e.g. TACACS, RADIUS, etc.) for authentication.

  _____
  _____

- Discrete and full separation of any networks (company/customer) at the meter.
  _____
  _____

- Local tamper detection of field devices via FIPS 140-Level 2
  _____
  _____

- Ability to encrypt data in-flight or at rest as needed.
  _____
  _____

- Centralized key and certificate management system.
  _____
  _____

- Automated patch and firmware management system with ability to roll back to last patch or firmware level on failure.
  _____
  _____

- Ability to provide non-repudiation for access to all components to the system.
  _____
  _____

- System monitoring with ability to log security changes, use of access rights, system changes, system state and anomalous system behavior on all devices included in proposed solution.
  _____
  _____

- Ability to verify integrity of data used for automation of physical systems.
  _____
  _____

- Ability to send all logs to syslog.
  _____
  _____

- Secure/Encrypted management interface.
  _____
  _____

- System has been developed using the Systems Development Lifecycle (SDLC) methodologies including regular auditable penetration testing by third party testers.
  _____
  _____

- Support for Virus and Malware detection systems.
  _____
  _____

- Ability to set a standard password policy across the system that matches Ameren Illinois password policy (password length, complexity and change frequency) with ability to disable accounts after set amount of invalid Logins for set length of time.
  _____
  _____

- Guaranteed confidentiality.
  _____
  _____

- Ability to encrypt data across all wireless methods included in system.
  _____
  _____

Describe the remote access requirements for the Product.

_____
_____

Describe the requirements related to data gathering for the Product.

_____
_____
_____
_____

Describe any unique requirements that may be necessary for the Product.

_____
_____
_____
_____
_____
_____

Describe the level of maturity of the Product.

(For example, is it generally available in the market, only deployed in pilots, academic, or lab only?)

_____
_____
_____
_____
_____

Describe the interoperability and cyber security standards incorporated into the Product.

(Has any third party testing in these areas been completed? Is the Product certified against these standards?)

_____
_____
_____
_____
_____
_____

Provide Device/System/Program certification-: (What entities have certified the technology – IEEE, ASTM, UL, etc. and what certification was provided?)

_____
_____
_____
_____
_____

Provide the test procedures that have been defined and written for each use case. (Attach to this Supplement).

 _____
_____
_____
_____

Provide any Devices/Systems/Software/Sensors required to perform the requested testing or analysis. (If not provided or described above.)

_____
_____
_____
_____
_____

Provide the Proposed Timeline and Activities:

(Attach a proposed schedule to this Supplement, e.g., Gant chart depicting key activities)