ATTACHMENT B

AMEREN ILLINOIS CYBERSECURITY TERMS AND CONDITIONS

The clauses identified in this Attachment B are hereby incorporated and made a part of the referenced Subcontract between Leidos Engineering, LLC ("Leidos") and Subcontractor or Supplier. In all such clauses, unless otherwise specified, the term "Ameren Illinois" as defined below shall mean "Leidos" as defined in the Subcontract and the term "Supplier" as defined below shall mean "Supplier" as defined in the Subcontract. The term "Agreement" shall mean the "Subcontract" and attachments.

It is intended that the clauses shall apply to Supplier in such a manner as is necessary to reflect the position of Supplier as a subcontractor to Leidos, to ensure Supplier's obligations to Leidos in meeting its obligations under its prime contract agreement with Ameren Illinois.

Definitions

"Ameren Data" shall mean any data and information, regardless of form or medium, used, accessed, processed or available for any use by Ameren or its Affiliates (including Ameren Affiliates) or by an authorized third party, and shall broadly include any and all Ameren-owned or licensed data or intellectual property, confidential or proprietary data or information or operational or financial data or information of Ameren or its Affiliates (including Ameren Affiliates), customer data, employee data, retiree data, shareholder data, and privacy data including , but not limited to, one or more of the following types of data: (a) Cardholder data as defined in the Payment Card Industry ("PCI") standards as the credit card account number or Primary Account Number ("PAN"), cardholder name, card expiration date, and the service code; (b) Electronic Protected Health Information ("ePHI") – any protected Personal Health Information ("PHI") which is stored, accessed, transmitted, or received electronically; (c) Energy Usage – electric and natural gas usage data gathered by Ameren's metering systems; (d) Personal Information, as defined below; (e) Non-Public Personal Information – as defined in the Gramm-Leach-Bliley Act of 1999; (f) Protected Health Information ("PHI") – as defined in the Health Insurance Portability and Accountability Act ("HIPAA") or personal health information that identifies an individual and relates to an individual's past, present, or future physical or mental health, the provision of health care to an individual or the past, present, or future payment for health care; (g) Critical Energy Infrastructure Information – as defined by Federal Energy Regulatory Commission ("FERC") regulations; (h) Information determined to be market-sensitive by FERC; (i) Bulk Cyber System Information – as defined by the North American Electric Reliability Corporation; (j) Chemical-Terrorism Vulnerability Information – as defined by the Department of Homeland Security's Chemical Facility Anti-Terrorism Standards; (k) Information deemed sensitive by the Nuclear Regulatory Commission; and (l) Information deemed sensitive by the Illinois Commerce Commission and/or the Missouri Public Service Commission and other applicable state statutes, regulations, or administrative orders. Ameren Data shall also include any and all data, documentation, methods, processes, materials, and all other information related to employees, shareholders, retirees, customers, contractors and/or suppliers of Ameren or its Affiliates, or utilized by Ameren or its Affiliates as part of its/their businesses or operations.

"Disclosed" means any circumstance when the security, integrity, or confidentiality of any Ameren Data has been compromised, including but not limited to incidents where Ameren Data has been damaged, lost, corrupted, destroyed, or accessed, acquired, modified, used, or disclosed by any unauthorized person, by any person in an unauthorized manner, or for an unauthorized purpose.

"Malware" shall mean the software used for disrupting computer operations, unauthorized altering or destroying of any information, gathering unauthorized sensitive information, and gaining unauthorized access to computer systems. Malware is commonly taken to include computer viruses, worms, Trojan horses, bots, root kits, spyware, ransomware, and adware.

"Security Incident" means any circumstance when (i) Supplier knows or reasonably believes that Ameren Data hosted or stored by the Supplier has been Disclosed; (ii) Supplier knows or reasonably believes that an act or omission has compromised or may reasonably compromise the cybersecurity of the products and services provided to Ameren by Supplier or the physical, technical, administrative, or organizational safeguards protecting Supplier's systems or Ameren's systems storing or hosting Ameren Data; or (iii) Supplier receives any complaint, notice, or communication which relates directly or indirectly to (A) Supplier's handling of Ameren Data or Supplier's compliance with the data safeguards in this Contract or applicable law in connection with Ameren Data or (B) the cybersecurity of the products and services provided to Ameren by Supplier.

Article B1 Data Protection

1. All Ameren Data maintained and the Services performed involving such Ameren Data must be retained and performed within the United States ("U.S."), unless Ameren is notified in advance by Supplier and has agreed in writing that the Ameren Data may be maintained or Services may be performed at the indicated non-U.S. location(s). Such approval may be revoked by Ameren in whole or in part at any time.
2. All Ameren Data must be encrypted at all times and protected against unauthorized access, disclosure, modification, or deletion.
3. Supplier shall notify Ameren within twenty-four hours of a confirmed Security Incident at Ameren's Network Operations Center by telephone and email, and subsequently via written letter. The written notice shall include the date and time of the Security Incident's occurrence (or the approximate date and time of the occurrence if the actual date and time of the occurrence is not precisely known) and a detailed summary of the facts and circumstances of the Security Incident, including a description of (a) why the Security Incident occurred (e.g., a precise description of the reason for the system failure), (b) the amount of Ameren Data known or reasonably believed to have been Disclosed, and (c) the measures being taken to address and remedy the occurrence to prevent the same or a similar event from occurring in the future. Supplier shall provide written updates of the notice to Ameren addressing any new facts and circumstances learned after the initial written notice is provided and shall provide such updates within a reasonable time after learning of those new facts and circumstances.
4. Supplier shall not grant access to Ameren Data to a third party without prior written authorization from Ameren.
5. Supplier shall only process, transfer, or store data as authorized by Ameren.
6. Upon completion of the delivery of the products and services to be provided under this Contract, or at any time upon Ameren's request, Supplier will return to Ameren all hardware and removable media provided

by Ameren containing Ameren Data. Ameren Data in such returned hardware and removable media shall not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by Ameren. If the hardware or removable media containing Ameren Data is owned by Supplier or a third-party, a notarized statement detailing the destruction method used and the data sets involved, the date of destruction, and the entity or individual who performed the destruction will be sent to a designated Ameren security representative within fifteen (15) calendar days after completion of the delivery of the products and services to be provided under this Contract, or at any time upon Ameren's request. Supplier's destruction or erasure of Ameren Data pursuant to this Section shall be in compliance with best industry practices (e.g., Department of Defense 5220-22-M Standard, as may be amended). Notwithstanding the foregoing, in the event that Supplier's document retention and destruction practices render the foregoing obligations impractical or impossible within thirty (30) calendar days, Supplier shall comply with such requirement at its earliest opportunity and shall advise Ameren in writing of its efforts to preserve and protect Ameren Data. In addition, during such period, Supplier shall ensure that Ameren Data is not disclosed or otherwise disseminated to third parties, and shall be responsible for any such claims arising out of such disclosure or dissemination. This obligation shall survive termination or expiration of this Contract.

7. In all instances where Supplier will have access to Ameren Data, networks, systems, and/or software, Supplier shall disclose or provide access to Ameren Data, networks, systems, and software only to authorized and agreed upon agents who have a need to have access to such Ameren Data, networks, systems, and/or software in order to provide Deliverables and Services under this Contract.

Article B2 General Cybersecurity Practices

1. To the extent permissible by law, Supplier shall be responsible to ensure that Supplier and its Subcontractors shall at all times maintain and enforce lawful policies and procedures to verify that the individuals assigned by Supplier or its Subcontractors to perform Services or Deliverables do not have criminal conviction histories or have impairments associated with the use of alcohol and "controlled substances" (as defined by Section 812 of the Controlled Substances Act, as amended) that would render such individuals unqualified to competently and safely (as to themselves and Ameren's employees and customers) perform the Services or Deliverables. Supplier, on behalf of itself and its Subcontractors, shall provide to Ameren any documents requested by Ameren to verify that Supplier and its Subcontractors are in compliance with this provision, and Ameren has the right to require that the verifications required by this provision be refreshed from time to time.

2. Upon request, Supplier will have, at a minimum, an annual site audit of Supplier's Information Technology general controls including, but not limited to, information security, privacy, and confidentiality controls, performed by a recognized third-party audit firm, which shall be provided to Ameren within thirty (30) days of its completion. The audit shall comply with the requirements of the American Institute of Certified Public Accountants' (AICPA) attestation standards SSAE 18, or the equivalent standard recognized by the industry at the time of such report (the "SOC Report") or shall comply with the requirements of the International Organization for Standardization (the "ISO Certification"). The SOC Report shall include both a Type I report and a Type II report, upon Ameren's written request. Ameren reserves the right to request additional site audits if a SOC Report or ISO Certification has revealed a security issue, or a security incident involving Supplier has been identified, which Supplier shall complete within sixty (60) days from the date requested. Any control exceptions noted in the SOC Report or equivalent will be addressed in the report with management's corrective action.

a. The SOC Report and ISO Certification shall be performed by a recognized third-party audit firm engaged by Supplier. Supplier shall provide Ameren with the results of each SOC Report and ISO Certification with respect to Supplier's security measures relating to electronic data at all facilities where Ameren Data is stored or accessed during the term of this Contract, regardless of the location of such facilities:

b. Supplier shall provide a copy of the related report and consents to the provision of copies of such report by Ameren to applicable regulators.

c. The report or attestation shall contain Supplier's management's response to the exception comments, if any are noted, together with appropriate target dates for completion of required changes. Supplier shall follow Ameren policies for the protection and operation of digital assets when accessing Ameren's networks or systems.

3. In the event that Malware is introduced into any Ameren network, system, software, or Ameren Data through any fault of Supplier, then Supplier shall promptly provide assistance to Ameren as requested to remove, quarantine, or remedy the effect of such Malware at Supplier's expense.

4. Supplier will provide to Ameren the Supplier's redacted cybersecurity policy which shall be consistent with industry standard practices (e.g., NIST Special Publication 800-53 (Rev. 4) as may be amended). Supplier will implement and comply with its established cybersecurity policy.

5. Ameren or its third-party designee may, but is not obligated to, request evidence that Supplier has undergone a high-confidence audit of Supplier's IT or systems environment and procedural controls, to include compliance with industry standard practices and NIST Special Publication 800-171. Ameren may use this information to determine Supplier's compliance with the system, network, data, and information security requirements of this Contract.

Article B3 Incident Response

1. Supplier shall develop and implement a "Response Plan," which shall include policies and procedures to address Security Incidents. The Response Plan shall include appropriate provisions for mitigating the harmful effects of Security Incidents and addressing and remedying the occurrence(s) to prevent the recurrence of similar Security Incidents in the future. Supplier shall provide Ameren access to inspect Supplier's Response Plan. The development and implementation of the Response Plan shall follow industry standard practices, such as those that at a minimum are consistent with the contingency planning requirements of NIST Special Publication 800-61 Rev. 2, NIST Special Publication 800-53 Rev. 4, CP-1 through CP-13 and the incident response requirements of NIST Special Publication 800-53 Rev. 4, IR-1 through IR-10 as those standards may be amended.
2. Within ninety days of a Security Incident, Supplier shall develop and execute a plan that reduces the likelihood of the same or a similar Security Incident from occurring in the future consistent with the requirements of its Response Plan and industry standards (e.g., NIST Special Publication 800-61 Rev. 2 and NIST Special Publication 800-184, as may be amended,) and shall communicate that plan to Ameren. Supplier shall provide recommendations to Ameren on actions that Ameren may take to assist in the prevention of recurrence, as applicable or appropriate.
3. Within seven days of notifying Ameren of the Security Incident, Supplier shall recommend actions to be taken by Ameren on Ameren-controlled systems to reduce the risk of a recurrence of the same or a similar Security Incident, including, as appropriate, the provision of action plans and mitigating controls. Supplier shall

coordinate with Ameren in developing those action plans and mitigating controls. Supplier will provide Ameren guidance, recommendations, and other necessary information for recovery efforts and long-term remediation and/or mitigation of cyber security risks posed to Ameren Data, equipment, systems, and networks as well as any information necessary to assist Ameren in relation to the Security Incident.

4. Supplier will, at its sole cost and expense, assist and cooperate with Ameren with respect to any investigation of a Security Incident, disclosures to affected parties, and other remedial measures as requested by Ameren in connection with a Security Incident or required under any applicable laws related to a Security Incident.

5. In the event a Security Incident results in Ameren Data being Disclosed such that notification is required to be made to any person or entity, including without limitation any customer, shareholder, or current or former employee of Ameren under any applicable laws, including privacy and consumer protection laws, or pursuant to a request or directive from a governmental authority, such notification will be provided by Ameren, except as required by applicable law or approved by Ameren in writing. Ameren will have sole control over the timing and method of providing such notification.

Article B4 Access Revocation

1. Supplier shall develop and implement policies and procedures to address the security of Supplier's remote and onsite access to Ameren Data, Ameren systems and networks, and Ameren property (an "Access Control Policy") that is consistent with the personnel management requirements of industry standard practices (e.g., NIST Special Publication 800-53 Rev. 4 AC-2, PE-2, PS-4, and PS-5 as may be amended) and also meets the following requirements:

    a. In the course of furnishing products and services to Ameren under this Contract, Supplier shall not access, and shall not permit its employees, agents, Suppliers, and other personnel or entities within its control ("Supplier Personnel") to access Ameren's property, systems, or networks or Ameren Data without Ameren's prior express written authorization. Such written authorization may subsequently be revoked by Ameren at any time in its sole discretion. Further, any Supplier Personnel access shall be consistent with, and in no case exceed the scope of, any such approval granted by Ameren. All Ameren authorized connectivity or attempted connectivity to Ameren's systems or networks shall be in conformity with Ameren's security policies as may be amended from time to time with notice to the Supplier.

    b. Supplier will review and verify Supplier Personnel's continued need for access and level of access to Ameren Data and Ameren systems, networks and property on a semi-annual basis and will retain evidence of the reviews for two years from the date of each review.

    c. Supplier will immediately notify Ameren in writing (no later than close of business on the same day as the day of termination or change set forth below) and will immediately take all steps necessary to remove Supplier Personnel's access to any Ameren Data, systems, networks, or property when:

        i. any Supplier Personnel no longer requires such access in order to furnish the services or products provided by Supplier under this Contract;

ii. any Supplier Personnel is terminated or suspended or his or her employment is otherwise ended;

iii. Supplier reasonably believes any Supplier Personnel poses a threat to the safe working environment at or to any Ameren property, including to employees, customers, buildings, assets, systems, networks, trade secrets, confidential data, and/or employee or Ameren Data;

iv. there are any material adverse changes to any Supplier Personnel's background history, including, without limitation, any information not previously known or reported in his or her background report or record;

v. any Supplier Personnel loses his or her U.S. work authorization; or

vi. Supplier's provision of products and services to Ameren under this Contract is either completed or terminated, so that Ameren can discontinue electronic and/or physical access for such Supplier Personnel.

Supplier will take all steps reasonably necessary to immediately deny such Supplier Personnel electronic and physical access to Ameren Data as well as Ameren property, systems, or networks, including, but not limited to, removing and securing individual credentials and access badges, RSA tokens, and laptops, as applicable, and will return to Ameren any Ameren-issued property including, but not limited to, Ameren photo ID badge, keys, parking pass, documents, or laptop in the possession of such Supplier Personnel. Supplier will notify Ameren once access to Ameren Data as well as Ameren property, systems, and networks has been removed.

Article B5 Remote Access

1. Supplier shall coordinate with Ameren on all remote access to Ameren's systems and networks, regardless of interactivity, and shall comply with any controls for interactive remote access and system-to-system remote access sessions requested by Ameren.

    a. Suppliers that directly, or through any of their affiliates, sub-Suppliers or service providers, connect to Ameren's systems or networks agree to the additional following protective measures:

        i. Supplier will not access, and will not permit any other person or entity to access, Ameren's systems or networks without Ameren's written authorization and any such actual or attempted access will be consistent with any such written authorization.

        ii. Supplier shall implement processes designed to protect credentials as they travel throughout the network and shall ensure that network devices have encryption enabled for network authentication to prevent possible exposure of credentials.

        iii. Supplier shall ensure Supplier Personnel do not use any virtual private network or other device to simultaneously connect machines on any Ameren system or network to any machines on any Supplier or third-party systems, without

            i. using only a remote access method consistent with Ameren's remote access control policies;

ii. providing Ameren with the full name of each individual who uses any such remote access method and the phone number and email address at which the individual may be reached while using the remote access method; and

iii. ensuring that any computer used by Supplier Personnel to remotely access any Ameren system or network will not simultaneously access the Internet or any other third-party system or network while logged on to Ameren systems or networks.

iv. Supplier shall ensure Supplier Personnel accessing Ameren networks are uniquely identified and that accounts are not shared between Supplier personnel.

Article B6 Vulnerability Management

1. Supplier shall implement a vulnerability detection and remediation program consistent with industry standards (e.g., ISO-27417 Vulnerability Disclosure, NIST Cybersecurity Framework v1.1 Reference RS.AN-5, NIST Special Publication 800-53 Rev. 4 RA-5, SA-11, and SI-2, as may be amended. Supplier shall ensure all relevant patches, system updates, and bug fixes are implemented on systems, applications, and networks under Supplier's care throughout the term of the Contract and so long thereafter as Supplier is in possession of, or has access to, Ameren Data or its systems.
2. Supplier shall identify or provide Company with a method to identify the country (or countries) of origin of the procured Supplier product and its components (including hardware, software, and firmware). Supplier will identify the countries where the development, manufacturing, maintenance, and service for the Supplier product are provided. Supplier will notify Ameren of changes in the list of countries where product maintenance or other services are provided in support of the procured Supplier product. This notification in writing shall occur at least 180 days prior to initiating a change in the list of countries.